HIDDEN COMMUNICATION IN FREQUENCY DOMAIN FOR INFORMATION EXCHANGE

F. Gönül Toz [a], H.M. Palancıoğlu [b], E. Beşdok [b]

[a] ITU, Civil Engineering Faculty, 80626 Maslak Istanbul, Turkey - tozg@itu.edu.tr
[b] Erciyes University, Engineering Faculty, Geodesy and Photogrammetry Dept., Kayseri, Turkey, (hpalanci ,ebesdok)@erciyes.edu.tr

Commission VI, WG VI/4

KEY WORDS: Spatial Information Sciences, Technology, Application, Data Mining, Pixel, and Theory..

ABSTRACT:

In last decade, Geoinformatic products such as geo-maps and aerial photos have been shared over the Web. The Web technologies have been employed in providing geo-information exchange. Today, there is a need to employ efficient tools such as Steganography to save copyrights of producers and prevent the *unauthorized users* from non-public geoinformation. In this paper, we propose a new method of hiding colored geo-images within gray scale images using Steganography methods.

1. INTRODUCTION

Cartography is the science of making maps. Though hand-drawn cartography is still prevalent, traditional drafting is being rapidly replaced by computers and graphics software, which allow maps to be created quickly and accurately. Complex geo-maps are made with sophisticated scanning equipment, while simpler geo-maps can be drawn on a personal computer. Generally, cartographers begin with a grid such as the latitude and longitude to which they add such information as streets, population density, and physical features. Many cartographers are employed by the governments around the world to make geo-maps for various *purposes*. Some of the geo-maps have been prepared for only *authorized users*. The Army Forces also employ cartographers for *private purposed* geo-map making. There are many companies making and selling all kinds of geo-maps from subsurface geo-maps to geo-thematic maps. In some countries, some kind of geo-maps such as *militarial geo-maps* or *subsurface mine geo-maps* have been prohibited to produce and use by unauthorized users. All public and private organizations have to secure their geoinformation based products in order to control their commercial market or rights. However, when they have to share some *geoinformations* over communication cannels such as over Web, some undesired and unsafe conditions could appear. The shared geoinformation should be hidden within a desired *container signal* such as images or audios in order to provide secure communication process.

Steganography (Derrick 2001, Gruhl 1998, Anderson 1996, Anderson 1998, Arnol'd 1992, Cachin 1998, Chang 1997, Csiszar 1978, Currie 1996, Tsai 2002, Dijk 1997, Ettinger 1998, Kahl 1996, Kurak 1992, Menezes 1997, Mittelholzer 2000, Ptzmann 1996) is the art of hiding the existence of a message. The word Steganography comes from the Greek words *steganos* (*secret*) and *graphy* (*writing*). An example could be a letter written with two different inks. When the letter is submerged in water one of the inks dissolves while the other remains on the letter, thus revealing the secret message. The original message on the letter is just a cover to hide the existence of the secret message. Steganography is hiding the very existence of communication. One famous example of early steganography is that of Herodotus who shaved the head of one of his slaves and tattooed a message on his head. After his hair had re-grown, he was sent to deliver a message to instigate a revolt against the Persians. Steganography has a wide range of forms from hiding messages in the soles of shoes to hiding messages in musical scores.

Steganography is sometimes confused with cryptography. *Cryptography* (Menezez 1997, Schneier 1994) is the art of concealing the contents of a message (encryption) whereas Steganography is the art of hiding the existence of a message. The message can be any type of digital information including a simple text file, a JPEG image, or any other type of file. Much of the available software that embeds steganographic content into a host file often employs cryptography as well. This greatly adds to the complexity and difficulty of retrieving concealed content.

One of the earliest examples of cryptography was used by Julius Caesar (Kahl 1996) when he sent military messages to his armies. Perhaps since that time, people have also tried to decode encrypted messages. Allies in World War II were able to break a secret German code called Enigma. This discovery enabled Allied forces to locate and sink many German U-boats. Moreover, they were able to obtain advanced information about German military operations that was critical to the campaign in Europe. Similar code-breaking abilities also allowed the United States Navy to intercept the Japanese fleet in one of the most decisive battles in the Pacific--The Battle of Midway. These are just a few examples of how cryptographic technology has played an important role in history (Kahl 1996).

Watermarking (Derrick 2001) is often discussed alongside Steganography. It is similar to Steganography because extra information is kept embedded in the image. Sometimes a watermark is visible and sometimes it is invisible. Watermarking is widely used to protect intellectual property. Whereas Steganography seeks to go unseen and undetected, watermarks seek to be robust (difficult to remove). Many

photographers and studios use watermarking techniques in an attempt to protect their intellectual property.
Still *satellite* or *geo-images* are all easily copied and illegally distributed causing the authors to lose out on considerable income in royalties. By embedding information in a file, watermarking software enables authors to control the distribution of and to verify ownership of their digital information. There are numerous steganography tools available on the Internet and elsewhere. The large number of steganography programs available also adds complexity to the task of recovering the hidden data from a file presumed to contain steganographic content.

The rest of the paper is organized as follows: The Steganography and Steganographic systems are summarized in Section 2. The proposed method explained in detail in Section 3 and some of the experiments are given in Section 4. The results and conclusions are given in Section5.

