Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

BPCS Steganography for more visual Imperceptibility and Data Security

Vikas S. Kait [1], Prof. Vrushali G.Raut [2]
[1]*Electronics and telecommunication, G.S.Moze C.O.E,Pune*
[2] *Electronics and telecommunication, Sinhgad C.O.E.Pune*

Abstract -- There are many techniques to conceal the existence of hidden secret data inside a cover object. Steganography is one of the most powerful techniques. The bit-plane complexity segmentation steganography has good visual imperceptibility and high data embedding capacity compare to other steganographic techniques.

In the traditional steganograhy techniques principle was either to replace a special part of the frequency components of the carrier image, or to replace all the least significant bits of a multi-valued image with the secret information. The bit-plane complexity segmentation (BPCS) steganography algorithm uses an image as the carrier data, and we embed secret information in the bit-planes of the carrier. 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. The technique used in the BPCS steganograhy is to replace all of the noise-like regions in the bit-planes of the carrier image with secret data without deteriorating the image quality. With this we can remove the noise by replacing the noise present in the cover image.

The design utilizes the Xilinx Spartan 3E Papilio one FPGA as well as specialized logic to perform the steganography steps. The design balances the tradeoffs such as imperceptibility, quality and capacity. The baud rate of 9600 bits per second may cause delay when we choose large image and huge amount of data.

Keywords — Cover Image, Information Hiding, Papilio, BPCS, Steganography, Baud rate.

I. INTRODUCTION

In recent years, information security issues have been paid more and more attention over internet and digital media, 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, information hiding realizes the function of copyright protection and secret communication. Information hiding mainly consists of three branches cryptography, digital watermark and steganography.

Cryptography means sender convert plaintext to secret text by using Encryption key and other side receiver decrypt secret text to plain text. While cryptographers invent clever secret codes, cryptanalysts attempt to break these codes. These two disciplines constantly try to keep ahead of each other. Ultimately, the success of the cryptographers rests on the Cryptographic systems tends to involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely.

Digital Watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence Data

embedding for copyright protection is specifically called digital watermarking. The robustness of the embedded data is important in digital watermarking.

Steganography is an important branch of information hiding, it is mainly used in secret communication. Steganography is an information security technology which transmit the secret information using images, audio and other digital media as a image, the secret information is embedded in the cover image which is to be sent. The cover image consisting of hidden message inside it called as stego image. This stego image is transmitted as an unnoticeable way through public channels, especially the internet, aiming at sending out the information secretly and safely with imperceptibility of the hidden message [1].

BPCS, which stands for Bit-Plane Complexity Segmentation Steganography, is the development of List significant bit (LSB) method, and it has better performance than the simple LSB method. The major idea is that the color image is split into RGB planes and multiple bit-planes of the RGB planes are formed which are divided into fixed-size blocks. This technique makes use of the characteristics of the human vision system whereby human can't detect the information in a very complicated binary pattern, therefore, we can replace all of the "noise-like" regions in the bit planes of the cover image with secret data without deteriorating the image quality, so this method has better visual imperceptibility. In the LSB steganography we can hide secret data in the least significant bits only while in case of the BPCS steganography we can hide the data up to higher bits in several bit planes . Because of we can embedded the data in several bit-planes, compared with the LSB method it has greater data embedding capacity. In LSB steganography we can hide maximum of 10% data of the cover image size while in BPCS steganography it is up to 50% to 60%.

The remainder of this paper is organized as follows: Section II discusses in detail the BPCS based image steganography. Section III presents concluding remarks.

II. BPCS BASED IMAGE STEGANOGRAPHY

2.1 BPCS Steganography

In BPCS steganography we can embed data if we can locate noisy regions in a carrir image correctly. The approach employed in new BPCS steganography is to take cover image and convert it to the gray scale so that its performance increase three times more than when we take the color image. Then split the image into the eight bit planes from LSB plane to the MSB bit plane. The next step is to divide each bit-plane of the cover image regularly into small square binary pixel blocks and to find blocks those have complex black-and white patterns. If a binary block has a complex black-and-white-pattern, we can expect that the block is in a noisy region. A complexity measure is introduced to determine whether a block is complex or not, i.e., whether the block has a complex black-and white pattern or not. It is defined by the total length of black-and-white borders within a block. If the value of this black-and-white border complexity measure for a block is higher than a given threshold value, the block is regarded as complex one. We can regard a secret message as a stream of binary blocks.

