ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Review on Steganography and BPCS Technology in Steganography for Increasing Data Embedding Capacity

Chintan Jain, VivekParate, Ajay Dhamanikar, Rakesh Badgujar.

MITAOE, Alandi(D), Pune University, Pune, Maharashtra, India.

ABSTRACT: Nowadays, Internet has become a convenient way for data transmission due to a fast development of modern technology. Data transmission over internet is done in many ways such as email, sms, via chat application etc. Protection for confidential data send over internet has become a necessity as unauthorized access to data by an intruder accessing it have become common, hacker also attack data via viruses for their own benefits have raised concern for protecting data. Various data hiding methods are being implemented such as steganography, cryptography and hybrid cryptography. This paper gives overview of steganography, its methods and review of existing BPCS (Bit Plane Complexity Segmentation) steganography technique which can be used to increase the data embedding capacity of image.

KEYWORDS:, Steganography, Steganography model,BPCS Steganography.

I. INTRODUCTION

With the advancements in digital technologies of communication, the growth of computer power and storage demand for Information security and privacy has a major concern in the recent years due to the increased data communication over internet. Information security is a major issue of concern while exchanging data in an open network. Encryption and steganography methods are developed for providing security to data which is transferred over a network. Fig 1 shows classification of steganography based on encoding method of secret information.

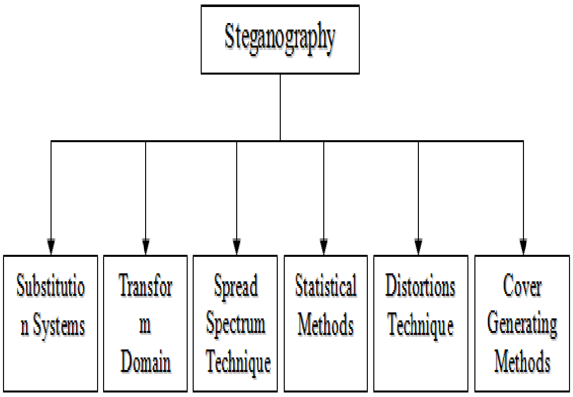


Fig. 1: Classification of steganography

Various steganography methods:

- *Substitution method:*In substitution method the redundant parts of the cover image are substituted by contents of the secret message.
- *Transform domain method:*This embeds secret information in a transform space of the signal (frequency domain).
- *Spread spectrum technique:* This technique adopts ideas from spread spectrum communication.

- *Statistical method:* The secret information is encoded by changing several statistical values of the cover image.
- *Distortion techniques:* This technique stores information by signal distortion and measure the deviation from the original cover in the decoding step.
- *Cover generation method:* Here the encoding is done in such a way that a secret communication is created.

Steganography is the art and science of writing hidden messages such that only the sender and intended recipient knows the existence of the message [1, 2]. Cryptography scrambles a message with the help of certain cryptographic algorithms for converting the secret data into unintelligible form whereas hiding of message in cover image is made in steganography so that it becomes invisible[18]. Sending a message in the form of cipher text might lead for suspicion on the part of the recipient whereas an “invisible” message created with steganographic algorithms will not. Anyone who needs to perform secret communication can use cryptographic algorithms to scramble the data before performing steganography to achieve additional security. For a steganography algorithm, a cover image is given or chosen, and the embedding process generates a stego-image using stego-key. The extraction method takes the stego image and applies the inverse algorithm using the shared key to extract the hidden message [3]. Table of comparison in cryptography and steganography is as shown in Table I.

Table I: Comparison of Steganography and Cryptography.

Criteria	Steganography	Cryptography
Carrier	Any kind of digital media	Plaintext/ image/audio
Hiding information	Yes	No
Additional carrier	Required	Not required
Hidden message	Imperceptible	Detection of message is possible
Key	Optional	Required
Visibility	Never visible	Always visible

Basic Steganography Model:

A basic steganographic model is shown in Fig 2. Steganography is a model consisting of mainly three components. Message component ‘M’ is secret data that the sender wishes to hide without any suspicion which a can be audio, video, image or text. “Message Wrapper” is second component i.e. the cover ‘C’ the original image, audio file, video file, in which the secret message ‘M’ is to be embedded. It is not necessary that the cover ‘C’ and the message ‘M’ should have homogeneous structure. For example, text message or an audio file can also be hidden into video or image. In this paper both the cover ‘C’ and Message ‘M’ are images [5].

