Dual Image Steganography for Communicating High Security Information

Ketki Thakre, Nehal Chitaliya

Abstract: ***The recent growth in computational power and technology has propelled the need for highly secured data communication. One of the best techniques for secure communication is Steganography-a covert writing. It is an art of hiding the very existence of communicated message itself. The process of using steganography in conjunction with cryptography, called as Dual Steganography, develops a sturdy model which adds a lot of challenges in identifying any hidden and encrypted data. Using cryptographic techniques to encrypt data before transmission may forestall any type of security problems. But the camouflaged appearance of encrypted data may arouse suspicion. Therefore using steganography inside steganography, give rise to improved version of dual steganography which will provide better security. This paper presents a technique for hiding data with two level of security to embed data along with good perceptual transparency and high payload capacity. Here the secret data is not restricted to images only but also applicable to any text, audio or video.***

Index Terms**: *Cryptography, Dual Steganography, LSB Technique, Steganography***

I. INTRODUCTION

Steganography is the science of invisible communication [1] which hides any private data within an innocent-looking cover object. The word Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing" [5].

Steganography is different from cryptography. The goal of cryptography is to provide secure communications by transforming the data into a form that cannot be understood. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it cumbersome for a third person to find out the message. Unlike steganography, sending encrypted information may draw attention. Accordingly, cryptography is not the good solution for secure communication but only part of the solution. Both techniques can be used together to better protect information [4]. The basic steganography model is shown in Fig.1.

The model consists of Carrier (C), Secret Data (D), and Stego Key (K). Carrier is the cover object in which the secret message is embedded. Secret data can be any type of confidential data i.e. plain text, cipher text or other image. Key mainly used to ensure that only recipient having the decoding key will be able to retrieve the secret message from the cover object. With the help of embedding algorithm, the secret data is embedded into the cover object in a way that does not change the original image in a human perceptible way. Finally, the stego object which is the output of the process is nothing but the cover object with embedded secret data.

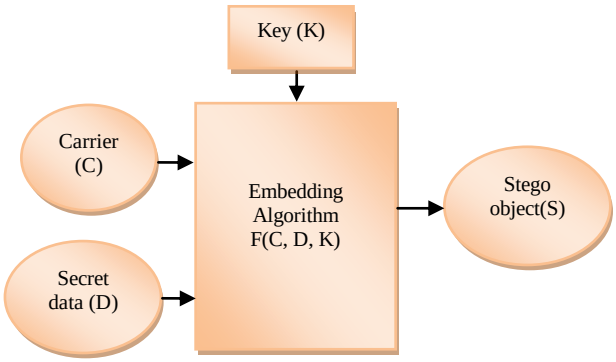


Fig.1 The Steganography Model [2]

Steganography can be used for wide range of applications such as defence organizations for safe circulation of private information, intelligence agencies for storing any confidential data, in smart identity cards where personal details are embedded inside the photograph for copyright purpose, medical imaging where patient's details are embedded within image for protection of information and also for reducing transmission time [2].

There are different types of steganography. They are as follows: a) Text steganography- In this method, the secret data is hidden in every nth letter of every word of a text message [12]. b) Image steganography- This technique exploits the weakness of the human visual system (HVS) [4]. c) Audio steganography- Audio steganography takes the benefit of psychoacoustical masking phenomenon of the human auditory system [HAS] [19]. d) Video steganography- Generally video files are a collection of images and audios. So most of the presented techniques used on images and audio, can also be applied to video files [6]. e) Protocol steganography- In this steganography, the secret information is embedded within messages and network control protocols which are used in network transmission [20].

There are various steganographic techniques for image file format which are as follows: a) spatial domain- It is a time domain (pixel based) and here the secret messages are embedded directly in the cover object [8]. b) Transform domain- Here the information is hidden in frequency domain

Manuscript received on July, 2014.

