1. Transform the cover image from PBC to CGC system.
2. Segment each bit-plane of the cover image into informative and noise-like regions by using a threshold value (α0). Typical value of threshold 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.
5. Embed each secret block into the noise-like regions of the bit-planes. If any of the blocks is conjugated, then record these blocks in a "conjugation map."
6. Also embed the conjugation map as was done with the secret blocks.
7. Convert the embedded cover image from CGC back to PBC.

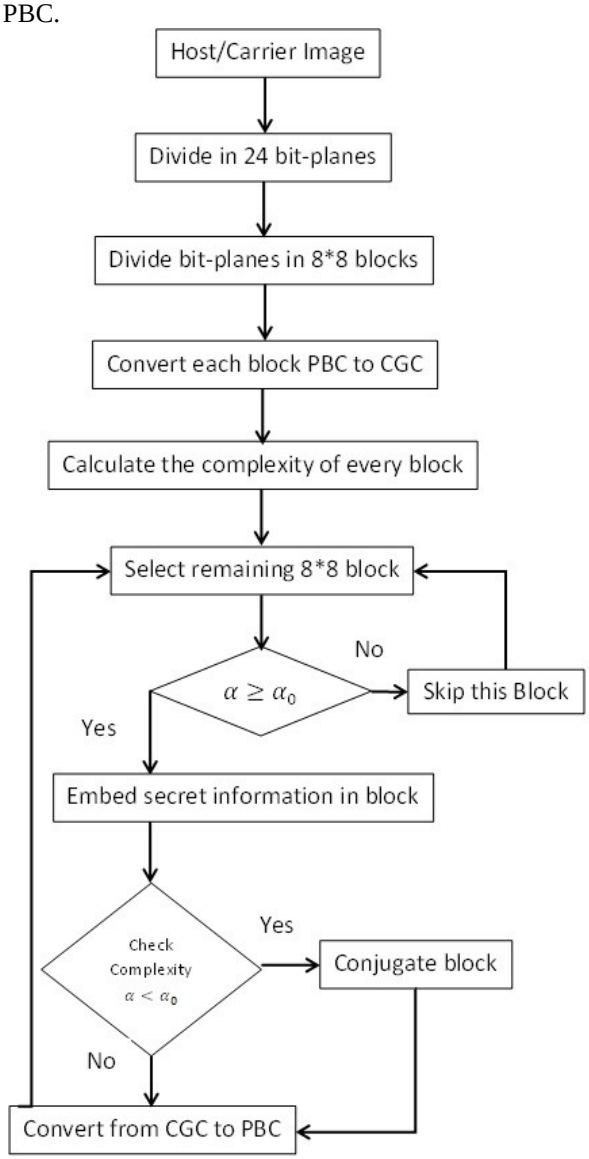

Figure 3: Flowchart- BPCS steganography [19]

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

3. Related Work

BPCS steganography provides 40% to 50% of data hiding capacity but there are several other techniques that can be used to increase the data hiding capacity. The original BPCS algorithm divides the carrier image into bit-planes, and there is high correlation between the bit planes. So setting the same embedding strength for different bit-planes have an influence on the correlation between the bit-planes and leading to the abnormalities of the complexity histogram, consequently, affect the security of steganography.

[12] Describe improved bit-plane complexity segmentation (BPCS) steganography. The Improved bit-plane complexity segmentation (BPCS) steganography carries on different processing's to different bit-planes. It will set high threshold value at the high bit-plane and low threshold value at the low bit planes. Through different bit-planes using different embedding strength, 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. [12] Concretely designs and carries out a steganography of the text secret information. In this, for the encryption of the text secret information RSA algorithm is used. The introduction of chaos theory conveniences to the test of steganography characteristics and enhance the safe of steganography. It provides good visual imperceptibility and data embedding capacity.

Vipul J. Patel and Neha Ripal Soni [13] provide a proposed modified BPCS steganography that increase hiding capacity and enhance security. With the use of fix block size and insert information into all bit planes, hiding capacity of image is not utilized. Security issues can be solved by comparative replacement of message block during hiding process. Therefore, we investigated the variable block size at each bit planes that increases hiding capacity and comparative replacement which increases security. As a result, the proposed modified BPCS Steganography method increases the embedding capacity and security compared to original BPCS technique.

On the other hand, [14] describes the techniques used in Steganography to hide information and deliver the message to the end user using Bit-planes without any loss of data. The method used is to replace lowest 3 or 4 LSB with message bits or image data (assume 8 bit values). We take the image and hide information in the LSB first and see the result and then implement by changing the pixel value from 1 to 7 bits. This Steganography algorithm based on embedding into the bit planes of the cover image and even tested for RS steganalysis, using a steganalysis tool "vsl1.1". The analyzer failed to detect the text which has been sent to the end user and LSB decryption which failed to detect the message by this we can say that our method is efficient.

