High Capacity Data Hiding Using BPCS Steganography

Akshay Gohil, Amey Ambre, Nimit Makwana, Santoor Rawle

Prof. Rajashree Gadhave

Department of Information Technology
Atharva College of Engineering, Malad (W), Mumbai-400095
akshayggohil@yahoo.co.in, ambre.amey19@gmail.com, nimitmakwana@yahoo.co.in, santoorslove.333@gmail.com

Abstract— **Steganography is the art of hiding the fact that communication is taking place, by hiding (Embedding) message or file in other file. Steganography derives from the Greek word *"Steganos"* meaning covered and *"Graphos"* meaning writing or drawing. *Steganography is the science and art of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message.* Steganography is to select an appropriate carrier file such as an image, video or audio file, removing the less important information from that file and injecting the hidden message in its place. When the secret message and the cover message are combined a stego image is created. Due to recent advancements, everything is trending towards digitization. And by the development of World Wide Web (WWW), Digital media has become the major traffic over the Internet. Therefore for secure messages, data must be made secure using Steganography Techniques and then transmitted over the Internet. This paper focuses on Steganography using Bit Plane Complexity Segmentation (BPCS). BPCS allows data embedding even for High capacity data, and more compression as compared to other Steganography methods. BPCS uses characteristics of human vision which cannot perceive any shape information in a very complicated binary pattern. Steganography pay attention to the degree of Invisibility while watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations(rotation, cropping, filtering), audio operations(rerecording, filtering)in the case of images and audio files being watermarked respectively.**

Keywords— **stegano, Steganography, data, hiding, high, capacity, embed, embedding, bpcs.**

I. INTRODUCTION

Issues of security of information have been increasing day by day, and information hiding has become a hotspot in the research field of information security. Through embedding unnoticeable secrets into digital media signals such as images, audio and video, data hiding realizes the function of copyright protection and secret communication. Information hiding mainly consists of two main branches, which are digital watermark and Steganography. It is an information security technology about secure transmission of secret data, which is using images, audio and other digital media as a vessel image, embedding the secret information to be sent into the carrier signal, transmitting as an unnoticeable way over the internet, aiming at sending out the information secretly and safely without causing suspicion of the hidden message in the vessel. Many people think steganography is a relatively new area in research but some examples of steganography trace far back to 440BC. Demeratus, a Greek at the Persian Court, warned Sparta of an invasion by Xerxes, King of Persia. Demeratus removed the wax from a writing tablet, wrote his message on the wood underneath and then covered the message with wax. Another example of early steganography involved Histiaeus, who shaved the head of his most trusted slave and tattooed a message. Once the slave's hair had regrown, he was sent to transport the message. This method was still used by German spies at the beginning of the 20th century. In 1499, Johannes Trithemius published Steganographia, one of the first books on steganography.

Steganographic messages may be encrypted before they are inserted into cover image for increasing the security; this adds more security for the secret message. Only the sender and the receiver will know about the technique used for encryption.

The very difference between cryptography and steganography is that in cryptography people know there is a secret message, while in steganography the purpose is to keep others from knowing the very existence of the information. If a third-person suspects of this carrier medium then the method has failed. The messages embedded into an image are often imperceptible to the human eye but they might bother the statistical data of the image. The cover image also needs to be chosen carefully as it affects the security techniques. Gray scale images have been recommended by many steganographic experts as the best to use as cover images.

Images are popular medium for data hiding in steganography world. With increase in the details in image there is less number of constraints for hiding data before making it suspicious. There is abundance amount of data on internet many of which could be steganographic. There have been rumors about terrorists using image steganography to communicate with the help of internet. Jack Kelley wrote two articles in USA Today (2001) which indicated that *Osama Bin Laden and his organization, Al-Qaeda as well as other terrorist groups were using steganography to plan and implement terrorist attacks* [1].

© 2014 JCT. ALL RIGHTS RESERVED

Steganography essentially exploits human perception, since human senses are not trained to look data hidden in such images. The simplest way to explain steganography is it hides message in another file.

RSA (abbr. for Ron Rivest, Adi Shamir and Leonard Adleman) is a public key cryptography algorithm used for Encrypting and Decrypting information, when used with BPCS Steganography, it does not only provides good visual imperceptibility and high data embedding capacity, but also capable of resisting the analysis of the whole complexity histogram.

