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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Review on Improving Data Security Using BPCS Steganography

Surabhi Agrawal

Assistant Professor, Dept. of Computer Science & Engineering, Subharti Institute of Technology & Engg , Meerut, UP, India

ABSTRACT: Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. We can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. We termed our Steganography "BPCS-Steganography," which stands for Bit-Plane Complexity Segmentation Steganography. This study focuses on basic Steganography and various characteristics necessary for data hiding. More importantly, the paper implements a Steganography technique that has hiding capacity. This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. The main principle of BPCS technique is that, the binary image is divided into informative region and noise-like region. The secret data is hidden into noise-like region of the vessel image without any deterioration.

KEYWORDS: Steganography, Discrete Cosine Transform(DCT), LSB(Least Significant Bit).

I. INTRODUCTION

Steganography, from the Greek, means covered, or secret writing, and is a long-practised form of hiding information. Although related to cryptography, they are not the same. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

More precisely,the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present.Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. A message is embedded in a cover media in an invisible manner so that one could not suspect about its existence.

In this thesis we present a substitution based information protection method where we combine cryptographic, steganographic and signal processing concepts together for achieving security. The method is known as **Steganography Based Information Protection method.** In this method we substitute the information bit in randomly selected pixels at random places within LSB region.

II. STEGANOGRAPHY METHODS

According to modification in covers, the methods can be categorized as

- Substitution
- Transform domain
- Spread spectrum
- Statistical
- Distortion
- Cover generation

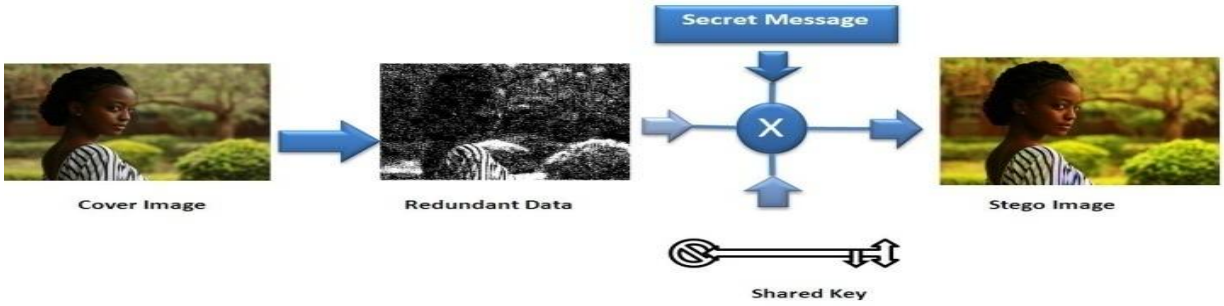
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016



III. SUBSTITUTION METHOD

It is commonly used simple method in which we can put information bits in LSB sequentially at fixed place, randomly at fixed place or randomly at random places in cover pixels. The message to be protected passes through scanning, coding, encryption process to form an embedded message.

Scanning, coding, encryption steps make the information unintelligible so that one cannot extract plain message.
Embedding make the message invisible so that one cannot detect it.
Reshaping spreads the message so that embedded message can be detected from distorted steganos by authorized receivers.
Cover processing makes detection of embedded message more difficult since the distortion is either due to noise addition or due to message embedding.
This would increase the robustness and security. Many attacks on such steganographic systems are suggested.

Some attacks that can be applied are given below:

i. Stego-Only Attack
ii. Message-Stego Attack
iii. Cover-Stego Attack
iv. Message-Cover-Stego Attack

Difference Analysis
The “difference-images” obtained by taking the difference between cover, processed cover and stego images are not visible. For making the difference visible in “difference-images” for visual interpretation, we first increase differences by multiplication of weight factor and then revert the values to get the strengthened “difference-images”.From analysis of these “difference-images “, on could not say that the changes are either due to cover processing or message embedding and hence we can say that the method is safe from known cover-stego attack.

Distortion Analysis
Distortion analysis of stego images is carried out by studying distortion / similarity messages statistically. There are many methods for measuring distortion that can be used for distortion analysis. Distortion between two different images is measured by considering Mean Square Error (MSE), Mean Absolute Error (MAE) or Histogram Similarity (HS).