In BPCS, data embedding is performed by replacing complex blocks in bit-planes of a cover image with the blocks obtained from the secret message. When we regard the secret message as a stream of binary blocks, some of them may be simple, i.e., not complex. If we embed a simple block as it is, noticeable changes may be left on the cover image. The secret message should hence be converted into a stream of complex blocks on embedding. In BPCS, an operation called conjugation is applied to convert simple blocks into complex ones. In order to extract the secret message embedded in the cover image, we should know which blocks of the secret message are conjugated and which are not. The first bit of the 8×8 block is taken as "zero" if we embed the secret message without complex conjugate operation and it is taken as "one" if complex conjugate operation is performed. This information is stored in a conjugation map. It should be embedded along with the secret message as blocks. Note that the blocks of the conjugation map should be also conjugated if they are not

complex enough. The above black-and-white border complexity is a suitable measure for classifying blocks into complex ones and simple ones.

The original BPCS algorithm divides the carrier image into several bit-planes, and there is high correlation between the bit-planes. We embed the data in the region where complexity is present The complexity is defined as the amount of all the adjacent pixels that get different values (one pixel is 0, and the other is 1). The higher the bit-plane is, the stronger the correlation between the pixels of the bit-planes. 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 less imperceptibility so the security of steganography will be affect. Such image can easily be get snoop by snooper [2]. To avoid the detection of the stego image, we shall make better use of the characteristics of the human

Vision system whereby a human cannot perceive any shape

Information in a very complicated binary pattern and consider the local characteristic of the image when embedding secret information. The idea behind the new BPCS steganography is to treat different bit-planes with different way, setting greater threshold for the higher bit-planes and smaller for the lower bit-planes. Using different thresholds for different bit planes i.e. using different bit-planes for 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 bit planes.

2.2 Block Complexity Measures

A secret data file is converted into binary data, and is replaced with the pixel data in noisy regions of a cover image. To embed the secret data file secretly we have to locate noisy regions appropriately. If not, informative regions of the cover image would be disordered by the embedded secret data file and noticeable changes would be left after embedding. In BPCS, the noisy region of an image is located on each bit-plane as small pixel blocks those have noisy patterns. Each bit-plane of a cover image is regularly divided into small square binary pixel blocks of 8×8 sizes. A binary pixel block can be regarded as noisy region if it has a complex black-and-white pattern. Only such complex blocks are used for embedding.

While embedding the secret data which is in the binary form, the care taken is that we should hide large amount of data on the LSB planes while the less amount of data should hide in the MSB planes to preserve the imperceptibility. The blocks in a cover image are examined one by one from those on the LSB plane through up to those on the highest bit-plane (the MSB plane).The secret data should be hide in the LSB planes and then in the MSB planes. A secret data file is embedded piece by piece as a complex block is found on a bit-plane [3].

This way of embedding is preferable, because changes in lower bit-planes would not spoil the quality of a cover image greatly. The problem here we encounter is how to measure the complexity of the black-and-white pattern in a block. We find that a block is simple when it is entirely or almost entirely in black or white Fig 1. Shows the simple or non-complex block. Block is perfectly complex if it's all adjacent pixels get different values as shown in Fig 2. It has maximum complexity of $\alpha = 1$.

Suppose that K out of M pixel borders lie between black and white pixels in a block, the complexity measure is then given by:

$$\alpha = \frac{K}{M} \qquad (1)$$

The block having many adjacent different black-and white transactions inside, we can regard it as complex. On the other hand, if α of a block is small, the block must be simple. The range of this measure is [0, 1]. A threshold value of the block T is regarded as complex if $\alpha(T) \geq \alpha_0$.The α_0 is

introduced to discriminate complex blocks from simple ones. In this paper we are taking threshold value as α= 0.3. This black and-white border complexity measure α is easy to understand and usually works well for classifying blocks into complex ones and simple ones.

