Survey on Modified BPCS Steganography based on sequence of cipher bits

Sumit S. Solanke[1], Prof. Deepak. C. Dhanwani[2]
[1]Student, Dept. of Computer Science & Engg,
[2]Asst. Prof. Dept. of Computer Science & Engg,
P. R. Pote (Patil) College of Engg & Mang Amravati, India

Abstract - Digital communication has become an indispensable part of today's world. The information can be communicated in numerous forms over several channels. Many times, it is desirable for the communicating parties that the conversation be kept secret. Need for such secrecy in communication arise from diverse applications such as bank transactions, business communications and credit card transfers. 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. This paper is based on review of hybrid cryptographic techniques based on DES and RSA algorithms to achieve data encryption and compression technique to store large amount of data. We discussed Modified BPCS (Bit Plane Complexity Segmentation) steganography technique that can replace all the "noise-like" -regions in all the bit-planes of the cover image with secret data without deteriorating the image quality.

***Keywords* - Steganography, Hybrid cryptography, BPCS, Bit-plane**

I. INTRODUCTION

Nowadays, for data transmission internet has become a convenient way due to a fast development of modern technology. However, development of Internet gave birth to some potential problems, such as the copy and corruption of digital information. Hence, the information security became one of the important topic to study. One solution to ensure secret information without being detected, destroyed or stolen is to use information hiding techniques. We create a stego medium by embedding the secret information into a digital medium by using these hiding techniques. The illegal party will be unable to detect that there are some secret information concealed in the medium since the stego medium is similar to the original one. Therefore, the safety of the secret information can be made sure. Thus there is a need to develop some means to facilitate secure communication. This brings us to study of cryptography.

Cryptography is the study and practice of techniques for secure communication between two parties. Cryptography, derived from Greek, literally means "secret writing". Generally, cryptography is concerned with developing new algorithms and devising better encryption techniques [5]. It mainly deals with mathematical computations and exploits the properties of discrete logarithms. With the advent of computers and increase in their capabilities, the cryptographic algorithms are becoming more and more complex [8] [9]. The techniques of cryptography are being increasingly used in a variety of domains. To address the security challenges, different cryptographic techniques have been evolved over time to prevent unauthorized access to secret information. The most popular method is encrypting the data.

Encryption provides means to transform data in such a way that only authorized recipient can read it. The encryption algorithm used to encrypt the plaintext transforms it into unreadable cipher text. Such data can only be read by a person having appropriate key. However, such encrypted message clearly arouse interest and attracts suspicion. Once the existence of secret message revealed, possibility is that it will be break. Further more such encrypted messages are incriminating in some countries. In many applications it is desirable to communicate secretly without anyone even noticing. For fulfilling such need we make use of steganography [4]. Applications of cryptography include ATM cards, internet passwords, and electronic commerce, military communications, etc.

Steganography is the art and science of concealing secret messages within appropriate carriers. The carrier can be any digital media, namely image file, text file, video, etc. The advantage of steganography over cryptography is that it does not invite undue attention to itself. In steganography the very existence of concealed message is hidden [5] [8]. Nobody apart from the intended recipient even knows that a message is being sent. Our project aims at applying the techniques and principles of both cryptography and steganography to provide a more secure means of secret communication between two parties [4] [8].