Ms. Ketki Thakre, P.G. Scholar (E&C dept.), Sardar Vallabhbhai Patel Institute of Technology (SVIT), Vasad, India,

Dr. Nehal G. Chitaliya, Associate Prof.(E&C dept.) , Sardar Vallabhbhai Patel Institute of Technology (SVIT), Vasad, India,

by changing the magnitude of all of transform coefficients of cover image [4]. c) Masking and filtering- These techniques embed the information in the more significant areas instead of hiding it into the noise level [4]. d) Distortion Techniques- It requires the knowledge of the original cover image during the data extraction process to restore the secret message [4].

This paper focuses on high payload capacity and good imperceptibility in addition to high security to secret data. Remaining paper is organized in the following sections: Section 2 describes the literature survey; section 3 presents the proposed scheme; section 4 shows the experimental results and finally conclusion is presented in section 5.

II. LITERATURE SURVEY

Shilpa Gupta, Geeta Gujral and Neha Aggarwal [11] developed an enhanced LSB algorithm which embeds the secret data only in one i.e. blue component instead of all RGB components. With this new technique, the performance of LSB has been improved which leads to the minimization of the distortion level that is negligent to human eye. This will increase the robustness but will decrease the payload capacity.

Shailender Gupta, Ankur Goyal and Bharat Bhushan [1] developed a technique for hiding data using LSB steganography and cryptography where the secret information is encrypted using RSA or Diffie Hellman algorithm before embedding in the image with the help of LSB method. With the proposed technique, time complexity is increased but high security is achieved at that cost.

Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri [13] proposed a DWT based Dual steganographic technique. By using DWT, a cover image is decomposed into four subbands. Two secret images are hidden within HL and HH subbands respectively by usage of a pseudo random sequence and a session key. By this technique fair amount of information is transferred in a secured way with an acceptable level of imperceptibility.

K.Sakthisudhan and P.Prabhu [14] proposed a dual steganography approach in which the secret data is firstly converted to encrypted form and then LSB technique of steganography is used to embed it within cover object. By this method, message is transferred with utmost security and can be retrieved without any loss of data.

Rosziati Ibrahim and Teoh Suk Kuan [15] developed a SIS (Steganography Imaging System) in which two layers of security are used, firstly username and password are required and once login done, key is used to embed the secret data. Due to this, integrity and privacy is maintained.

Weiqi Luo, Jiwu Huang and Fangjun Huang [16] proposed a technique in which the secret data is embedded in the edges of the objects of an image. With the proposed scheme, embedding regions are selected according to size of secret message and difference between two consecutive pixels in cover image. Here, LSB matching revisited is used which uses a pair of pixels as embedding unit. Sharper images are selected for hiding data so that good security and visual quality is increased.

Mazen Abu Zaher [17] developed a modified LSB method in which 8 bit ASCII codes of secret message are converted into 5 bit codes with the aid of encryption algorithm and then embedded in the cover image by using LSB method. So with this scheme, more amount of information can be hidden with a level of protection.

Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and G.M.Bhat [21] developed a technique in which steganography and cryptography are used together, in which the cover image is first converted into scrambled form and then divided into bit planes in which the secret data is embedded. With this method, good imperceptibility along with high security is obtained but has less payload capacity and also limited to grayscale images only.

Phad Vitthal S., Bhosale Rajkumar S. and Panhalkar Archana R. [22] proposed a novel security scheme in which steganography is combined with cryptography. In this scheme, secret data is converted to encrypted form using Advanced Encryption Standard (AES) and then the encrypted data is embedded into the cover image using Pixel Value Differencing (PVD) and K-bit LSB substitution method of steganography. Due to which high security along with good imperceptibility and sufficient amount of payload capacity is obtained.

III. PROPOSED WORK

In the proposed scheme, dual image steganography is used. The reason behind using image steganography is that images are more popular among the internet users. In this work, 4 bit LSB substitution technique falling under the category of spatial domain is used by which high security is achieved for secret data along with good amount of imperceptibility as well as high payload capacity. Here new version of dual steganography is used where steganography is used within steganography. Section A and B presents the data hiding and data extraction process for the proposed scheme.

