Research Inventy: International Journal Of Engineering And Science
Vol.3, Issue 2 (May 2013), PP 08-16
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Steganography Using BPCS technology

[1]Pranita P. Khairnar, [2]Prof. V. S. Ubale
[1]Electronics Department,[2]Asst. Prof. Electronics Department,
Amrutvahini College of Engineering, Sangamner

ABSTRACT: *Steganography is the art of hiding information in ways that prevent detection. Steganography is a technique to hide secret information in some other data (we call it a vessel) without leaving any apparent evidence of data alteration. All of the traditional steganographic techniques have limited information-hiding capacity. They can hide only 10 to 15 % of the data amounts of the vessel. This is because the principle of those techniques was either to replace a special part of the frequency components of the vessel image, or to replace all the least significant bits of a multivalued image with the secret information.*

New steganography uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel.

This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. 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.We have discussed here two techniques, 1.Web based BPCS, 2.Improved BPCS.

Key Words: *Stegnography, BPSC, Web based BPCS, Improved BPCS.*

I. OVERVIEW OF STEGANOGRAPHY

Data embedding or data hiding is a technique that enables us to secretly embed extra data into a file such as an image file, a movie file, and an audio file. The embedded data disappear into the file and we cannot recognize the embedded data in the file. We will neither find any header data or comments added to the file. The embedded data, however, do exist in the file, and we can extract it from the file.

Steganography literally means covered writing and is the art of hiding secrete messages within another seemingly innocuous message or carrier. The carrier could be any medium used to convey any information, including wood or slate tables, tiny photographs or word arrangements. With the advent of digital technology, the list of carriers has been made to include e-mails, audio and video, disk spaces and partitions and images.

There are two major branches of information hiding, **Steganography** and **Watermarking**

Watermarking:

- Communication in watermarking is the host signal, with the embedded data providing copyright protection.
- The existence of a watermark is often declared openly.
- Any attempt to remove or invalidate the embedded content renders the host useless.

Cryptography:

- Doesn't conceal the communication.
- Scrambles the data to prevent eavesdroppers understanding the content.
- Cryptography involves various methods and implementations.
- May be considered complementary and orthogonal (unrelated).[7]

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.[1] Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.[1]

Applications

1., Usage in modern printers

Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

2.Use by terrorists

When one considers that messages could be encrypted steganographically in e-mail messages, particularly e-mail spam, the notion of junk e-mail takes on a whole new light. Coupled with the "chaffing and winnowing" technique, a sender could get messages out and cover their tracks all at once.[1]

3.Other applications

- To have secure secret communications where cryptographic encryption methods are not available.
- To have secure secret communication where strong cryptography is impossible.
- In some cases, for example in military applications, even the knowledge that two parties communicate can be of large importance.
- The health care, and especially medical imaging systems, may very much benefit from information hiding techniques.

II. BASIC STEGANOGRAPHY MODEL

A basic steganographic model is shown in Figure 1. The message 'M' is the secret data that the Sender wishes to hide without any suspicion. The secret data can be audio, video, image, text. The cover 'X' is the original image, audio file, video file, in which the secret message 'M' is to be embedded. The cover 'X' is also called as "Message Wrapper". It is not necessary that the cover 'X' 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 'X' and Message 'M' are images.

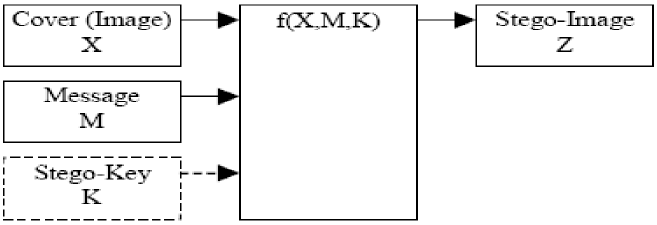


Figure 1: Basic digital Steganography Encoder

Stego – Image 'Z' is basically the image in which the secret image 'M' is embedded. It should be ensured that at any point, the stego-image should resemble the cover image else it will cause suspicion. Stego-key 'Z' is provided to the receiver so that only he can be able to extract the secret image from the cover image[2-8]

