STEGANOGRAPHY TECHNIQUE USING MODULUS ARITHMETIC

Sayuthi Jaafar, Azizah A Manaf, Akram M Zeki.
University Technology Malaysia/Malaysian Armed Forces Academy

ABSTRACT

This new technique will use modulus arithmetic to incorporate secret-information into a host-image. Modulus arithmetic is used as the mechanism for embedding and extracting process. Modulus-m operation indicates l-bits of the secret-information can be incorporated into the host-image pixel. This approach works in a fully spatial domain manner, so one need to deliberately observe the spatial characteristic among the pixel distribution in the host-image and the secret-information. Pixels are represented by a decimal value
(0 – 255).

Keywords: data hiding, steganography and modulus

1. INTRODUCTION

Steganography is the art of concealing secret information. It is a method of communication, which hides the existence of the communication from a third party. Cryptography scrambles secret information so that it cannot be understood, but enemy is allowed to detect, intercept and modify the information. In cryptography the presence of an encrypted message is clearly obvious though its meaning is not.

Steganography present another approach to information security. In steganography, data is hidden inside a vessel or container that looks like it contains something else. A variety of vessels are possible, such as digital images, sound clip, and even executable file. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret messages present[1].

2. PRESENT TECHNIQUE

LSB coding is limited to embedding in only the lower bit planes (LSB). This technique can only promise the embedding capacity less than 10% of the host size (12.5% for 8-bit format). Embedding in the higher bit planes increase the embedding capacity, but adds a larger noise component to the value of each pixel. Some published papers discuss about this technique are [2] [3] [4]. There is no specific published paper discussed this in detail, most of them give general idea about the effect on embedding in the higher bit planes. This motivated the researcher to conduct the experiments and survey on the relationship between embedding in the higher bit and the quality of the stego-image.

Instead of substituting the LSB with the secret information bit, Pan et al [5] proposed Chen Pan Tseng (CPT) scheme. This scheme uses the modular arithmetic which is SUM $((F_i \oplus K) \oplus W) \cong b_1 b_2 b_3 \ldots . b_r \pmod{2^r}$. This give an open platform for further modification to suite with the new technique or approach designing new embedding and extracting process.

Differencing method introduced by Wu Tsai [6][7] gave new idea of embedding or extracting technique. The embedding process involve with changing differencing value of the cover image with the differencing value of the secret image if they fall in the same index. This technique is limited to embedding images into another image only . This technique required leading information for the extraction process. The leading information is the index table to record the gray value of each pixel during the replacement process.

3. PROPOSED TECHNIQUE

In this steganography model, the modules are divided into three: Host Image Selection, Secret Message Reconstruction, Embedding and Extracting.

3.1 Host Image Selection

The host-image pixels will be treated as it is (decimal value). The pixel value varies from 0 to 255, means in binary it varies from 00000000 to 11111111. This module will test the host image. The result of this test will give the maximum change permitted. This test is to find the relation between PSNR (Peak Signal to Noise Ration) and the embedding capacity for difference modification on the pixels. In this test, a Test Matrix is required and it composed of random numbers. The random numbers range from [0 , 2^l -1] for different l. The Test Matrix has the same size as the host image. The algorithm and results of the preliminary test is shown in Figure 1 and 2 below:

The results from the preliminary test confirm certain facts:

- Stego-image quality degrade when the capacity increase.
- Difference host image will give difference stego-image quality.
- Difference range of modification on each pixel will produce difference stego-image, where larger range will degrade the quality of the stego-image.
- These results give the motivation to improve the stego-image quality while getting optimum embedding capacity.

3.2 Secret Information Representation

The secret information is treated as a bit string of l-bit segmentation. Every l-bit segmentation can be represented by decimal number. For a bit string with fixed segmentation length l, the corresponding decimal integer is supposed to fall in the range of [0, 2l – 1].