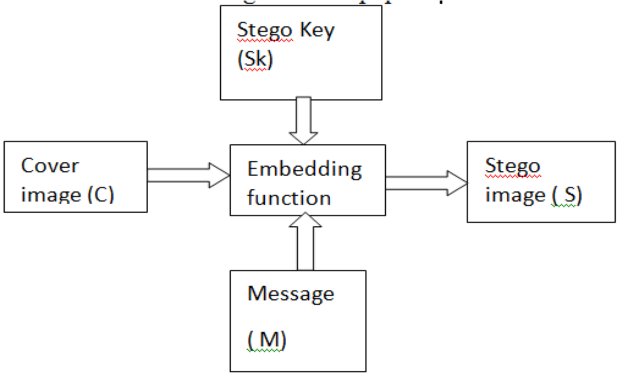


Fig. 2 Basic steganography model

Message ‘M’ is embedded in Stego – Image ‘S’ where ensuring about the stego-image should resemble the cover image. Stego-key is also provided to the receiver so that only receiver can be able to extract the secret image from the cover image [5].

Characteristics of Steganographic techniques:
In steganography, the message that is to be hidden inside the cover – media must consider the following features.

- *Hiding Capacity:* Hiding capacity means the size of the information that can be hidden inside the original image. More the hiding capacity more the size of the information can be hidden into original image [6].
- *Perceptual Transparency:* Perceptual transparency is an important feature of steganography. Each cover – media has certain information hiding capacity. If more information or data is hidden inside the cover, then it results in degradation of cover – media. As a result, the stego – media and cover – media appear to be different. This distortion should not be noticed by attackers [6].
- *Robust:* Robustness is the ability of the hidden message to remain undamaged even if the stego – media undergoes transformation, sharpening, linear & non-linear filtering, scaling & blurring, cropping and various other techniques [6].
- *Resistance:*It is an important property because, if an intruder is successful in destroying the steganographic technique then the Resistance property makes it difficult for the attacker to alter or damage the original data. This protects the integrity of the original work [6].

II. RELATED WORK

This paper analyses the various articles on steganography and its BPCS technology which help understand the topic in a new perspective.

In C.P.Sumathi [8], S.Singhet.al's[14] the authors present various techniques using which steganography methods can be implemented in an effective way. Various steganography methods such as Substitution methods, Transform domain techniques, Spread spectrum techniques, Statistical methods, Distortion techniques, Cover generation methods were discussed and various research work done in this field were discussed. The authors A.Cheddadet.al's [9] provide a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. Various methods of steganography in spatial medium and frequency medium are discussed in this paper. Rahna E et.al's [10] proposed an algorithm in which an array of locations of each possible character in English message in the image. Then for each character in the secret message we will search the array; the array index of the exact character is sent to the receiver. Receiver will then reverse the process so as to get the secret data. Proposed method is on lossless, infinite payload capacity, it has key size which is only about 10 to 20 percentage of the message size and has improved security. This paper main focus is to increase payload capacity of an image.

Piyush and Paresh [11] presented a technique that combines the features of cryptography, steganography along with multimedia data hiding. In order to provide higher security levels the algorithm uses a reference database. In this method, they first encrypted the message using DES. and then the cipher is saved in the image using a modified bit encoding technique. For each byte of data one cover pixel will be edited. S.Bhattacharyyaet.al's [12] provides a critical review of steganography as well as to analyze the characteristics of various cover media namely image, text, audio and video in respects of the fundamental concepts, the progress of steganographic methods and the development of the corresponding steganalysis schemes.S.G.K.D.N. Samaratunge[4] uses palette based images for steganographic method. S.Charleset.al's [13] used cryptography algorithm AES along with steganography's BPCS algorithm to embed large amount of data in image. AES algorithm provides a secure way to transfer secret data over internet. So this paper proposed a technique in which both security methods of cryptography and steganography are for transfer of data in more secure way. S.Khaire [6], V.J.Patel [15], F.Petitcolas [16], E.Kawaguchi [17], B.Ahujaet.al's [20] the authors in these papers proposed BPCS steganography technique which was introduced by Eiji Kawaguchi and Richard O. Eason. In traditional techniques such as Least Significant Bit (LSB) technique, transformation technique, perceptual masking technique, having limited data hiding capacity can hide up to 10 – 15 % of the vessel data amount. BPCS is to overcome the short coming of traditional steganography techniques by increasing data embedding capacity. BPCS technology can increase the hiding capacity of color image by 50%. This technique makes use of the characteristics of the human vision system whereby a human can't perceive any shape information in a very complicated binary pattern. M.S.Sutaone [19], C.Changet.al's [22] these authors proposed a LSB bit substitution technique of image. In the LSB method, the 8th bit of every byte of the carrier file is substituted by one bit of the secret information. This method works fine in the image carriers because if the least significant bit is changed from 0 to 1 or vice versa, there is hardly any change in the appearance of the color of that pixel. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted.