Characteristics of Strong Steganography

Though steganography's most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength. These include capacity (how much data can be hidden), invisibility (inability for humans to detect a distortion in the stego-object), undetectability (inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects), robustness (message's ability to persist despite compression or other common modifications), tamper resistance (message's ability to persist despite active measures to destroy it), and signal to noise ratio (how much data is encoded versus how much unrelated data is encoded). The three main components, which work in opposition to one another, are capacity, undetectability, and robustness. Increasing one of these causes the others to decrease; thus, no steganographic technique can be perfectly undetectable and robust and have maximum capacity. In most cases, capacity is not as important as the other two, and whereas watermarking favors robustness most strongly, general steganography considers undetectability the most important. A summary of the properties of good steganography is presented in figure 2 below.[5]

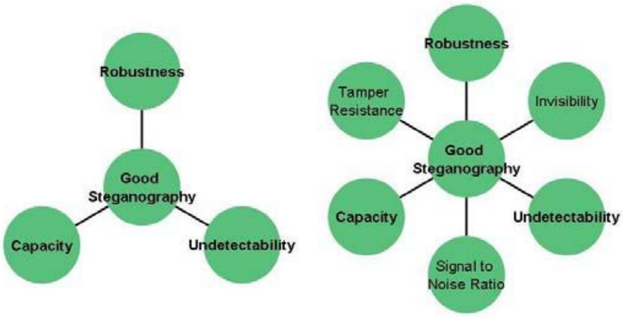


Figure 2.Properties of Good Steganography: the three most simple opposed properties (left) and a display of all six key properties (right)[5]

III. BPCS

Data embedding Technique – BPCS (Bit Plane Complexity Segmentation) steganography:

Introduction

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason, to overcome the short comings of traditional steganographic techniques such as Least Significant Bit (LSB) technique, Transform embedding technique, Perceptual masking technique.

Previously steganographic techniques have limited information-hiding capacity.50–60% Data can be hidden after implementation of this paper . This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. BPCS steganography makes use of important characteristic that of human vision. In BPCS, the vessel image is divided into "informative region" and "noise-like region" and the secret data is hidden in noise blocks of vessel image without degrading image quality. In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits. But in BPCS technique, data is hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region.[2-9]

The merits of BPCS-Steganography are as follows.

1) The information hiding capacity of a true color image is around 50%.
2) A sharpening operation on the dummy image increases the embedding capacity quite a bit.
3) Randomization of the secret data by a compression operation makes the embedded data more intangible.
4) Customization of a BPCS - Steganography program for each user is easy. It further protects against eavesdropping on the embedded information
5) It is most secured technique and provides high security.[4]

Hiding and Extracting Data

We start off by converting a sample 8-bit grayscale image into CGC (Canonical Gray Coding) form. CGC allows us to manipulate each bit plane without affecting the other bits that represent each grayscale value. 8x8 pixel blocks are segmented within the image and each of the bits (8 bits per pixel) in CGC form will have their own corresponding 8x8 plane. Visually, this would be like slicing the 8x8 planes into 8 8x8 black and white bit planes (*see CGC diagram*). Each bit plane will be measured for complexity, which is determined by the number of borders (transitions between black and white in each pixel plane) present in an 8x8 bit plane versus the maximum borders possible. If a region is complex enough, we will embed our data into the cover image, which is broken up into appropriately sized 8x8 blocks for each bit plane.

If the data to embed (8x8 blocks at a time) in the cover file is statistically complex, it can be embedded into the complex blocks of the image. If not, we will conjugate (exclusive or) the data with a checkerboard pattern (the most complex pattern possible) to ensure complexity. There will be a conjugation bit in each plane that will show whether the data was conjugated with a checkerboard pattern. This technically gets rid of 1 bit of embedding capacity per 8x8 region giving 63 bits to embed per 8x8 bit plane.

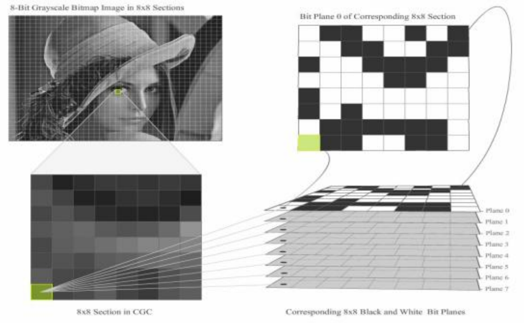
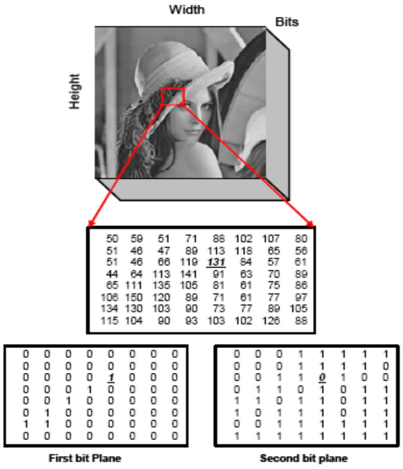