A. Data Hiding Process

The block diagram for the proposed data hiding technique is shown in Fig.2. Here two cover images are used i.e. cover image1 and cover image2. For providing more security two stego keys are used which are different from each other. The stego key used is of 10 bit in length. The key can be made of numbers, characters, and symbols but should be of 10 bit length. These keys are hidden in the cover image during the hiding process. This should be known at the receiver side during the decoding process for retrieving the secret file.

As shown in Fig.2; the secret data has been embedded inside the cover image1 with the help of 4 bit LSB embedding algorithm along with the stego key1 mainly used for security purpose from which stego image1 is generated. Next, the stego image1 is considered as the secret data and hidden inside the cover image2 using 4-bit LSB algorithm and stego key2 after which final stego image is generated.

The algorithm works as follows:

1) Cover image1 is separated into RGB planes.
2) Secret data taken is then converted into binary form.
3) Those values are separated into upper and lower nibbles which are embedded in two separate planes of the cover image1.
4) Upper nibbles are embedded in green plane and lower nibbles in red plane.
5) Stego key is embedded inside the blue plane.
6) After which, all the three planes are combined to generate stego image1.
7) Stego image1 is then interpreted as secret data and embedded in the cover image2 using the same algorithm and thus the final stego image is generated.

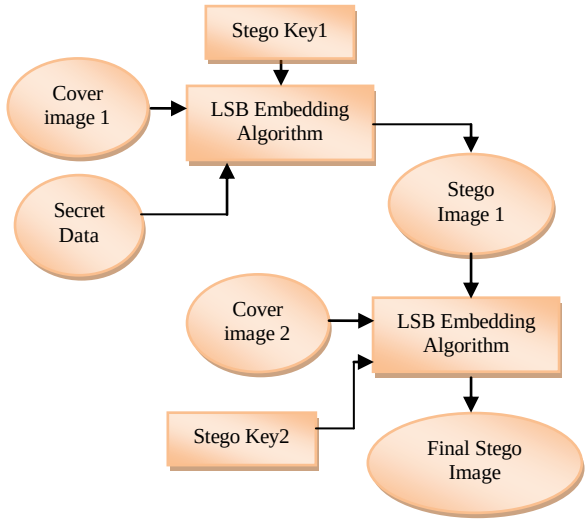


Fig.2 New Data Hiding Process

The purpose of using two planes instead of three planes is to maintain the perceptual quality of cover image along with good amount of embedding capacity. Embedding the secret data in binary form in two separate planes will ensure that it cannot be easily retrieved by the eavesdropper.

B. Data Extraction Process

The block diagram of data extraction process is presented in Fig.3. From the final stego image, the stego image1 is extracted using stego key1 and LSB recovery algorithm. Next, from stego image1, secret data is extracted by using stego key2 and same LSB recovery algorithm. The proposed scheme is irreversible one as the cover image is not recovered at the receiver side.

The algorithm works as follows:

1) Final stego image is separated into RGB planes.
2) Stego key which acts as password is entered which is then verified with the stored key that is embedded in the blue plane of cover image2.
3) If the key is matched then the upper and lower nibbles of binary secret data is extracted from green and red planes respectively.
4) Then the upper and lower nibbles are combined to make the binary form of stego image1.
5) Finally, the original stego image1 is obtained from binary form.
6) Next, using the same algorithm the original secret data is retrieved from stego image1.