III. PROPOSED ALGORITHM

BPCS STEGANOGRAPHY:

BPCS steganography was introduced by Eiji Kawaguchi and Richard O in order to overcome the the shortcomings of the traditional Least Significant Bit (LSB) technique. This technique makes use of the characteristics of the human vision system whereby a human can't perceive any shape information in a very complicated binary pattern. First, the vessel image is divided into "informative region" and "noise-like region". Now replace the entire noise-like region" in the bit-planes of the vessel image with secret data without destroying the image quality. BPCS steganography is same like LSB technique but difference is LSB technique hide data in last four bits i.e. only in the 4 LSB bits and BPCS technique hide data in MSB plane along with the LSB planes, thereby providing more storage and embedding data. Some of the advantages of BPCS steganography are as follows:

1) Increased information hiding capacity
2) Canonical Gray Coded (CGC) bit planes are more are preferred for BPCS steganography compared to Pure Binary Coded (PBC) bit planes.
3) Physical presence of secret information visible by human eyes.

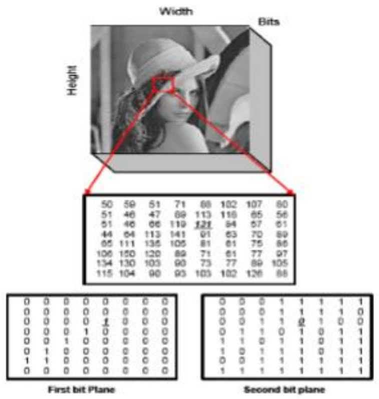
Basic Principle of BPCS Steganography:

In the first step of BPCS steganography the image is split into bit planes. Each bit plane is a binary image which contains the bit of each pixel where 'i' is the plane number. Slicing of planes are represented by a Pure Binary Coding system (PBC) and Canonical Gray Coding system (CGC). Each bit plane can be divided into "informative" and "noise" region. Noise-looking region consist complex pattern and replace each noise looking region with another noise-looking region without changing the overall image quality [23, 15].

The main goal of BPCS Steganography is to increase the capacity of image for data hiding without much distortion in the visual appearance of the original image. Pure Binary Coding (PBC) bit planes provides much greater region for embedding. But PBC suffers from "Hamming cliff", wherein a small change in color affects many bits of color value which can be overcome using CGC in BPCS system [6].The featuresof BPCS-Steganography are summarized as below.

A) Segmentation of each bit-plane of a color image into "Informative" and "Noise-like" regions.
B) Introduction of the B-W border based complexity measure (α) for region segmentation.
C) Introduction of the conjugation operation to convert simple secret blocks to complex blocks.
D) Using CGC image plane instead of PBC plane.

Bit Plane Slicing Concept in BPCS:



50	59	51	71	88	102	107	80
51	46	47	89	113	118	65	56
51	46	66	119	121	94	57	61
44	64	113	141	91	63	70	89
65	111	135	105	81	61	75	86
106	150	120	89	71	61	77	97
134	130	103	90	73	77	89	105
115	104	90	93	103	102	126	88

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0

0	0	0	1	1	1	1	1
0	0	0	1	1	1	1	0
0	0	1	1	0	1	0	0
0	1	1	0	1	0	1	1
1	1	0	1	1	0	1	1
1	0	1	1	1	0	1	1
0	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Fig 3: Bit Plane Slicing concept.

The bit plane slicing can be better understood with the help of Fig 3. The technique of splitting the image into its constituent binary planes is called “Bit plane slicing”. Pixels are digital numbers composed of bits. In an 8-bit image, intensity of each pixel is represented by 8-bits. The 8-bit image is composed of eight 1-bit plane regions from bit plane ‘0’ (LSB) to bit-plane ‘7’ (MSB). Plane ‘0’ contains all lowest order bits of all pixels in the image while plane ‘7’ contains all higher order bits. Bit plane Slicing is useful for image compression. Complexity of each bit–plane pattern increases from MSB to LSB [6].

BPCS Steganography Algorithm:

In BPCS steganography, uncompressed image file is used as carrier image. Each secret file to be embedded is segmented into a series of blocks having 8 bytes of data each which are called as secret blocks. The steps for encoding algorithm (i.e. to hide private information in carrier image) in BPCS-steganography:

The original image is divided into 24 different bit-planes. This division creates binary image for all 24-bits.

Steps of BPCS algorithm are as follows:

1) First transform all 24 bit-planes of carrier image from PBC to CGC system. Then all the bit-planes are divided into small pieces of the same size, which is called bit-plane blocks, such as bits.

2) Now segmentation of each bit-plane of the carrier image into “informative” and “noise-like” regions by using a threshold value $a_o$id done.

3) Now the secret file is divided into bytes which are grouped into series of blocks.

4) Embed each secret block into the noise-like regions of the bit-planes.

5) If a block (let say P) is less complex than the threshold (a_o), than conjugate it to make it a more complex block (P*). The conjugated block must be more complex than.