8-Bit Grayscale Bitmap Image in 8x8 Sections
Bit Plane 0 of Corresponding 8x8 Section
Plane 0
Plane 1
Plane 2
Plane 3
Plane 4
Plane 5
Plane 6
Plane 7
8x8 Section in CGC
Corresponding 8x8 Black and White Bit Planes

Figure 3.CGC Diagram

Once the data has been embedded, the image is converted back into the original format from CGC and saved. Extraction is basically the same as embedding, except if a bit plane is determined to be complex, it will then look at the conjugation bit and extract the data accordingly. Because the embedded data in the complex regions has to be complex, the complex regions before and after embedding data will remain complex. Color is basically the same process. However, it will have 3 8-bit grayscale values that represent each color, thus giving approximately three times the file size and three times the embedding capacity (to its corresponding grayscale version). A subtle other difference is that the color file has a slightly different file structure that does not contain a palette for the pixel values.[3]

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	***131***	84	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

First bit Plane

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

Second bit plane

Ex. 131(10)=10000011(2)

Figure 4: Bit Plane Slicing concept considering pixel having value 131.

The bit plane slicing can be better understood with the help of figure 4[2-10]. The operation 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 monotically from MSB to LSB[2-11]

IV. WEB BASED BPCS STEGANOGRAPHY

This system integrates web applications, web services, client-server applications, application servers, and applications on the local client into a desktop environment using the desktop metaphor. The user can access functionality of Steganography services through client console.[4]

Objectives:
1) To provide the better data security.
2) Prevent form hacking.

1. Algorithm

1) Convert the carrier image(of any file format) from PBC to CGC system and in png format.
2) Perform the histogram analysis.
3) After that bit-plane analysis is performed.
4) Perform size-estimation i.e. calcalate the places where we can store the secrete image.
5) Perform bit plane complexity segmentation on image i.e. embed secrete blocks into carrier image.
6) After embeding mail that image to another user.
7) For extracting the embedded image perform de-steganography which is exactly opposite to steganography.[4]

2.System Architecture

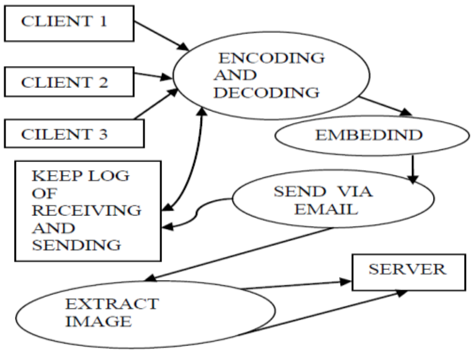


Fig.5 Data Flow diagram.[4]

The data flow diagram for this paper is as shown in fig 5.This paper implements a client server application where number of clients can work at a time. Along with the BPCS steganography they can they can perform various functions such as

A. File conversion
B. Histogram.
C. Size estimation.
D. Bpcs steganography.
E. Mailing.
F. De-steganography.

A. File conversion:

a. Portable Network Graphics - PNG

The PNG compression algorithm is one of the best that can be found. Unlike standard JPEG images, PNG compression involves no loss of image data, so there is no smudging or blurring.Nearly all the latest browsers support PNG's variable transparency, including WebTV and Microsoft Internet Explorer for Macs PNG format allows all kinds of extra information to be stored inside image files. The two most potentially helpful features for web images are gamma correction and embedded text.

Portable Network Graphics format was originally devised at a time when there was no browser support for GIF animation, so animation was not included in the specification.

B. Histogram:

Histograms are functions describing information extracted form the image.The histogram function is defined over all possible intensity levels. For each intensity level, its value is equal to the number of the pixels with that intensity.