II. EXISTING SYSTEM

Image Steganography techniques are classified as: Spatial-domain based and Transform domain based Steganography.

A. *Spatial Domain Method*

In spatial domain scheme, the secret messages are directly embedded. The Least Significant Bits (LSB) insertion method is the most common and simplest Steganography method. Here in this LSB technique, the LSB of the pixels are replaced by the message bits before embedding [2].

1) Least Significant Bit (LSB):

In a cover image it is very important to embed information for insertion we use LSB technique. The LSB in other words, 8 bytes inside an image get replaced to a bit of the secret message. A bit of each of the red, green and blue colour components can be used when we are using a 24-bit image (each represented by a byte). That is we can store 3 bits in each pixel. A total amount of 1,440,000 bits or 180,000 bytes of embedded data in an image can be stored in 800 x 600 pixel image [3].

For e.g., a 24-bit image having a grid for 3 pixels can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the LSB of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Just the 3 underlined bits needed to be changed according to the embedded message out of the 8 bytes, but the embedded message gets stored in all the 8 bytes. Only half of the bits in an image need to be modified on an average, to hide secret message using the maximum cover size. If we change the LSB of a pixel results in small changes in the intensity of the colours because there are 256 intensities of a colour. Which cannot be perceived by human eye and the image remains secret and hidden.

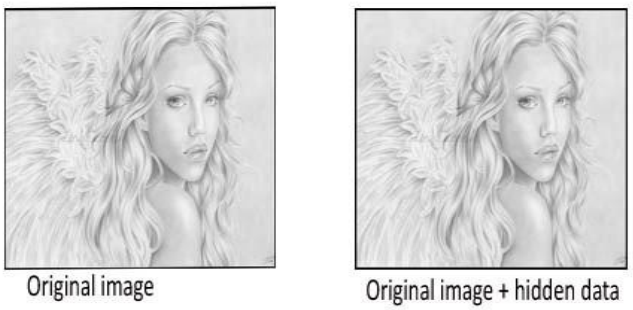

Fig. 1 Steganography using LSB

2) Hiding Grey Images Using Blocks Method

Due to internet becoming popular for communication security of Digital media comes to the mind. Message hiding becomes an important part which will reduce the probability of detecting the message. This method hides an image (grey) in one another. Blocks of equal sizes are made in cover, which equals to size of the embedding image [4].

We compare each pixel of embedding image with all the corresponding pixels in the blocks of the cover image eg. Assuming there are C blocks .i.e. as pixel (i,j) in the embedding image is compared with the pixel (i,j) in all C blocks of cover image. The best pixel selected is to be embedded. The one that gives minimum pixel difference between it and the pixel to embed is called the Best Pixel. For Example, if pixel (i,j) to embed has a value 290, and corresponding pixels values are: 208, 260, 249, 282, 255, 289, 270, and 262 (assume cover is divided into 8 blocks). Then the pixel with value 289 will be selected to embed pixel of 290.

3) Hiding Secret Message in Edges of The Images Method

In Edge Based Steganography only the sharper edged regions are used for hiding the message and keeping the other smoother regions as they are. Changes at the sharper edges are difficult to observe than those in smoother regions [4].

We use method called Enhanced Least Significant Bit algorithm which reduces the pixel modification rate thereby increasing the security both statistically & visually.

4) Grey Level Modification Steganography Method

This method is based on image layers. In this host image is divided into blocks and the corresponding secret message bits are embedded into each block by the binary representation of pixel values. It then searches on rows and columns of the layers for finding the most similar row or column. A new location is marked based on rows or columns and then differences from the secret message is then marked by modifying minimum number of bits in the LSB of the blocks.

B. *Transform Domain Method*

The technique is used for hiding a large amount of data which provides high security, good invisibility and no loss of secret message. The main idea is to hide information in frequency domain by slightly changing carrier magnitude of

© 2014 JCT. ALL RIGHTS RESERVED

all of DCT (discrete cosine transform) coefficients of cover image. The image blocks are converted from spatial domain to frequency domain using 2-D DCT. The carrier image is divided into non overlapping blocks of size 8×8 which are called Bit-plane Blocks and forward DCT is applied on each of blocks of cover image [5].