Depth Vs Distortion Analysis
Distortion occurred in different steganos is required by varying the depth of hiding for embedding information in cover image. The relation between depth of hiding used and distortion occurred in the stego images is shown in Fig. that depth of hiding within some LSB region is most suitable for message embedding as the distortion is very small in this region. As the depth of hiding increases beyond preferable region, the distortion becomes noticeable and unsuitable for message hiding.

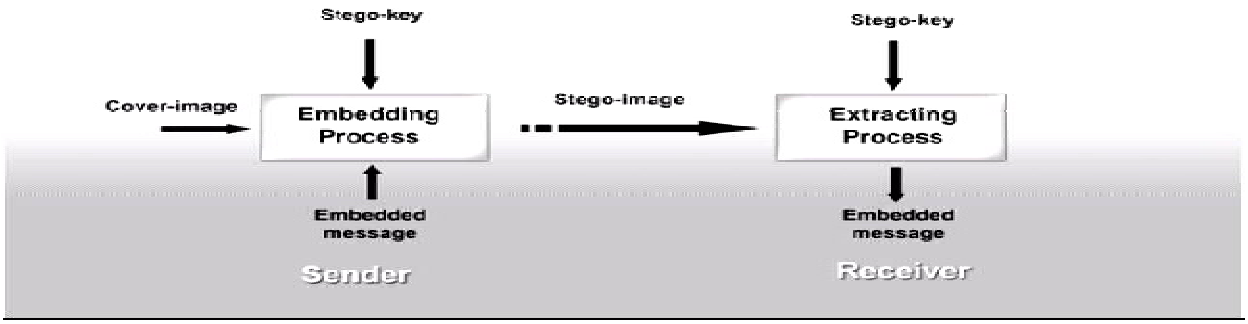
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016



IV. IMAGE ST EGANOGRAPHY TECHNIQUES

i. Least significant bit insertion (LSB)
ii.Masking and filtering
iii.Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.
Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.

V. METHODOLOGY

In Proposed methods, The main purpose of this research is to improve the quality of image to hide the secret images in a vessel image using bit plane complexity segmentation to the integer wavelet transformed images. This technique will mainly concentrate on the increase data hiding capacity by keeping the imperceptibility of the hidden data and also the vessel image should have less distortion, that means the original image and the image after embedding the data should be almost the same.
•In Steganography, data is hidden inside a vessel or container that looks like it contains only something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files.
•All of the traditional steganographic techniques have limited information-hiding capacity. They can hide only 10% (or less) of the data amounts of the vessel.
•This Technique uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel.
•We can replace all of the “noise-like” regions in the bit-planes of the vessel image with secret data without deteriorating the image quality
•We termed our Steganography “BPCS-Steganography,” which stands for Bit-Plane Complexity Segmentation Steganography

The framework of proposed **Steganography Based Information Protection method** is shown in Fig . Its description

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

International Journal of Innovative Research in Computer and Communication Engineering

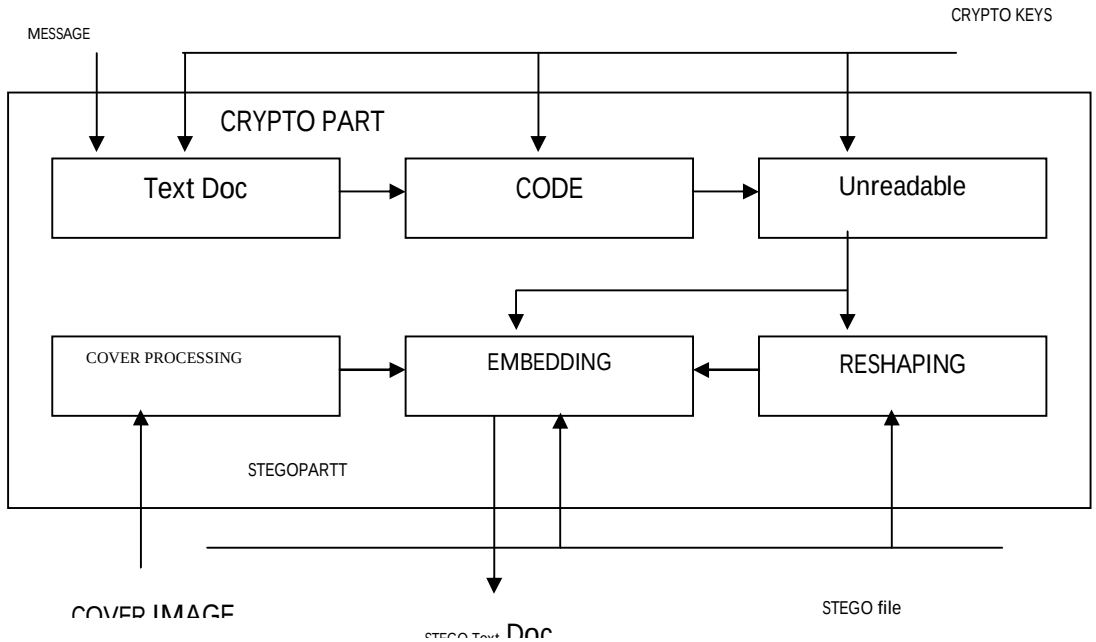
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