Fig. 6 Original image[4-12]

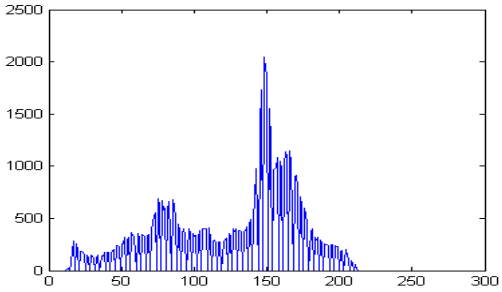


Figure 7. Graph of the histogram function[4-12]

C. Size estimation:

In size estimation we have to calculate the regions where maximum color variations are observed. After doing this we have to store pixel value of secret image at that variation regions.While doing so we use the concept of embading capacity. For a given image, embedding capacity can be traded with image quality by altering the complexity threshold. If image used has a threshold of 24 border pixels per 8 × 8 region; so regions having more border pixels than this were eligible for embedding.[4-13]

D. BPCS Steganography:

Here the actual steganography is performed. In our method we call a carrier image a “carrier” . 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) Convert the carrier image from PBC to CGC system i.e. convert file from any format into png format.
2) Segmentation on carrier image is performed i.e. each bit-plane of the carrier image into informative and noise-like regions by using a threshold value (α0).That means complexity of image is calculated.
3) Group the bytes of the secret file into a series of secret blocks.
4) If a block is less complex than the threshold (α0), then conjugate it to make it a more complex block .
5) The conjugated block must be more complex than α0.
6) Embed each secret block into the complex regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks) where maximum color changes are observed.
7) Convert the embedded dummy image from CGC back to PBC.[4-14]

E.Mailing:

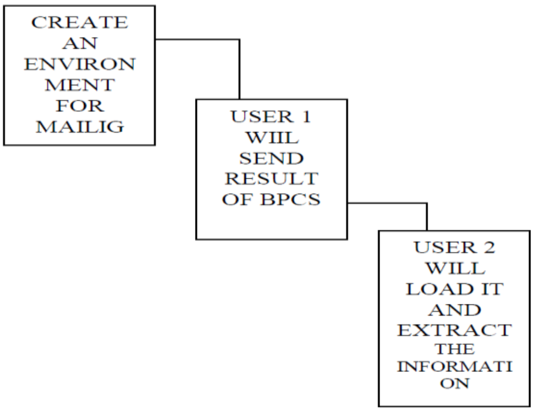

CREATE AN ENVIRON MENT FOR MAILIG
USER 1 WIIL SEND RESULT OF BPCS
USER 2 WILL LOAD IT AND EXTRACT THE INFORMATI ON

Figure 8. Mailing. [4]

In mailing we create an environment just like yahoo or rediff and send r image from one user to other.After receving the image form user one user two loades that image and extract the hidden data from it by performing de-steganography.

F. De-steganography:

De-steganography is exactly opposite of steganography.Here we will extract secret image from vessel image.In this way we will get the secret image form hiding it from the third person.[4-14]

V. IMPROVED BPCS STEGANOGRAPHY

The improved bit-plane complexity segmentation (BPCS) steganography carries on different processing’s to different bit-planes, with setting high threshold value at the high bit-plane and low threshold value at the low.[6]

1.The Conversion Of Text Information

The meaningful text messages need to be translated into encrypted binary data stream. The data stream is used for the embedding of carrier image, which makes preparations for the steganography. The conversion is shown as Fig. 9.

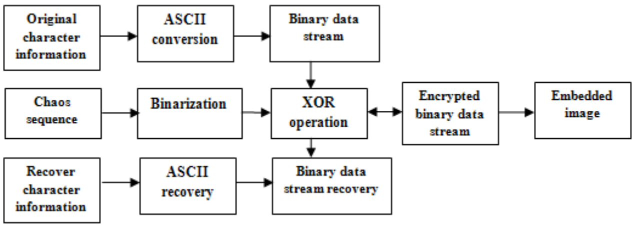

Original character information
ASCII conversion
Binary data stream
Chaos sequence
Binarization
XOR operation
Encrypted binary data stream
Embedded image
Recover character information
ASCII recovery
Binary data stream recovery

Figure 9: Conversion of text information[6]

2. RSA Algorithm

The RSA algorithm, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman, is currently one of the favorite public key encryption methods. RSA algorithm [6-15] is applied for the encryption of text information which is secure against a man-in-the-middle attack. It is very simply to multiply numbers together, especially with computers. But it can be very difficult to factor numbers. Steps involved in RSA algorithm:

A. Key generation:

1. Choose two distinct prime numbers p and q.

2. Compute $n = pq$.

3. Compute $\varphi(pq) = (p - 1)(q - 1)$. ($\varphi$ is Euler's totient function).

4. Choose an integer e such that $1 < e < \varphi(pq)$, and e and $\varphi(pq)$ share no divisors other than 1 (i.e., e and $\varphi(pq)$ are coprime).