1) JPEG Steganography

JPEG images were thought as unsupportive to steganography as they use lossy compression method which leads to parts of the image data being altered. One of the major characteristics of steganography is that it lives in the redundant bits and also the secret data is hidden in these bits of the carrier and since in JPEG these redundant bits are left out it might destroy the secret data stored there. Even if the message is somehow kept intact it becomes difficult to embed the secret data without making the carrier image look suspicious because of the harsh compression applied. However, compression algorithm's properties have been exploited in order to develop a steganographic algorithm for JPEGs [6]

One of these properties of JPEG is exploited to make the changes to the image invisible to a human eye. In DCT transformation phase of the compression algorithm, the unnoticeable rounding errors occur in the coefficient data. Though this property is classifies this algorithm as being lossy, still it can be used to hide secret information. It is neither possible nor feasible to embed valuable information in an image that uses lossy compression, as the secret information might be destroyed in the process of compression. So the JPEG compression is actually a two stage process which includes lossy and lossless stages. The quantization phase and the DCT are part of the lossy stage, while the lossless stage includes Huffman encoding used to further compress the data.

Steganography can take place between these two stages. The same principle of LSB insertion can be used here and the message can be embedded into the least significant bits of the coefficients before Huffman encoding is applied. By embedding the information in the transform domain and in this stage, it is very difficult to detect it, since it is not in the visual domain.

2) Spread Spectrum Steganography

In spread spectrum techniques, secret information is spread throughout the cover-image making it difficult to detect. A system proposed by Marvel et al. combines image processing, error control coding and spread spectrum communication to hide the secret information in images. The process of spreading the bandwidth of a narrowband signal across a wide band of frequencies is called spread spectrum communication. The narrowband waveform with a wideband waveform, such as white noise is adjusted to accomplish this. After spreading, the narrowband signal in any one frequency band has low energy and is therefore difficult to detect.

In spread spectrum steganography the secret information is embedded in noise and then combined with the cover image to produce the final "stego" image. The fact that the power of the embedded signal is much lower than the power of the carrier image makes it imperceptible to the human eye or by computer analysis without access to the original image [3].

III. PROPOSED SYSTEM

A. *BPCS steganography*

In BPCS steganography following arithmetic is used:

1) First the carrier image is divided into 8 different Bit-Planes. These bit-planes are further divided into 8x8 which is known as bit plane blocks all of same sizes.

2) The amount of all the adjacent pixels that get different values (assume one pixel is 0, and the other is 1) is called complexity. After the division of carrier image the complexity of each block is calculated. The next step is to find the value of Cmax; the maximum possible value of the complexity is denoted by Cmax.

3) C omplexity threshold of the bit-plane block is set as αCmax, here α is a parameter. Those bit-plane blocks whose complexity is larger than αCmax are used to embed the secret message or file. The value of α is inversely proportional to the amount of secret information that can be embedded in the image.

4) The secret information is disguised into bit-plane blocks that can be replaced directly with the original one if the complexity of original bit-plane block is greater than αCmax. Still we need to take conjugate processing with checker-board pattern (as shown in Fig. 2)

If complexity ≤ αCmax, than take the new block replace the original one.

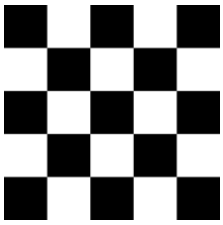

Fig. 2 Checker-board Pattern

5) The blocks that needed conjugate processing should be listed and this list is also embedded in the carrier image. The embedding of this extra information cannot produce an effect on the embedded secrets, and it must be correctly picked up.

In the process of secret information extraction first, all those pieces of carrier data whose complexity is greater than αCmax are collected, and the list that is embedded in the carrier as mentioned in step (5) to confirm the blocks that have taken conjugate processing. The blocks collected need to take XOR operation with tessellated chock to get the recovery of secret data.

B. *Improved BPCS Steganography*

The original BPCS algorithm creates a set of bit-planes from the carrier image; these bi-planes have a high correlation between them. The higher the number of bit-plane is, the stronger is the correlation between the pixels of the bit-planes [7]. Here setting same embedding strength for different bit-

© 2014 JCT. ALL RIGHTS RESERVED

planes surely influences the correlation between the bit-planes, which leads to abnormalities in complexity histogram. Hence, the security of steganography will be affected. Analysis of complexity histogram can show the existence of secret information. The analyst can also estimate the embedding threshold value accurately [7]. To resist this statistical method improved BPCS algorithm is used.