Robust steganography using BPCS is proposed in [15]. This algorithm permits to implement hiding information into images for its secure transmission through no secure channels. This algorithm offers higher hiding capacity due to that it exploits the variance of complex regions in each bit plane. Unlike the similar methods based on BPCS, it uses the variance of complexity in each region of the image to determine optimal regions to insert the secret message. Simulation results of the proposed algorithm show that it is robust against noisy channels.

HIOKI Hirohisa [16] presents a new method for embedding data into an image called "A Block Complexity based Data Embedding". This method based on same principle as that of BPCS-Steganography. The two new complexity measures called the run-length irregularity and the border noisiness are proposed to properly discriminate noisy regions. An M-sequence is employed for converting data to be embedded into noisy data. ABCDE can be successfully applied to various images. We can expect that near 50% pixels of an image can be used for embedding without degrading its quality.

Rosane English [17] implements the bit plane complexity segmentation (BPCS) algorithm and provides a comparison in terms of effectiveness and hiding capacity with the list significant bit (LSB) algorithm using four bits. The Bit Plane Complexity Segmentation algorithm was chosen due to the effective high data hiding capacity.

On the other hand, [18] demonstrate the effectiveness of bit plane complexity segmentation in hiding medical records in color cervical images. Medical records of patients are extremely sensitive, needing uncompromising security during both storage and transmission. In addition, these records often have to be traceable to patient medical data such as X-ray or scan (CAT, MRI etc.) images. The BPCS approach presented here outperforms the current state-of-the art in high capacity steganography, both in terms of data hiding capacity and in terms of robustness of the encoding mode.

References

[1] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010, PP 19-23.
[2] Ronak Doshi, Pratik Jain, Lalit Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012, PP 4634-4638.
[3] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen", IEEE February 1998, PP 26-34.
[4] Ross J. Anderson and Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, May 1998, PP 474-481.
[5] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An overview of image steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa, 2005.
[6] Mehdi Hussain and Mureed Hussain," A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May 2013, PP 113-124.
[7] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier Signal Processing 90 (2010), PP 727-752.
[8] Steve Beaullieu, Jon Crissey, Ian Smith, "BPCS Steganography" University of Texas at San Antonio.
[9] Shrikant S. Khaire, Sanjay L. Nalbalwar, "Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique", ISSN: 0975-5462, 2012 PP 4860-4868.
[10] Eiji Kawaguchi and Richard O. Eason, "Principle and Applications of BPCS-Steganography", Kyushu Institute of Technology, Kitakyushu, Japan-University of Maine, Orono, Maine 04469-5708.
[11] Sheetal Mehta, Kaveri Dighe, Meera Jagtap, Anju Ekre, "Web Based BPCS Steganography" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 2, PP 126-130.
[12] Ms. Pradnya R. Rudramath, M. R. Madki, "High Capacity Data Embedding Technique Using Improved BPCS Steganography" International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012.
[13] Vipul J. Patel, Neha Ripal Soni, "Image Steganography System using Modified BPCS Steganography Method" International Journal of Engineering Research & Technology (IJERT), vol. 3, Issue 6, June-2014, PP 728-730.
[14] B. Ramesh Kumar, K. Suresh, S. K. Basheer, M. Raja Krishna Kumar, "Enhanced Approach to Steganography Using Bitplanes" International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012, PP 5472-5475.
[15] Silvia Torres Maya, Mariko Nakano Miyatake, Ruben Vazquez Medina, "Robust Steganography using Bit Plane Complexity Segmentation" 1st International Conference on Electrical and Electronics Engineering 2004, PP 40-43.
[16] Hioki Hirohisa: A Data Embedding method using BPCS principle with new Complexity measures, in: Proceedings of Pacific Rim Workshop on Digital Steganography, July 2002, PP 30-47.
[17] Rosane English, "Comparison of High Capacity Steganograhy Techniques" International Conference of Soft Computing and Pattern Recognition, IEEE-2010, PP 448-453.
[18] Yeshwanth Srinivasan, Brian Nutter, Sunanda Mitra, Benny Phillips, and Daron Ferris, "Secure Transmission of Medical Records Using High Capacity Steganography" Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems, 2004.
[19] Vipul J Patel, Neha Ripal Soni, "Uncompressed Image Steganography using BPCS: Survey and Analysis" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 15, Issue 4 (Nov. - Dec. 2013), PP 57-64.