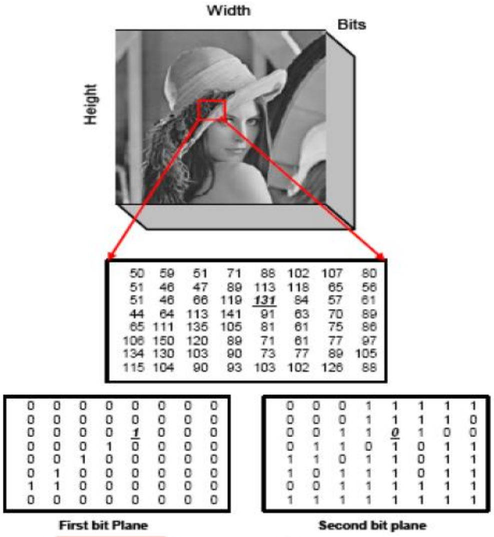
II. RELATED WORK

A. Bit Plane Slicing Concept

Digitally, an image is represented as pixels. These pixels are further expressed in the form of bits. The operation of splitting the image into its component bit planes is called Bit plane slicing [8]. In an 24-bit image, intensity of each pixel is represented by 24-bits. Such image is composed of 3 colour channels- RGB. Eight bits dedicated to each of the 3 colour component with range from 0-255. A 'n' th-bit plane can be formed by selecting the nth bit from each pixel of the image. BPCS-Steganography makes use of multiple bit-planes. It replaces complex areas on the bit-planes of the carrier image with other complex patterns [8]. This replacing operation is called 'embedding'. The bit plane slicing can be better understood with the help of following figure.

B. Complexity of Binary Image

BPCS steganography makes use of the 'noise-like'/complex regions of an image. Complexity values are measured for each bit plane. Data well be embedded in bit-planes with higher complexity [8]. As such, there is no standard measure for determining complexity. With study and experience, one can come to the conclusion that no. of transitions across black-white border is correct measure for complexity [4] [8]. If the no. of transitions is large, the image is considered as complex. Complexity is determined as follows:



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

Figure 2.1: Bit Plane Slicing

Complexity (alpha) = number of borders/ maximum borders possible
where, border = transitions across black and white borders [7] [8].
Min-alpha

- Min-alpha is o ne of the two customization parameters used in the application.
- Sender is required to set the complexity threshold for the image.
- The bit-planes whose complexity is greater than minAlpha is used to hide confidential data.
- As value of minAlpha is lowered, more confidential data can be embedded.

This technique works very well with complex images, as they have many regions of high complexity. Images with complex textures and well shady objects generally have a high data hiding capacity [8] [5]. BPCS steganography doesn't works well with plain and uniform images, as these images have large areas of uniform and well-defined boundaries.
With these types of images, there is very little complexity to use and any attempt to hide results in easily detectable output.

C. Image Histogram

An image histogram is a graphical representation of the intensity distribution in a digital image [7]. It plots the number of pixels for each intensity value. By viewing the histogram for an image a viewer will be able to see the entire intensity distribution in one glance. The horizontal axis of the histogram represents the intensity values, while the vertical axis represents the number of pixels in that intensity. The left side of the horizontal axis represents the dark and black areas, the middle represents grey and the right hand side represents light and white areas. The vertical axis represents the size of the area that is covered in each of these zones [7] [5]. Thus, the histogram for a dark image will have the most of its point on the left hand side of the histogram. Alternately the histogram for a bright image will have most of its data points on the right hand side of the histogram. The histogram can be viewed for all 3 colour channels- RGB. In the picture above

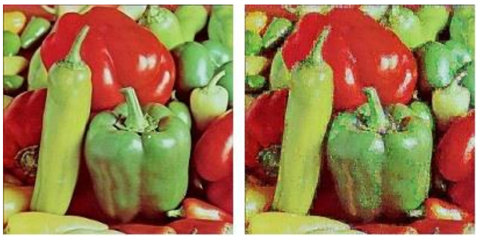


Figure 2.2: Image: 'Pepper' before and after steganography

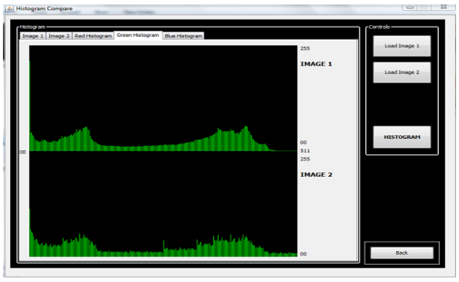


Figure 2.3: Histogram for 'Pepper' before and after steganography

we have shown green histogram and it can be seen that, there is no visible difference in histogram before and after steganography. Thus the design has high undetectability.