When the bit-plane is high there is strong correlation adjacent pixels, due to this correlation we can see sketchy outline of the image. Here the dates of the lower bit-planes are similar to random noise. Therefore, we shall make better use of Human Vision System (HVS) characteristic and consider the local characteristic of carrier when embedding secret data, and treat all bit-planes with different ways, with setting greater threshold for the higher bit-planes and smaller for the lower ones. By using different embedding for different bit-planes, this scheme resist statistical analysis, and it also 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.

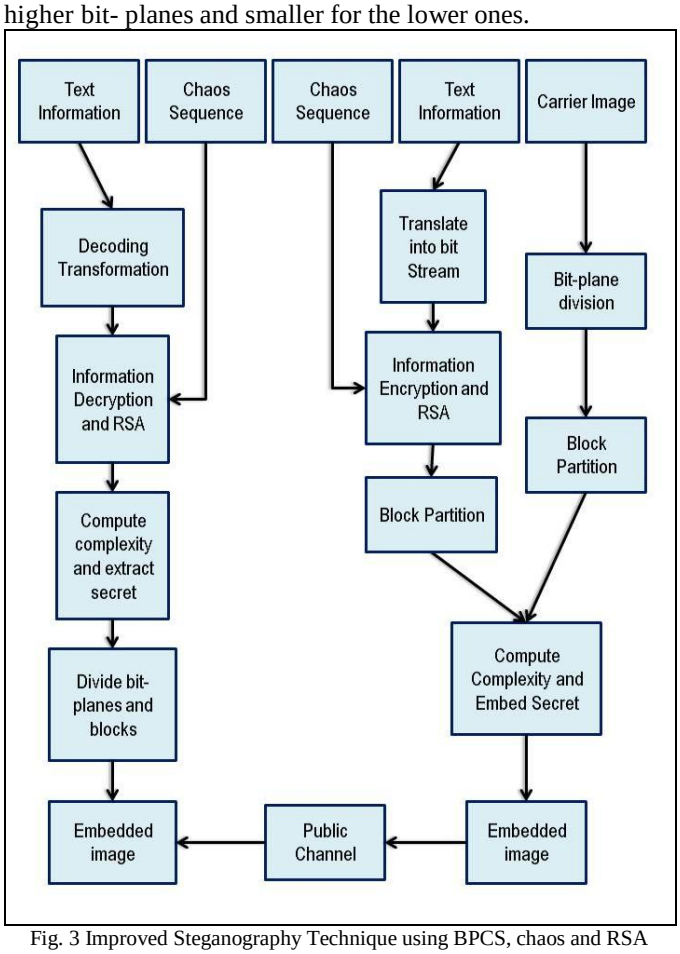

Fig. 3 Improved Steganography Technique using BPCS, chaos and RSA algorithm

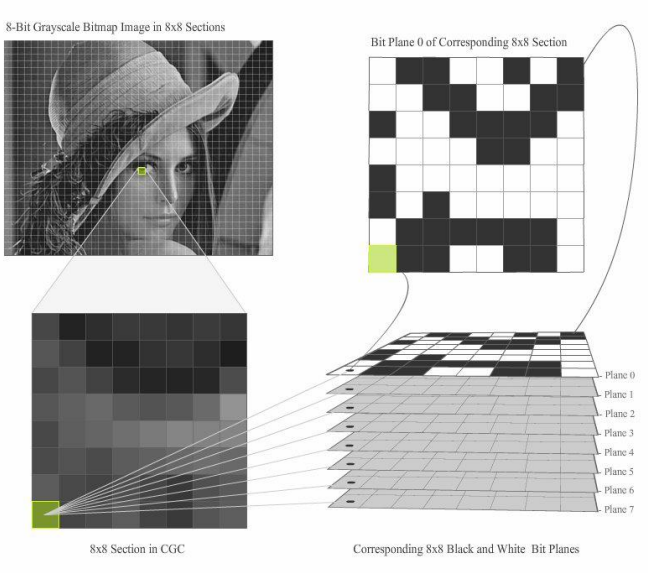

Fig. 4 CGC Diagram

Fig. 5 Golf Images at Relative Embedding Capacities.

