The Eighth International Workshop on Image Media Quality and its Applications, IMQA2016
March 10-11, 2016, Nagoya, Japan

A NOVEL STEGANOGRAPHY USING HILL CIPHER AND MICROARRAY IMAGES

Chaur-Chin Chen and Chin-Kuang Chen

National Tsing Hua University
Institute of Information Systems & Applications
101 Kwan-Fu Road, Sec. 2, Hsinchu, Taiwan 30013

ABSTRACT

Most of the Internet users either satisfy or ignore the current security and privacy of communication over network transmission until their information are misused or stolen. On the other hand, the costs of storage space and computational speed are both significantly reduced and the bandwidth of network is sufficient enough to transmit an image that recalls the adoption of an ancient methodology, steganography, to serve as an act of covert communication.

This paper implements a simple and secure data hiding system by means of a Hill cipher and microarray image templates based on a novel steganography flowchart. This scheme posseses two distinguished properties: (1) a secret message in a text format is first encrypted by a Hill cipher of order 4 to raise a security level, (2) the cover image is generated based on an artificial microarray image template or other mathematical models. The advantage is that we can easily generate a cover image (gray or color) to meet the various sizes of secret messages. An experiment of embedding a secret message of an article *falls.txt* into a 576×896 color microarray image template shows that a stego image and a cover image cannot be distinguished by naked eyes.

This work is supported by Taiwan MOST Grants 104-2221-E-007-035 and 104-2221-E-007-096-MY2.

1. INTRODUCTION

Data hiding [3, 5, 11] plays an important role of the Internet era when most people rely it to do information broadcast and mass communication in the daily life. Stegonography, an ancient technique which embeds secret message into a cover media to protect the data, is widely studied during the past two decades [6, 7, 8, 12] due to the cost of storage space is significantly reduced while the comunication network speed is significantly increasing. Although steganography using JPEG compressed images based on discrete cosine transform (DCT) [8, 9, 12] as cover images are widely studied, the techniques concentrate on the usage of very low frequency positions of quantized DCT coefficients so that the capacity of embedding the secret message is relatively low compared with the cover image size. Thus motivated, this paper aims to provide a simple, secure, and practical steganography system based on a flowchart [5] as depicted in Figure 1. This novel framework has two distinguished properties: (1) a secret message in a text format is first encrypted by an encryption algorithm such as Hill ciphers to raise a security level, (2) a cover image can be generated based on mathematical models or user provided algorithms to meet the size request of the secret message. An artificial microarray image template [4] and Markov random field

textures [5] are two typical cover images.

This work provides a practical user-friendly embedding and extracting software for secret message transmission between users by encrypting a secret mesage (plaintext) by a Hill cipher, embedding the ciphertext into the blue signal of a color RGB image selected from microarray image templates, and recovers the original secret message from the stego image. Experiments show that a stego image and its corresponding cover image looks alike (Naked eyes cannot distinguish them) and the hidden message can be completely extracted.

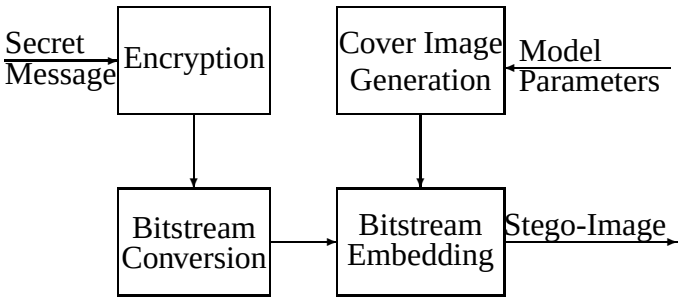


Fig. 1. A Novel Flowchart for Data Hiding.

2. COVER IMAGE SELECTION FROM MICROARRAY IMAGE TEMPLATES

Microarrays are widely adopted for simultaneously investigating gene expression in a number of diseases such as adenocarcinoma, colon cancer, and lymphoma and etc. [1, 2] A microarray is in general a glass or polymer slide onto which DNA molecules are attached at fixed locations called spots. The resolution of a microarray image is usually 1000 pixels per centimeter. In the beginning of biological experiments of hybriding dyed normal genes and dyed tumor genes, researchers should design or prepare a micorarry image template for their studies [4]. A typical small microarray image used in a research Lab shown in Figure 2(a) will be used as our cover image. This color cover image has 576 pixels in height and 896 pixels in width.