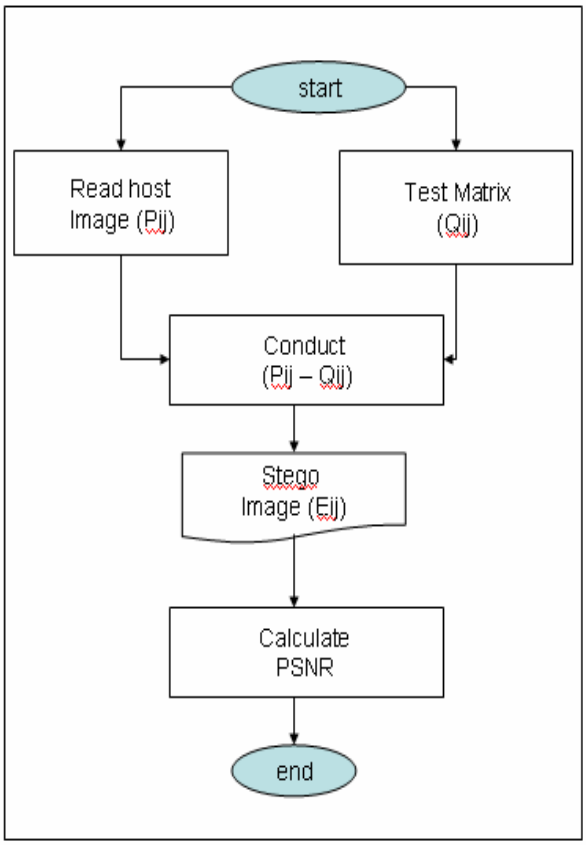

Figure 1: Preliminary Test Algorithm

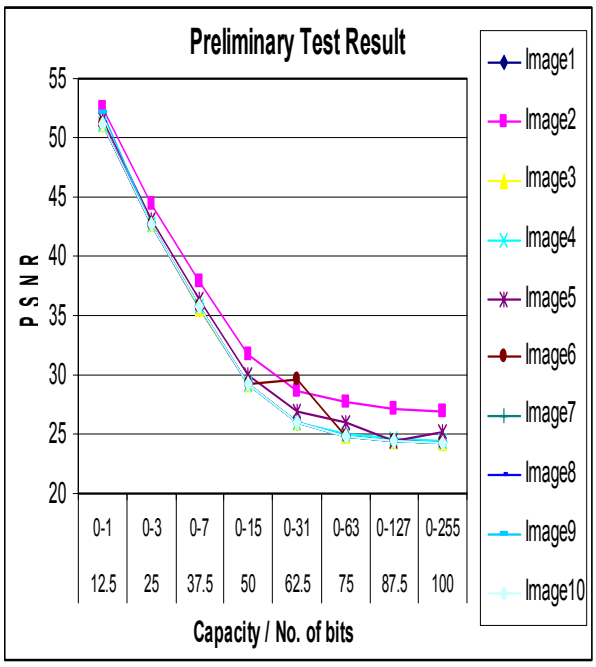

Figure 2: Preliminary Test Result

Therefore if the secret-information is l bit string segmentation, the possible secret-information range is $[0 , (2^l -1)]$ in decimal equivalent.

Example:

If $l = 3$, so the decimal value is from 0 to 7.
If $l = 4$, the decimal value is from 0 to 15.

3.3 Embedding Mechanism

This paper will use modulus arithmetic as a mechanism to do the embedding process, instead of direct substitution as applied in normal LSB technique. The image is read pixel by pixel and the image after the modification is called stego-image. The embedding algorithm is shown figure 3.

Example:

If host pixel value (p_{ij}) is 146, secret information value (s_i) is 4 and conducts a mod-8 operation:

Code generated (from host pixel) is 2, Therefore change the (p_{ij}) value to 148 and it becomes stego-pixel. Now stego-pixel (148) will generate 4 from the mod-8 operation.

Therefore by changing value of p_{ij} from 146 to 148, means we embed 4 into the p_{ij}.

3.4 Extracting Mechanism

Stego-image is read pixel by pixel. Conduct mod-m operation to related pixels. Remainders obtain from the mod-m operation are the secret information segmentation string.

Example:

If stego pixel value (p_i) is 148 and conduct a same mode as embedding process (mod-8). Code generated after doing mod-8 operation is 4.

Stego image pixel 148 obtained code 4, means the segmentation embedded of secret information is 4.