III. DATA EMBEDDING TECHNIQUES

Data embedding is a technique used to embed additional data into a multi-media file such as an image, a video or an audio file [5]. The embedded data gets hidden into the file and one cannot differentiate the embedded data from the original data [8]. There will be no information added to the file which informs existence of data. However, the embedded data does exist in the file, and can be extracted from the file applying appropriate procedure [13] [8]. The two major branches of data hiding are:

A. Watermarking

- Watermarking technique is used to verify the authenticity of the _le or to prove the identity of its owners.
- Further it is popularly used for tracking copyright infringements and for currency authentication.
- It is extremely robust against modifications to tampering to image, i.e. attacker cannot remove or replace watermark. Any attempt to remove or tamper the embedded data leaves the carrier useless.
- The presence of a watermark on the file is often declared publicly.

B. Steganography

- In steganography the very existence of concealed message is hidden.
- Steganography involves developing various methods and algorithm implementations.
- It is usually used in combination with cryptography for providing security applications [5] [8].
- Steganography does not attract attention/suspicion to itself.
- Large multimedia files are ideal for steganographic communication. Owing to their large size, they provide high embedding capacity.

C. Difference between the Watermarking and Steganography

Steganography is different from watermarking in three basic ways. The foremost point of difference is steganography exhibits very large embedding capacity as compared to watermarking. The second point of difference is that Steganography does not have robustness. It is affected by even minor changes in output image. This is a good property in itself and is useful in projects an unauthorized user might get access to output image. Changes like cropping, blurring or image compression would damage the image. Lastly, while steganography endeavours to hide the existence of secret data, in watermarking the presence of the watermark is often declared publicly.

IV. BIT PLANE COMPLEXITY SEGMENTATION (BPCS)

BPCS technique was jointly proposed by Eiji Kawaguchi and Richard Eason in 1998. In BPCS steganography method all the "noise-like" and "complex" regions in the cover image are replaced with secret message [4] [8]. True colour images (i.e. 24-bit images) are generally used as cover data. BPCS steganographic method has high embedding capacity and undetectability.

A. Hiding and Extracting Data

Cover Image

- The carrier image is divided into square blocks of 8X8 pixels [8].
- Every such block is further divided into 24 bit-planes, eight for each colour channel-RGB. This would appear as slicing the 8x8 pixel planes into 24- 8x8 black-and-white bit planes [5] [8].
- Complexity are then measured for each bit plane. Complexity is calculated as follows
- Complexity (alpha) = number of borders/ maximum borders possible
  Where, border = transition across black and white boundary [8] [5].
- Data is embedded in bit planes with higher complexity.

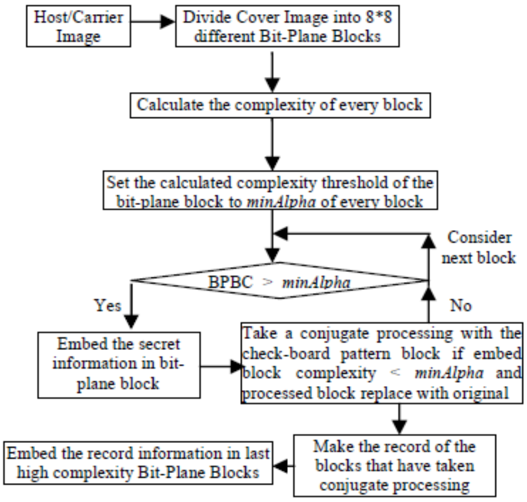

Host/Carrier Image
Divide Cover Image into 8*8 different Bit-Plane Blocks
Calculate the complexity of every block
Set the calculated complexity threshold of the bit-plane block to minAlpha of every block
Consider next block
BPBC > minAlpha
Yes
No
Embed the secret information in bit-plane block
Take a conjugate processing with the check-board pattern block if embed block complexity < minAlpha and processed block replace with original
Make the record of the blocks that have taken conjugate processing
Embed the record information in last high complexity Bit-Plane Blocks