- e is released as the public key exponent.

5. Determine d (using modular arithmetic) which satisfies the congruence relation

$$de \equiv 1 \pmod{\varphi(pq)}$$

- d is kept as the private key exponent.

The public key consists of the modulus and the public (or encryption) exponent. The private key consists of the private (or decryption) exponent which must be kept secret.

B. Encryption:

c = me mod n

Where m is an integer 0<m<n

C. Decryption:

m = cd mod n

3. CHAOS Theory

Chaos is a kind of behavior about nonlinear dynamics law control. This adopts Logistic mapping method to generate chaotic sequence:

αk+1=µ.ak. (1-αk), k=0, 1, 2…..

The value traverses in the interval [0, 1], and µ is a control parameter or a bifurcation parameter. When 3.5699456_.<µ<=4, the logistic map works in chaotic state. The data stream gene- rated is disordered, and it's similar to random noise.

The new binary sequence, which is the binarization of acquired chaotic sequence, has two main functions in this paper.

1. It is used to the encryption of text data information, steganography.

2. It is used to stimulate the binary data stream, which can facilitate the process of various experiments.[6]

4. Improved BPCS steganography

The original BPCS algorithm divides the carrier image into serious bit-planes, and there is high correlation between the bitplanes. The higher the bit-plane is, the stronger the correlation between the pixels of the bit-planes is [16]. So setting the same embedding strength for different bit-planes is sure to have an influence on the correlation between the bit-planes, leading to abnormalities of the complexity histogram, consequently, the security of steganography will be affect. Through detecting the complexity histogram, the analyst can analysis the existence of secret information, besides, he can estimate the embedding threshold value accurately. In order to resist this statistical analysis method, this paper improves the BPCS algorithm. The correlation of adjacent pixels is relatively strong when the bit-plane is high, and we can see the sketchy outline of the image.

There is a certain degree of regularity among these pixels. Yet, the dates of the lower bit-planes are similar to random noise. Therefore, we shall make better use of HVS (human vision system) characteristic and consider the local characteristic of the image when embedding secret information, and treat different bit-planes with different way, with setting greater threshold for the higher bit-planes and smaller for the lower ones. Trough different bit-planes using different embedding strength, not only does this scheme resist statistical analysis, but also it can realize that embedding less secret information in higher bit-planes to have good visual imperceptibility and embedding more in lower bit-planes to have high data embedding capacity, solving the problem that keeps the balance on the contradiction between embedding capacity and visual imperceptibility. Different bit-planes make different contributions to carrier image, this design sets greater threshold for the higher bit planes and smaller for the lower ones.[6-16]

5. Design and Implement

The technique of improved steganography text based on Chaos, RSA and BPCS designs as Figure 10.

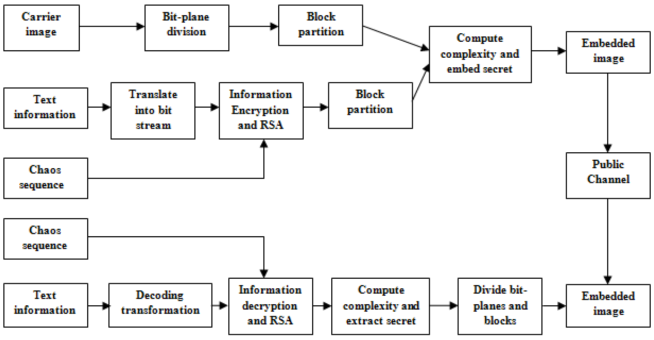


Figure 10: The technique of improved steganography text based on chaos, RSA and BPCS[6]

6. Analysis

Select standard 24-bit "pepper" image

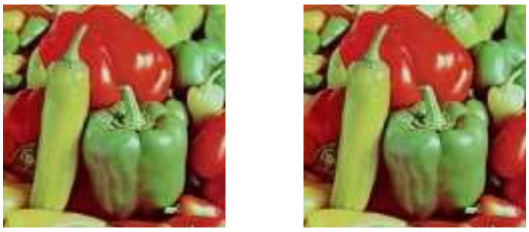


Figure 11: The image "pepper" before and after steganography[6]