© 2014 JCT. ALL RIGHTS RESERVED

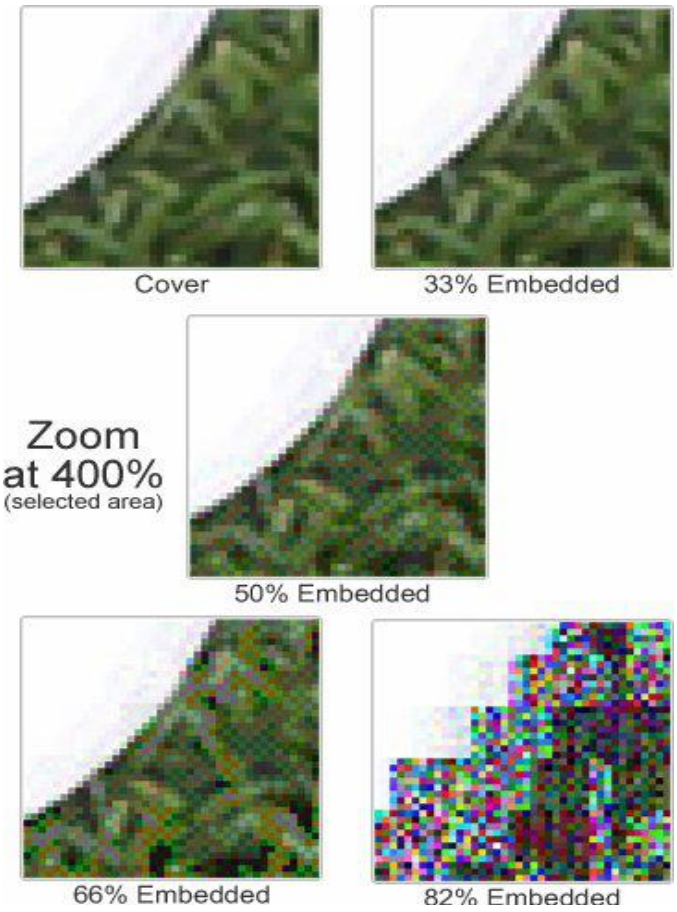

Fig. 6 Golf Images at Relative Embedding Capacities, Zoomed

IV. Applications

In applications of BPCS Steganography, it differs from digital watermarking in two ways. The first is that for full color for images e.g. 24-bit, which has a very large capacity of embedding.

The obvious application of BPCS Steganography is to make a secret communications. For example suppose a person or company has a web page containing secret information meant for other clients. So anyone can download that web page, but they are not able to get that hidden information. For extracting that the secret data would require software with our customized parameters (like public or private key). Encryption of the embedded data improves security of the data.

In some applications, the presence of the embedded data may be known, but without the customized parameters, the data is inseparable from the image. In such cases, the image can be viewable as normal image, but the data is secretly tied in the image and can't readily be replaced with other data. Others may know the data present in the image, but without the key they cannot alter/change it and still make it readable by the customized software.

Applications of BPCS Steganography are not limited to secrecy only. For such applications, the presence of the embedded data may be known, and the software for extraction or getting and embedding can be standardized to a common set of customized parameters. An example of this is a digital photo. We can add the details of the photos like where photo has been taken and all related information of that photo in photo itself.

V. Conclusions

BPCS algorithm has some disadvantages which are removed by the proposed improvisations. The amount of secret information that can be embedded in the carrier image has also increased by use of this method. The improved BPCS algorithm is better than LSB insertion and spread spectrum steganography. The use of RSA algorithm further increases the security of the secret information.

REFERENCES

[1] Terror groups hide behind Web encryption: http://usatoday30.usatoday.com/tech/news/2001-02-05-binladen.htm

[2] Johnson, N.F and Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 2008.

[3] T. Morkel, J.h.p. Eloff, M.S. Olivier "An overview of image Steganography" Information and Computer Security Architecture (ICSA) Research group.

[4] Jagvinder Kaur and Sanjeev Kumar, "Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011

[5] Comparison of Various Image Steganography Techniques http://www.ijcsmr.org/vol2issue1/paper177.pdf.

[6] JPEG Compression Steganography & Cryptography Using Image-Adaption Technique http://ojs.academypublisher.com/index.php/jait/article/download/0103141145/2012

[7] High Capacity Data Embedding Using BPCS Steganography http://www.ijsrp.org/research_paper_jul2012/ijsrp-july-2012-96.pdf

© 2014 JCT. ALL RIGHTS RESERVED