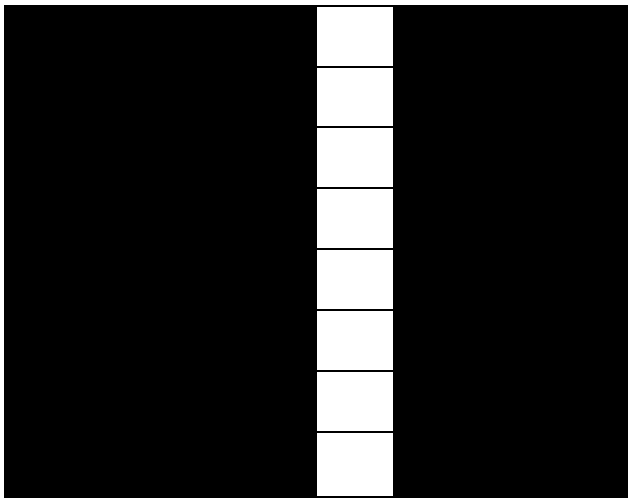

Figure 1. Non Complex Block of 8 × 8 ,$\alpha = 0.1429$

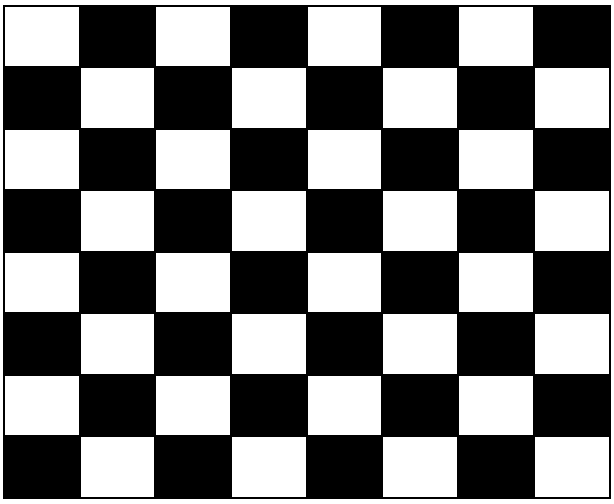

Fig 2. Perfectly complex block of 8 × 8 ,$\alpha = 1$

2.3 Encoding Procedure

The encoding procedure of BPCS steganography is as follows:

1) The carrier image is divided into 8 different Bit-Planes. These bit-planes are divided into small size blocks of 8 × 8 size, which is called, bit-plane blocks.
2) Calculate the shift in bits from 0 to 1 of every block i.e. the complexity. The C_{max} is denoted as maximum possible value of the complexity. For example the C_{max} of the 8 × 8 blocks is 7×8×2=112.
3) Set the complexity threshold of the bit-plane block as αC_{max}, where α is a parameter such that $0< \alpha<1$. In this paper it taken as 0.3. The bit-plane blocks having complexity greater than αC_{max} are used to embed secret information. More secret information can be embedded if the value of α is smaller.
4) If the complexity of bit-plane block is greater than αC_{max} then we can embed the secret information in the bit-plane block straightly. If the complexity is less than or equal to αC_{max}, it need to take conjugate operation with the checkerboard pattern block. Then replace the original block.
5) Make a record of the blocks that have taken conjugate processing as it necessary while decoding. The first bit of the 8 × 8 blocks is set as 1 if the conjugate processing is done, otherwise it is set as 0.

2.4 Decoding Procedure

The decoding procedure is systematically revers the operations of the encoding. The way the encoding is organized; all the blocks that are complex in the original image are complex in the encoded image as well. The decoding procedure can be summarized as follows:

1) The stego image is divided into 8 different Bit-Planes. These bit-planes are divided into small size blocks of 8 × 8 size, which is called, bit-plane blocks.
2) Collect all the blocks of the carrier data whose complexity is greater than αC_{max}.
3) Collect the extra information embedded using conjugate processing.
4) These blocks needed to take XOR operation with check board pattern to get the recovery of Secret Message[4].

III. CONCLUSION

3.1 Conclusion

In conclusion, it can be seen that the BPCS technique hides the secret data with large imperceptibility. It has shown a significant improvement over a LSB implementation.
The future work should focus on the steganography method presented here can be combined with some digital watermarking method to keep the data non reasonable even if it were detected.

3.2 Applications

1) The BPCS Steganography has more obvious applications relate to transmission of secret data.
2) BPCS steganography has plenty of military and satellite communication applications.
3) The health care, and especially medical imaging systems, may very much benefit from information hiding techniques.
4) Image steganography could also be used to embed secure information like customer name, account information and key presses in ATM, camera feeds and numerous other legal applications.
Of course, it could also be used for various illegal applications like storing inappropriate material on shared computers and smuggling proprietary information from offices[5],[6].

IV. ACKNOWLEDGMENT

The authors would like to thank the anonymous Reviewers for their valuable suggestions and they would also like to thank the prof. Pradip D. Dudhat for his valuable guidance and his enthusiastic assistance in improving the clarity of this article.

REFERENCES

[1] Peipei Shi and Zhaohui Li, ‘‘An improved BPCS Steganography based on Dynamic Threshold”, IEEE International Conference on Multimedia Information Networking and Security,2010.
[2] Tao Zhang , Zhaohui Li, Peipei Shi ,“Statistical Analysis Against improved BPCS Steganography”, The 2nd IEEE International Conference on Advanced Computer Control, 2010: 237-240.
[3] E. Walia, P. Jain and Navdeep , “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science and Technology, April, 2010, Vol. 10, pp. 4-8.
[4] Peipei Shi, Zhaohui Li and Tao Zhang ‘‘A technique of improved steganography text based on chaos and BPCS”,2nd International Conference on Advance Computer Control(ICACC),2010 IEEE.
[5] D. Saravanan , A. Ronald Doni and A. Abisha Ajith, ‘‘Image Information Hiding: An Survey’’, The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013.
[6] K. Prasad, V. Jyothsna, S Raju and S. Indraneel, “High Secure Image Steganography in BCBS Using DCT and Fractal Compression”, International Journal of Computer Science and Network Security, vol. 10 No.4, April 2010.