Figure 4.1: Control Flow of BPCS

Input Data

The input message is broken up into square blocks of 8x8 pixels. If the data to embed (8x8 blocks at a time) in the cover file is found to be complex, it can be directly embedded into the complex blocks of the cover image [4] [5]. If not, we would conjugate (exclusive-or) the data with a white checkerboard pattern (the most complex pattern) to ensure minimum complexity [8]. We will need a conjugation bit in each plane to indicate whether the data is conjugated with a checkerboard or not. This uses up 1 bit of embedding space per 8x8 region leaving 63 bits to embed per 8x8 bit plane [3] [8]. Once the data has been embedded, image is converted into the PNG format (Portable Network Graphics) and saved on to disk. The PNG compression algorithm is among the best in providing lossless compression. Unlike JPEG format, PNG compression involves no loss of data. Use of PNG format is indispensable for our application because any lossy compression of output image will lead to significant data-loss [8].

Extraction

Extracting the data is the same as embedding, except if a bit plane is determined to be complex, it will first check for the conjugation bit and extract the data appropriately [8] [4].

Destruction of Data

As far as the destruction of our embedded data goes, there were no preventive measures put in to prevent an attacker from actively destroying the data [3]. Even minor changes would completely destroy our embedded data and make it useless. Apparently this may seem like a drawback, but the BPCS technique is specifically used for embedding capacity as opposed to robustness, which is present in watermarking [8] [3].

V. CONCLUSION

From the study conducted over several sets of images from varying sources, it is observed that the BPCS method demonstrates high data-embedding capacity (in the range 50-60 percent). Also, it is seen that the original image and the final output appears to be almost identical to the human eye. In future work, we can experiment using different complexity techniques and compare the results obtained.

REFERENCES

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

[2] William Stallings, "Cryptography and Network Security: Principles and Practice" Pearson Publications, 2013.

[3] Smita P. Bansod, Vanita M. Mane Leena R. Ragha ; "Modified BPCS Steganography Using Hybrid Cryptography For Improving Data Embedding Capacity", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India, 978-1-4577-2078-9/12 IEEE 2012.

[4] Peipei Shi and Zhaohui Li: "An improved BPCS Steganography based on Dynamic Threshold", 2010 International Conference on Multimedia Information Networking and Security, 978-0-7695-4258-4/10 $26.00 © 2010 IEEE, DOI 10.1109/MINES.2010.87, IEEE 2010.

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

[6] Subba Rao Y.V , Brahmananda Rao S.S , Rukma Rekha N: "Secure Image Steganography based on Randomized Sequence of Cipher Bits", 2011 Eighth International Conference on Information Technology: New Generations, 978-0-7695-4367-3/11, DOI 10.1109/ITNG.2011.65, IEEE 2011.

[7] Eiji Kawaguchi and Richard O. Eason: "Principle and applications of BPCS-Steganography", 04469-5708.

[8] Shrikant S. Khaire, Dr. Sanjay L. Nalbalwar: "Steganography Bit Plane Complexity Segmentation Technique", International Journal of Engineering Science and Technology, Vol. 2(9), 2010, ISSN: 0975-5462, 4860-4868, IEEE 2010.

[9] Jinsuk Baekl, Cheonshik Kim, Paul S. Fisherl, and Hongyang Cha, "(N, 1) Secret Sharing Approach Based on Steganography with Gray Digital Images", Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference, 2010, pp-325 – 329

[10] Wuling Ren, Zhiqian Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", Second International Conference on Modeling, Simulation and Visualization Methods, 2010- IEEE, pp-221-225.

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

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

[13] Gandharba Swain, Saroj Kumar Lenka, "A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels", Proceedings of the International Conference on Communication and Computational Intelligence – 2010,Kongu Engineering College, Perundurai, Erode, T.N.,India.27 – 29 December,2010.pp.529-534