6) If the block is conjugated, then record this fact in a “conjugation map”. This Make a record of the blocks that have taken conjugate processing, and this information also need to be embedded into the carrier.

7) Also embed the conjugation map as was done with the secret blocks.

8) Convert the embedded carrier image from CGC to PBC.

The algorithm for decoding is reverse of embedding.

IV. CONCLUSION

The main part of this paper is to study techniques of steganography and BPCS-steganography algorithm. BPCS-steganography provides maximum hiding capacity of image. BPCS-steganography can be combined with different cryptographic algorithms to create more secure system. The embedded data will be more secure by using encryption technique.

REFERENCES

[1]. "Steganography." Wikipedia. Wikimedia Foundation, 20 Nov. 2012. http://en.wikipedia.org/wiki/Steganography.

[2]. N. F. Johnson, and S. Jajodia., “Steganography: Seeing the Unseen,” IEEE Computer, pp. 26-34, Feb. 1998.

[3]. Al-Mohammad A., “Steganography-based secret and reliable communications improving steganographic capacity and imperceptibility,” School of Information Systems, Computing and Mathematics, 2010.

[4] S.G.K.D.N. Samaratunge., “(August 2007): New Steganography Technique for Palette Based Images”, ICIISSecond International Conference on Industrial and Information Systems, 2007.

[5] Pranita P. Khairnar, V. S. Ubale.,” Steganography Using BPCS technology”, Research Inventy: International Journal Of Engineering And Science Vol.3, Issue 2., PP 08-16 Issn(e): 2278-4721,(May 2013),Issn(p):2319-6483, Www.Researchinventy.Com.

[6] Shrikant S. Khaire, Dr. Sanjay L. Nalbalwar.,”Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique”, International Journal of Engineering Science and Technology Vol. 2(9), 4860-4868, 2010.

[7] Smita P. Bansod, Vanita M. Mane, Leena R. Ragha., “Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity “,International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-202012, Mumbai, India.

[8] C.P.Sumathi, T.Santanam and G.Umamaheswari.,” A Study of Various Steganographic Techniques Used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[9] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt.,”Digital Image Steganography: Survey and Analysis of Current Methods “.

[10] Rahna E1, V.K Govindan.,” A novel technique for secure, lossless steganography with unlimited payload and without exchange of stegoimage” , International Journal of Advances in Engineering & Technology, July 2013. ©IJAET.

[11] P. Marwaha., “Visual cryptographic steganography in images," in Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on, pp. 1-6, IEEE, 2010

[12] Souvik Bhattacharyya, Indradip Banerjee and GautamSanyal.,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science,2 (4), pp.1-16, April 2011.

[13] Shiney Charles, ShrutiGajare, SnehalWagh, VrundaBhusari.," An Advance Tactic to Embed Large Encrypted Data in Encrypted Image Using AES and BPCS algorithm" , International Journal Of Scientific Research And Education ||Volume||2||Issue||9||Pages-1892-1898||September-2014|| ISSN (e): 2321-7545 Website: http://ijsae.in.

[14] Sandeep Singh, Aman Singh.,"A Review on the Various Recent Steganography Techniques", IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013 ISSN ,www.IJCSN.org

[15] Vipul J Patel, Ms. Neha RipalSoni.,"Uncompressed Image Steganography using BPCS: Survey and Analysis", OSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 4, PP 57-64, (Nov. - Dec. 2013) www.iosrjournals.org

[16] Ross J. Anderson, Fabien A.P. Petitcolas.," On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, Special Issue on Copyright & Privacy Protection. ISSN 0733-8716, May 1998..

[17] Eiji Kawaguchi, Richard O. Eason. ."Principle and applications of BPCS-Steganography",Kyushu Institute of Technology, Kitakyushu, Japan – University of Maine, Orono, Maine.

[18] Behroz A. Forouzan., "Cryptography & Network Security", McGraw Hill Publication,2008, New Delhi.

[19] M. S. Sutaone, M.V. Khandare, "Image Based Steganography Using LSB Insertion Technique", Wireless, Mobile and Multimedia Networks, IET International Conference, pp-146 – 151, Jan-2008.

[20] Babita Ahuja and Manpreet Kaur, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[21] Hassan Mathkour, Batool Al-Sadoon, AmeurTouir, "A New Image Steganography Technique", Wireless Communications, Networking and Mobile Computing, 4th International Conference, IEEE,pp-1-4, 2008 .

[22]Chin-Chen Chang, Hsien-Wen Tseng, "Data Hiding in Images by Hybrid LSB Substitution", Third International Conference on Multimedia and Ubiquitous Engineering, pp- 360 – 363, 2009.

[23] Hideki Noda MichiharuNiimi and EijiKawguchi. "A steganography based on region segmentation by using complexity measure." Trans. of IEICE, J81-D-II, pp.1132-1140, 1998.