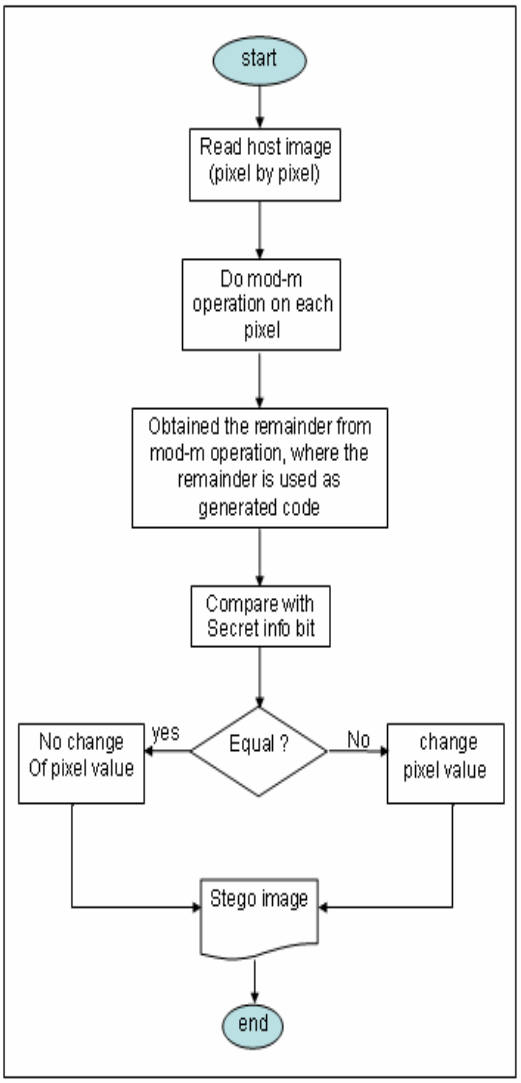

Figure 3 : Embedding Process

4. CONCLUSION

In this paper, the embedding and extracting technique using modulus-m arithmetic operation is proposed. In this paper one also proposed module to test the host image, different host image will give different embedding capacity. Future research is to improve the technique by doing grouping or multiple pixel embedding and extracting.

ACKNOWLEDGEMENT.

The authors express his grateful thanks to Dr Richard Eason, University of Maine, USA and Dr Simon See, ActiveMedia Innovation Sdn Bhd, Malaysia. This research was supported by Universiti Teknologi Malaysia under IRPA Grant – 74249.

References:

[1] K David, *The Code Breakers*, 2nd Edition, Macmillan New York, 1996.

[2] A P Febien Petitcolas, R J Anderson, M G Kuhn, *Information Hiding – A Survey*, Proc of IEEE (USA), vol 87, no 7, pp 1062-1078, 1999.

[3] W Bender, D Gruhl, N Morimotor, and Lu, *Techniques for Data Hiding*, IBM Systems Journal, Vol 35, Nos 3-4, pages 313-336, 1996

[4] N F Johnson, Z Duric, and S Jajodia, *'Information Hiding: steganography and Watermarking – Attacks and Countermeasures'*, Kluwer Academic Publisher. 2001

[5] Y C Tseng, Y Y Chen and H K Pan, *'A Scure Data Hiding Scheme for Binary Images'*, IEEE Transactions on Communication, vol 50, no 8, 2002.

[6] M S Liaw and L H Chen ,*' An Effective Data Hiding Method'*, Proc of IPPR Conference on ' Computer Vision, Graphics and Image Processing', Taiwan ROC, pp 146-153, 1997.

[7] D C Wu and W H Tsai, '*Spatial-domain Image Hiding using Image Differencing'*, IEEE Proc Visual Image Signal Process, Vol 147, no 1, Feb 2000, pp 29-37, 2000.

[8] W Min and L Bede *, 'Data Hiding in Binary Image for Authentication and Annotation'*, IEEE Transactions on Multimedia, vol 6 no 4, 2004.

[9] M Wu, B Liu, *'Data Hiding in Image and Video: Part 1 – Fundamnetal Issues and Solution and Part 2 – Design and Application'*, IEEE Trans Image Processing, vol 12, pp 685-695 and 696-705, 2003.

[10] M Wu, E Tang and B Liu, *Data Hiding in Digital Binary Images*, Proc IEEE Int'l Conference on Multimedia and Expo, New York, 2000.

[11] E Koch, J Zho, *Embedding Roburst Labels Into Image for Copyright Protection*, Proc of Int'l Congress on Intellectual Property Rights for Specialized Information Knowledge & New Technologies, Vienna, 1995.

[12] Piyu Tsai, Yu Chen Hu, Chin Chen Chong, *An Image Hiding Technique Using Block Truncation Coding,* Proc of Pacific Rim Workshop on Digital Steganography 2002, pp 55-64, 2002.

[13] R Eason, *'A Tutorial on BPCS Steganography and Its Application'*, Department of Electrical and Computer Engineering, University of Maine, 1998.

[14] E Kawaguchi, R Eason, *Principle and Application of BPCS-Steganography'*, SPIE's International Symposium on Voice, Vidoe and Data Communication, 1998.

[15] R Eason, E Kawaguchi, *'Depth-First Coding for Multi-valued pictures using bit-plane Decomposition'*, IEEE Trans. On Comm., vol 43, no 5 pp 1961-1969, 1995.

[16] H Wang, S Wang, *Cyber Warfare: Steganography vs Steganalysis*, Communication of the ACM, vol 47, 2004.

[17] R J Anderson, *'Stretching the limits of Steganography'*, in Information Hiding, Springer Lecture Notes in Computer Science, vol 1174, pp 39-48, 1996.

[18] N F Johnson and S Jajodia, *'Steganography: Seeing the Unseen'*, IEEE Computer , pp 26-34, 1998.

[19] Peter Wyner, *Disappearing Crytography, Information Hiding : Steganography & Watermarking,* 2nd Edition, Morgan Kaufman Publishers, 2002