3. HILL CIPHER AND DATA ENCRYPTION

3.1. Hill Cipher of Order 4

A Hill cipher [10] is an encryption method based on a matrix multiplication under some modular arithmetic. In our experiment, we assume that our secret message is a text composed of general ASCII characters including EOL, EOF, space, and etc. We adopt a Hill cipher of order 4 under mod p=127. Such a Hill cipher can be specified by a 4×4 matrix *H*, whose inverse matrix under modulo $p = 127$ is denoted as *G*. An example of the matrices *H* and *G* are listed as follows.

$$H = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 3 & 2 & 4 & 6 \\ 5 & 4 & 3 & 2 \\ 7 & 6 & 2 & 9 \end{bmatrix}, \; G = \begin{bmatrix} 119 & 85 & 27 & 0 \\ 85 & 61 & 4 & 104 \\ 27 & 4 & 4 & 46 \\ 0 & 104 & 46 & 104 \end{bmatrix}$$

3.2. Data Encryption

Suppose that a message consists of characters whose ASCII code is from 0 to 127, for example, a message of four characters 'cake' can be represented as a 4-dimensional vector $\mathbf{x} = [99, 97, 107, 101]^t$, then the Hill ciphertext under modulo $p = 127$ becomes $\mathbf{y} = H\mathbf{x} = [108, 1, 9, 112]^t$. We further partition each number of the ciphertext into a number of most significant 4 bits and another number of least significant 4

bits. That is,

$$\begin{aligned}\mathbf{y}^t &= [108,\ 1,\ 9,\ 112] \\ &= [(0110\ 1100), (0\ 1), (0\ 9), (0111\ 0000)] \\ &= [(6\ 6),\ (0\ 1),\ (0\ 9),\ (7\ 0)]\end{aligned}$$

The 4-bit numbers 6,6,0,1,0,9,7,0 are then sequentially embedded into the least significant four bits of each pixel in the *blue signal*. In a microarry image template or a real microarry image, the blue channel is generally not used, therefore, we have never changed any important contents in embedding.

4. EXPERIMENTAL RESULTS

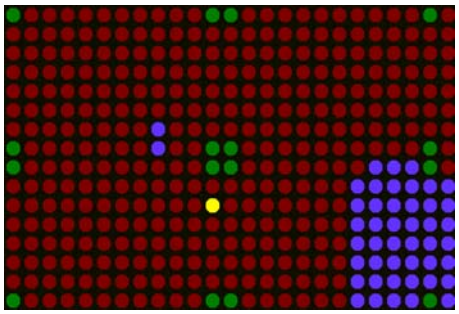
There are three major programs: *gen384.c, ench4.c, dech4.c* [15] required to implement our proposed steganography system. The results of embedding a travel recommendation article *falls.txt*]citeWeb02 into a microarrqay image template is shown in Figure 2(b). A cover image and the corresponding image are listed as in Figure 2. Naked eyes cannot distinguish a stego image from the cover image with a secret message (a text article: *falls.txt* [14] whose contents are listed below) consisted of 20 lines and 1203 characters being embedded.

Experience The Niagara Falls

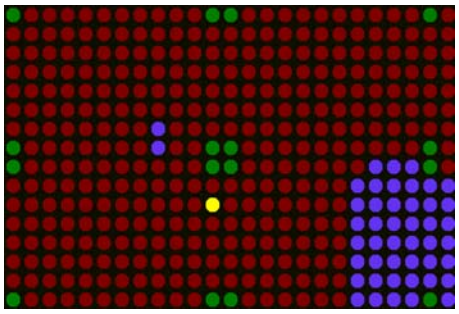
The New Niagara Falls, Canada-with eclectic restaurants, contemporary hotels, and electrifying attractions-is a true Canadian vacation destination for couples and families alike. Grown ups have upscale hotels, modern casinos, nightlife and concerts, fine dining, golf courses and spas, and wine country is just down the road. For children, Niagara Falls is a veritable theme park with ultra tall buildings (Skylon Tower), water parks inside hotels, Ferris wheels and kid-friendly restaurants (Clifton Hill), and we even sneak in some education at Niagara Falls attractions like the Butterfly Conservatory and Marineland. Let's not forget the Falls. From the Maid of the Mist to Journey Behind the Falls, there are plenty of ways to experience this great wonder of the world.