Histogram measure:

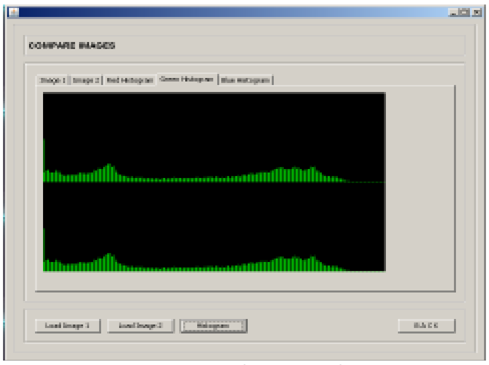


Figure 12.Green histogram before and after steganography[6]

The histogram can be seen with any colour Red Green or Blue.We have shown green histogram and it can be seen that, there is no obvious difference in histograms before and after steganography. Then the design has high security.

VI. CONCLUSION

The objective of this paper was to demonstrate BPCS-Steganography, which is based on a property of the human visual system. The most important point for this technique is that humans can not see any information in the bit-planes of a color image if it is very complex.

We have specified the two techniques of BPCS one is web based BPCS and another is Improved BPCS technology.

Web Based technology guarantees secret Internet communication. This steganography is a very strong information security technique, especially when combined with encrypted embedded data.

The technique of improved steganography text based on chaos and BPCS apply to text secret information, the design has good visual imperceptibility and high data embedding capacity, and furthermore, it has a great advantage in resisting the analysis of the steganalysis. By introducing chaos theory and RSA algorithm, it is convenient to test the performance of steganography, and the design has higher security and reliability.

REFERNCES

[1] http://en.wikipedia.org/wiki/Steganography

[2] IEEE paper on **Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique** IJEST Vol. 2(9), 2010

[3] **BPCS Steganography -Steve Beaullieu, Jon Crissey, Ian Smith**

[4] IEEE paper on Web Based BPCS Steganography- IJCTEE VOLUME2ISSUE2

[5] http://www.cse.wustl.edu/~jain/cse571- 09/ftp/stegano/index.html

[6] IEEE paper on **High Capacity Data Embedding Technique Using Improved BPCS Steganography-** ijsrp research_paper_jul2012/

[7] Ppt on steganography by Khan, Mohammed Minhajuddin [8] E. T. Lin and E. J. Delp: A Review of Data Hiding in Digital Images, Video and Image Processing Laboratory, Indiana.

[9] Eiji Kawaguchi, Richard O. Eason: Principle and applications of BPCS – Steganography.

[10] ENEE408G Multimedia Signal Processing (fall '03) – Overview of MATLAB Programming.

[11]] Rafael C. Gonzalez, Richard E. Woods: Digital Image Processing, Third Edition, Pearson Education, pp. 117 – 119.

[12] ASAM - Image Processing 2008/2009. Lecture 5

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

[14] A.Habes, (Feb 2006): Information Hiding in BMP image Implementation, Analysis and Evaluation, Information Transmission in Computer Networks.

[15] Rivest, R.; A. Shamir; Adleman (1978). "A Method for Obtaining Digital Signature and Public-key Cryptosystems"(http://theory.lcs.mit.edu/~rivest/rsapaper.pdf). Communication of the ACM21:120-126.

[16] Wu J, Zhang R eta. Reliable Detection of BPCS Steganography [J].Journal of Beijing University of Posts and Telecommunications, 2009,32(4): 113-121

AUTHOR PROFILE

Ms. Pranita P. Khairnar,

Has completed her B.E (Electronics) & currently appear to M.E (Electronics) at Amrutvahini College of Engineering, Sangamner. Dist. - Ahmednagar, Maharashtra, India.

Prof. V. S. Ubale,

Has completed his M.E.(Electronics) & B.E. (E& TC). He is working as a Assistant Professor in Electronics Department, Amrutvahini College Of Engineering, Sangamner, Dist. Ahmednagar, Maharashtra, India. Prof Ubale has teaching experience of 11 years to Undergraduate, Graduate & Post Graduate Students. Prof V. S Ubale has Published 03 papers in International Journal,& presented 04 papers in International Conference & 03 papers in National Conferences