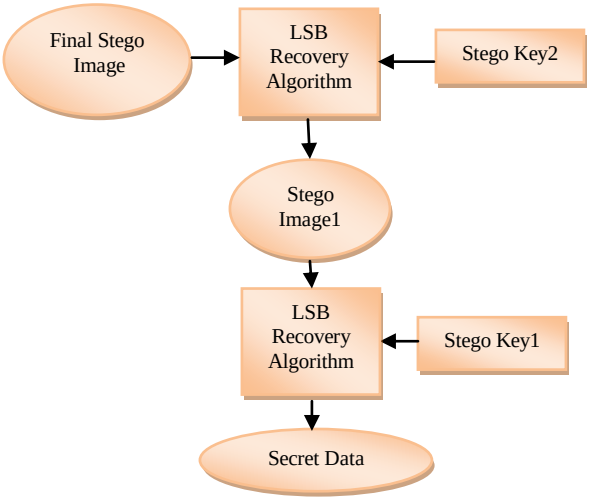


Fig.3 Data Extraction Process

The extraction process is strictly blinded as the secret data is extracted from stego image without the original cover image reference. This is done by using the same key at the receiver side whichever was used at the transmitter side. The complete and successful extraction of data needs the knowledge of keys-K1 and K2 which been extracted from blue plane of cover image. To make the secret data extraction more cumbersome, the concept of hiding the secret data in two planes has been adopted.

IV. EXPERIMENTAL RESULTS

There are three main requirements of data hiding techniques-imperceptibility, security and robustness. Robustness is mainly related to watermarking systems whereas imperceptibility and security are related to steganographic system. Payload is also one of the important parameter to be considered in application based steganographic system. The efficiency of the proposed method has been computed in terms of following image quality metrics.

A. Image Quality Metrics

Two image quality parameters are described below: 1) MSE and 2) PSNR. If Cj,k and Sj,k respectively represent original image and its corresponding stego image, P and Q are number of pixels in row and column directions, respectively[21].

1) Mean Square Error (MSE):

$$MSE = 1/PQ \left(\sum_{j=1}^{p} \sum_{k=1}^{Q} (Cj,k - Sj,k)^2\right) \quad (1)$$

It can be computed by performing byte by byte comparisons of the cover image and stego image. Higher the value of MSE indicates dissimilarity between compared images [9].

2) Peak Signal to Noise Ratio (PSNR):

$$PSNR = 10 \log 10 \left(255^2/MSE\right) \quad (2)$$

It measures the quality of the stego image with cover image. Higher PSNR means better the quality of image. It is measured in decibels [9].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

B. Imperceptibility Analysis

In this section, the experimental results are analyzed in terms of mentioned image quality metrics. The experimental work has been carried out on Intel core i3-330M, 2.1 Ghz processor with 3GB RAM. The simulations of the work has been carried on MATLAB 2010a running on Windows 7 platform. The proposed scheme has been tested on number of RGB images of size (512x512). The scheme embeds 25% of secret data in the cover image. Table I shows all the images that have been tested with their corresponding stego images. Table II shows the MSE and PSNR values of all the tested images. To check efficacy of the proposed scheme in terms of imperceptibility, the obtained results are compared with [21, 22] and results are presented in Table III. Fig.4 shows the comparison results in the graphical form. The proposed system provides good PSNR values in addition to two level of security.

C. Security Analysis

Data hiding system is said to be secured if little knowledge of hiding algorithm does not help the eavesdropper to detect hidden data or know the secret data. Stego keys play an important role in improving the security of data hiding technique. As in the proposed work, two different stego keys are used, the system is said to be double protected.

In order to enhance the security, in proposed work instead of combining cryptography with steganography, only steganography is used twice. The reason behind this is that National Security Agency (NSA) has developed a quantum computer that could crack most types of encryption algorithms. So if the steganography is partly defeated then secret data becomes visible which can be cracked using quantum computer. Therefore if steganography is used two times, then even if at first level steganography gets defeated then the second level will keep the secret data secured.

D. Payload Capacity Analysis

In the proposed work, the secret data is not necessarily to be image only; it can be various other files as PDF, Word Document, Matlab, Zip, Excel, PPT and MP3/MP4.