Situated just 20 minutes from Buffalo International Airport and an hour from the Toronto area, a Niagara Falls vacation is easy to get to and fun to plan. Use the Vacation Planning tools on our site to help you choose your Niagara Falls hotels and attractions and pull together the perfect itinerary.

Start your trip at Niagara Falls Tourism. We'll introduce you to this new Ontario vacation destination!



(a) Cover Image



(b) Stego Image

Fig. 2. Cover Image and Stego Image.

5. CONCLUSION

This paper propses a practical user-friendly steganographic system for data hiding based on using a Hill cipher encryption and a microarray

image template. Three major programs written in ANSI C programs [15] are used to implement this system: (a) gen384.c is used to provide a microarray image template as a color cover image; (b) ench4.c is used to do data encryption and embedding based on Hill ciphering; (c) dech4.c is used to recover the message. A Hill cipher matrix of order 4, H, should be provided when running *ench4.c* and its inverse matrix under modulo $p = 127$, G, should be off-line preprocessed before running *dech4.c*. By inspecting a cover image and its corresponding stego image, people cannot distinguish them. The current program only works for plaintext files, a future research of extending this work for hiding other file formats such as word, excel, and pdf formats merit further studies. Implementations using Matlab programs and tools are also recommended [13].

6. REFERENCES

[1] A.A. Alizadeh et al., "Distinct types of diffuse large B-cell lymphoma identified by gene expression profiling," *Nature*, vol. 403, 503-511, 2000.

[2] U. Alon et al., "Broad Patterns of Gene Expression Revealed by Clustering Analysis of Tumor and Normal Colon Tissues Probed by Oligonucleotide Arrays," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 96, no. 12, 6475-6750, 1999.

[3] C.K. Chan and L.M. Cheng, "Hiding Data in Images By Simple LSB Substitution," *Pattern Recognition*, vol. 37, 469-474, 2004.

[4] C.C. Chen, C.Y. Kao, C.F. Chang, H.T. Chu, and C.N. Chen, "Simple Software for Microarray Image Analysis," *IEEE Proceedings of Computer and Robot Vision*, Pid163, Quebec City, Canada, 2006.

[5] C.C. Chen and W.J. Lai, "High-Capacity Steganography Using MRF-Synthesized Cover Images," *Annual Conference on Engineering and Information Technology*, 237-242, Chiyoda, Japan, March 28-30, 2014.

[6] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *IEEE Computer Magazine*, vol. 31, no. 2, 26-34, 1998.

[7] C.L. Liu and S.R. Liao, "High-Performance JPEG Steganography Using Complementary Embedding Strategy," *Pattern Recognition*, vol. 41, 2945-2955, 2008.

[8] N. Provos and P. Homeyman, "Hide and Seek: An Introduction to Steganography," *IEEE Security & Privacy*, vol. 1, no. 3, 32-44, 2003.

[9] W.B. Pennabaker and J. Mitchell, "JPEG Still Image Compression Standard," *New York: Van Nostrand Reinhold*, 1993.

[10] D.R. Stinson, "Cryptography Theory and Practice," *3rd. ed., Chapman & Hall/CRC*, 2006.

[11] A. Westfeld, "F5 - A Steganography Algorithm: High Capacity Despite Better Steganalysis," *International Workshop on Information Hiding*, Berlin, vol. 2137, 289-302, 2001.

[12] http://en.wikipedia.org/wiki/Steganography, *last access on January 22*, 2016.

[13] http://www.mathworks.com/products/matlab, *last access on January 22*, 2016.

[14] http://www.cs.nthu.edu.tw/∼cchen/Textdata/falls.txt, *last access on January 22*, 2016.

[15] http://www.cs.nthu.edu.tw/∼cchen/IMQA2016, *last access on January 22*, 2016.