is presented in the following steps**.**

For any steganography based secure system, the perception of steganos should be as cover image itself so that one cannot differentiate them and detect the existence of embedded message.



Work Flow Diagram

Modules Types

1. BPCS Technique
2. Data embedding Technique
3. Bit Plane slicing Technique

BPCS TECHNIQUES

In this algorithm, BPCS-Steganography (Bit-Plane Complexity Segmentation Steganography) is a type of digital Steganography. Digital Steganography can hide confidential data (i.e., secret files) very securely by embedding them into some media data called "vessel data." The vessel data is also referred to as "carrier, cover, or dummy data". In BPCS-Steganography true color images (i.e., 24-bit color images) are mostly used for vessel data. The embedding operation in practice is to replace the "complex areas" on the bit planes of the vessel image with the confidential data.

DATA EMBEDDING TECHNIQUE

In this module, the most important aspect of BPCS-Steganography is that the embedding capacity is very large. It can embed confidential information in vessel data which is typically a true color image (24-bit BMP format) and sometimes in an 8-bit indexed color image.

Embedding (actually, replacing) is made on the bit-planes of the image. The most important feature of this Steganography is that its embedding capacity is very large.

BIT PLANE SLICING TECHNIQUE

In this module, the operation of splitting the image into its constituent binary planes is called “Bit plane slicing”. Pixels are digital numbers composed of bits.Bit plane Slicing is useful for image compression. Complexity of each bit plane pattern increases monotically from MSB to LSB.Given an X-bit per pixel image, slicing the image at different planes (bit-planes) plays an important role in image processing. An application of this technique is data compression. In general, 8-bit per pixel images are processed. We can slice an image into the following bit-planes. Zero is the least

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

significant bit (LSB) and 7 is the most significant bit (MSB) .In our method we call a carrier image a "vessel" or "dummy" image. It is a color image in BMP file format, which hides (or, embeds) the secret information (files in any format).

We segment each secret file to be embedded into a series of blocks having 8 bytes of data each. These blocks are regarded as 8 × 8 image patterns. We call such blocks the secret blocks. We embed these secret blocks into the vessel image using the following steps.

1. Transform the dummy image from PBC to CGC system.
2. Segment each bit-plane of the dummy image into informative and noise-like regions by using a threshold value (α0). A typical value is α0 = 0.3.
3. Group the bytes of the secret file into a series of secret blocks.
4. If a block (S) is less complex than the threshold (α0), then conjugate it to make it a more complex block (S*). The conjugated block must be more complex than α0 as shown by equation (6).
5. Embed each secret block into the noise-like regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks). If the block is conjugated, then record this fact in a "conjugation map."
6. Also embed the conjugation map as was done with the secret blocks.
7. Convert the embedded dummy image from CGC back to PBC.

The Decoding algorithm (i.e., the extracting operation of the secret information from an embedded dummy image) is just the reverse procedure of the embedding steps.

The novelty in BPCS-Steganography is itemized in the following.

A) Segmentation of each bit-plane of a color image into "Informative" and "Noise-like" regions.
B) Introduction of the B-W boarder 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

P is interpreted as follows. Pixels in the foreground area have the B pattern, while pixels in the background area have the W pattern. Now we define P* as the conjugate of P which satisfies:

The foreground area shape is the same as P.
The foreground area has the Bc pattern.
The background area has the Wc pattern.
Correspondence between P and P* is one-to-one, onto. The following properties hold true and are easily proved for such conjugation operation. "⊕ " designates the exclusive OR operation.