From the Table IV, two types of secret files are considered for the analysis purpose.i.e PPT and excel file with different sizes. By increasing the size of the files manually and embedding inside the cover image, it has been concluded that for given cover image, almost 4.7times of cover image size, the secret data can be embedded which is equal to 750kb in this case As the secret file is converted in binary format, its hidden depending upon the number of pixels of the cover image. So the payload capacity of secret file is dependent on the number of pixels of cover image. Therefore, secret file capacity differs from one cover to other cover image.

One of the advantage of this work is that its not necessary to take secret file 25% or 50% of the cover image but it can be taken twice the size of cover image also. And along with that the retrieved secret file is exact the same as that of the original one with 0% of data loss which is the biggest advantage of this method.

Table I Cover images and corresponding Final Stego images

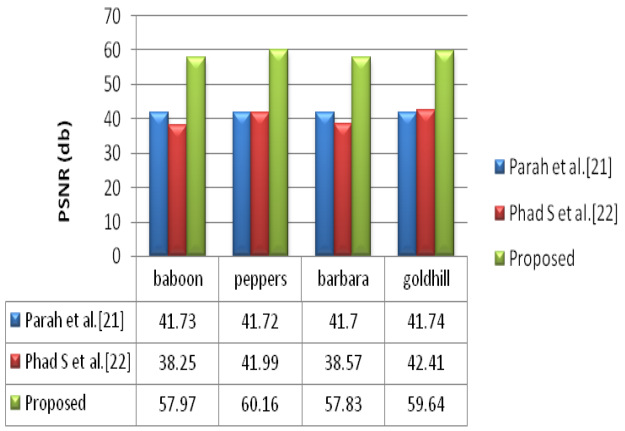
Cover image2	Final Stego image
	
	
	
	
	

Table II MSE and PSNR Values of Tested Images

Cover Image	MSE	PSNR (dB)
Baboons	0.099	57.97
Peppers	0.062	60.16
Barbara	0.094	57.83
Gold hill	0.070	59.64
Choco	0.069	59.74

Table III Comparison of proposed technique with [21, 22]

Cover Image	PSNR in decibels (dB)		
	Parah et al.[21]	Phad S et al.[22]	Proposed
Baboons	41.73	38.25	57.97
Peppers	41.72	41.99	60.16
Barbara	41.70	38.57	57.83
Goldhill	41.74	42.41	59.64



	baboon	peppers	barbara	goldhill
Parah et al.[21]	41.73	41.72	41.7	41.74
Phad S et al.[22]	38.25	41.99	38.57	42.41
Proposed	57.97	60.16	57.83	59.64

Fig.4 Comparison of proposed scheme with [21, 22]

Table IV Analysis of maximum payload capacity

Cover Image	Original Secret File	Max. Capacity of Secret File embedded and retrieved successfully
Choco.jpg 960*800pixels 158kb	1. PPT (208kb) 2. Excel file(60kb)	Both files expanded max. upto **750kb** (4.7 times of cover image)

V. CONCLUSIONS

Information security has become one of the most significant problems due to the exponential growth of internet users. Unauthorized access to secret data can have serious repercussions like financial loss etc. Steganography is one of the solutions whose goal is to hide the existence of communicated message. In this paper, highly secured data hiding technique has been presented where steganography is used inside steganography. The proposed method embeds data in two cover images using four bit LSB technique. The secret data is hidden in binary form in two cover images due to which double protection has been provided to confidential data which can be any text, audio, video or image. The experimental results show that the proposed scheme can be a good alternative for secure communication where two level of security is obtained in conjunction with high payload capacity and good imperceptibility.

ACKNOWLEDGMENT

I place my sincere thanks and regards to my project guide (Ph.d) Dr. Nehal Chitaliya for her excellent support in my dissertation work. I extend my thanks to all other teachers who supported me throughout my work. I am also thankful to all my friends for their wonderful encouragement.