A) $P^* = P \oplus Wc$ …….(1)
B) $(P^*)^* = P$ …….(2)
C) $P^* \neq P$ …….(3)

The most important property about conjugation is the following. D) Let α (P) be the complexity of a given image P, then we have,

$$\alpha(P^*) = 1 - \alpha(P).$$

It is evident that the combination of each local conjugation (e.g., 8 × 8 area) makes an overall conjugation (e.g., 512 × 512 area).

(6) says that every binary image pattern P has its counterpart P*. The complexity value of P* is always symmetrical against P regarding α = 0.5. For example, if P has a complexity of 0.7, then P* has a complexity of 0.3.

VI. CONCLUSION

Several methods for hiding data in, images were described, with appropriate introductions to the environments of each medium, as well as the strengths and weaknesses of each method. The key algorithm for designing the steganography system has been dealt. Most data-hiding systems take advantage of human perceptual weaknesses, but have weaknesses of their own. We conclude that for now, it seems that no system of data-hiding is totally immune to attack .) We can categorize the bit-planes of a natural image as informative areas and noise-like areas by the complexity thresholding.
(1) Humans see informative information only in a very simple binary pattern.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

(2) We can replace complex regions with secret information in the bit-planes of a natural image without changing the image quality. This leads to our BPCS-Steganography.
(3) Gray coding provides a better means of identifying which regions of the higher bit planes can be embedded.
(4) A BPCS-Steganography program can be customized for each user. Thus it guarantees secret Internet communication. We are very convinced that this steganography is a very strong information security technique, especially when combined with encrypted embedded dat**a.**

REFERENCES

1. *M.Kuhn. Steganography mailing list. WWW: http://www.jjtc.com/Steganography/steglist.htm, 1995. Private Site, Hamburg, Germany*
2. *N.F. Johnson. Steganography. WWW: http://www.jjtc.com/stegdoc/. George Mason University*
3. *C. Kurak and J. McHugh. A cautionary note on image downgrading. In Proceedings of the 8th Annual Computer Security Applications Conference, pages 153-159, 1992.*
4. *W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. In IBM Systems Journal, Vol. 35, Nos. 3-4, pages 313-336, February 1996.*
5. *Ã, A. C., Condell, J., Curran, K., & Kevitt, P. M. (2010). Digital image steganography : Survey and analysis of current methods. Signal Processing, 90(3), 727–752. doi:10.1016/j.sigpro.2009.08.01*
6. K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik,*"Authentication of Secret Information in Image Steganography"* Microprocessor Applications Laboratory, Indian Institute of Science,Bangalore
7. Proceedings of the 2006 International Conference on "*Intelligent Information Hiding and Multimedia Signal Processing* "(IIH-MSP'06)0-7695-2745-0/06
© 2006 IEEE.
8. Asghar Shahrzad Khashandarag and Naser Ebrahimian, "*A new method for color image steganography using SPIHT and DCT, sending with JPEG format*", International Conference on Computer Technology and Development, IEEE, 2008
9. CHEN Zhi-li, HUANG Liu-sheng, YU Zhen- shan, LI Ling-jun and YANG wei, "*A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words*", 3RD International Conference on Availability, Reliability and Security, IEEE, 2008..
10. K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" Microprocessor Applications Laboratory, Indian Institute of Science, Bangalore in 2008
11. Mamta Juneja Parvinder Singh Sandhu, "*Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption*"2009 International Conference on Advances in Recent Technologies in Communication and Computing.
12.]KokSheik Wong, Xiaojun Qi, and Kiyoshi Tanaka, ―A DCT based Mod4 Steganography Method‖ Signal Processing 87, 1251-1263, 2009.

BIOGRAPHY

Surabhi Agrawal is Assistant professor in the Computer Science & Engineering Department, Subharti Institute of Technology & Engineering , Meerut , U.P. India. She received Master of Technology degree in 2015 from SVSU,Meerut, , India. Her research interests are Computer Networks , Data Security and Image Processing etc.