REFERENCES

1. Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" International Journal Modern Education and Computer Science, vol. 6, pp. 27-34, 2012
2. Kanzariya Nitin K, Nimavat Ashish V., "Comparison of Various Images Steganography Techniques" International Journal of Computer Science and Management Research, vol. 2,pp. 1213-1217, 2013
3. Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications, vol. 9, pp. 19-23, 2010
4. Pratap Chandra Mandal, "Modern Steganographic technique: A survey", International Journal of Computer Science & Engineering Technology, vol. 3, pp. 444-448, 2012
5. T. Sharp, "An implementation of key-based digital signal Steganography", Proc. Information Hiding Workshop, Springer, vol. 2137, pp. 13-26, 2001
6. Johnson, Neil F., "Steganography", IRM Conference, 2000
7. Johnson, N.F and Jajodia, S., "Exploring Steganography: Seeing the Unseen", IEEE Computer Journal, vol. 31, pp. 26-34, 1998
8. H. Arafat Ali "Qualitative Spatial Image Data Hiding for Secure Data Transmission" International Journal on Graphics, Vision and Image Processing, vol. 7, pp. 35-43, 2007
9. Himanshu Gupta, Prof. Ritesh Kumar, Dr. Soni Changlani, "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging Technology and Advanced Engeneering,vol.3,pp. 212-214,2013
10. Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar "Image Steganography Using Least Significant Bit With Cryptography" Journal of Global Research in Computer Science, vol. 3, pp. 53-55 , 2012
11. Shilpa Gupta, Geeta Gujral and Neha Aggarwal, " Enhanced Least Significant Bit algorithm For Image Steganography", International Journal of Computational Engineering & Management, vol. 15, pp. 40-42, 2012
12. T. morkel , J.h.p. eloff , M.s. olivier "An overview of image Steganography", Information and computer security architecture research group ,pp. 1-11, 2005
13. Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum" International Journal of Modern Engineering Research, vol. 1, pp. 157-161, 2012
14. K.Sakthisudhan, P.Prabhu, "Dual Steganography Approach for Secure Data Communication" International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering, vol. 38, pp. 412-417, 2012
15. Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application, vol. 2, pp. 102-108, 2011
16. Weiqi Luo, Jiwu Huang, Fangjun Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, vol. 5, pp. 201-214, 2010
17. Mazen Abu Zaher, "Modified Least Significant Bit (MLSB)" Computer and Information Science, vol. 4, pp. 60-67, 2011
18. Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, pp. 1-8, 2001
19. Ronak Doshi, Pratik Jain, Lalit Gupta, "Steganography and Its Applications in Security" International Journal of Modern Engineering Research, vol. 2, pp.4634-4638, 2012
20. Udit Budhiaa, Deepa Kundura. "Digital video steganalysis exploiting collusion sensitivity", Proc. of SPIE. vol. 5403, pp. 210-221,2004
21. Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and G.M. Bhat, "Data hiding in scrambled images: A new double layer security data hiding technique" Computers and Electrical Engineering, Elsevier,vol. 40,pp. 70-82, 2014
22. Phad Vitthal S.,Bhosale Rajkumar S.,Panhalkar Archana R., " A Novel Security for Secret Data using Cryptography and Steganography" International Journal Computer Network and Information Security, vol. 2, pp. 36-42,2012

AUTHORS PROFILE

Ms. Ketki Thakre received the Bachelor degree in Electronics and Communication from Babaria Institute of Technology, Vadodara, India in 2011. She is currently pursuing the Master degree in Electronics and Communication Engineering from Sardar Vallabhbhai Patel Institute of Technology, Vasad, India. Her research interests include Digital Image Processing.

Dr. Nehal G. Chitaliya received B.E Electrical (1996) and M.E Electrical(2000) and Ph.D. Electrical (2013) from the Electrical Engineering department, Faculty of Technology and Engineering, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India. She is Associate Professor of Electronics and Communication Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India. Her research interests are in the field of Digital Image Processing, Signal Processing and Motion Analysis. Dr. Chitaliya is a member of professional bodies like Indian society for Technical Education (ISTE) and International Association of Computer Science and Information Technology (IACSIT).