2. STEGANOGRAPHIC METHODS

Steganography simply takes one piece of information and hides it within another. Computer files such as *images* and *audio-files* contain unused spaces or insignificant data. Steganography takes advantage of these spaces by replacing them with information that is required to hide. The files can then be exchanged without anyone knowing what really lies inside of them. A shared image might contain vitally important geoinformation about the desired position over the world. Steganography and *watermarking* can also be used together to place a hidden *trademark* in images, music files, and software.

Following features of both Steganography and Watermarking methods can be listed.

- A secure permutation key giving exceptional levels of security is used.
- There is no need for additional metadata
- File formats are unaltered and there is no increase to object data file size.
- Digital watermarks do not affect print workflows in any way.
- File transfer times remain unchanged.
- Watermarking can support a host of standard and proprietary formats.
- Embedded messages can survive high levels of data compression.

Within the context of modern computing systems, steganography is the process of hiding secret information within files. Most commonly data is stored within *images*. Images make good hosts for steganographic data due to small changes can be made to the image without a perceivable change in the image characteristics. Other types of digital files also make good steganographic hosts such as *shared movie*, *clip* and *audio* files. Typically hidden data is stored within the least significant bit (LSB) of each block of data. For example, if a digital image were made up of a series of pixels each representing a color from a palette of 2^n colors, each number would represent a shade with a value of 0 to 2^n-1. Changing the shade by one number would not make a noticeable difference to the image. It is in these least significant values that steganographic data can be concealed. Any file format that can withstand variation without greatly compromising the file's integrity is a suitable file format for embedding information. It essentially "copyrights" digital information on geo-images. Steganography makes or read invisible signatures in the image. Certain steganography (Derrick 2001) techniques will also support *change detection*, *data compression*, *integrity checking*, and *integrated metadata*. Change detection lets you know when a feature has been modified. Data compression reduces the space needed to store information. Integrity checking verifies that the data are correctly stored and transmitted. Metadata is information about the data such as how it was developed, processed, projected, and so on.

3. THE DISCRETE COSINE TRANSFORM

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. For example, the DCT is at the heart of the international standard lossy image compression algorithm known as JPEG.

The two-dimensional DCT of an M-by-N matrix A is defined as follows:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} Cos \frac{\pi(2m+1)p}{2M} Cos \frac{\pi(2n+1)q}{2N} \tag{1}$$

and

$$\begin{cases} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{cases} \tag{2}$$

where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & p = 0 \\ \sqrt{\frac{2}{M}} & 1 \le p \le M-1 \end{cases} \tag{3}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & q = 0 \\ \sqrt{\frac{2}{N}} & 1 \le q \le N-1 \end{cases} \tag{4}$$

The DCT is an invertible transform, and its inverse is given by

$$A_{m,n} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{PQ} Cos \frac{\pi(2m+1)p}{2M} Cos \frac{\pi(2n+1)q}{2N} \tag{5}$$

$$\begin{cases} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{cases} \tag{6}$$

$$\alpha_p \alpha_q Cos \frac{\pi(2m+1)p}{2M} Cos \frac{\pi(2n+1)q}{2N} \tag{7}$$

where

$$\begin{cases} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{cases} \tag{8}$$

4. EXPERIMENTS

In this paper, a new method based on DCT has been proposed in order to achieve hidden communication over the communication networks. The experiments conducted on the images given in Figures 1-4. The image given in Fig.1 has been used as cover image and all of the other images have been embedded into the cover image. The success of the hiding process has been evaluated both objectively and subjectively. The well known MSE value has been used as objective evaluation measure for hiding performance. And the given images have been used as objective evaluation measure of the hiding performance of the proposed method.

The information hiding process has been given below step-by-step:

1. Compute the frequency domain coefficients of the cover image by using the DCT with for 8x8 pixels sized unoverlapping blocks.
2. Use the numerical values of lower sub-triangle of the DCT blocks in order to hide message information(s).
3. Recode the message information(s) by using the appropriate tools such as,
    a. Rescaling intensity coding,
    b. Sampling intensity values,
    c. Using block-coding techniques (i.e., run-length coding).
4. Use one of the computationally secure cryptographic methods (i.e., position permuting, color shifting, and vigenerre-image coding) for images in order to increase the security level of the message.
5. Replace the numerical values, which have been determined at Step-3, with the values of the information coefficients, which are still in spatial domain.
6. Send to stego-object to audiences over the communication net.

The proposed method has some advantages and disadvantages that are listed below,

1. The proposed method is a computationally secure; therefore, the minimum size of the cover image determines the level of the security of message information.
2. The proposed method is NOT an information lossless coding technique until audiences uses frequency domain.
3. The information hiding capacity of the proposed method depends on to the methods that are used in Step-3 of the proposed method and inherit specifications of the message information(s) images.
4. The proposed method is not based on the *bit-change method*; therefore it can produce artificial impulses if stego-message converted into spatial domain.

In the experiments, The Fig.2, Fig.3, and Fig.4 message images have been embedded in to first, second, and third band of the message image, respectively. The stego-message image, Fig.5, has been converted into spatial domain for visualization.

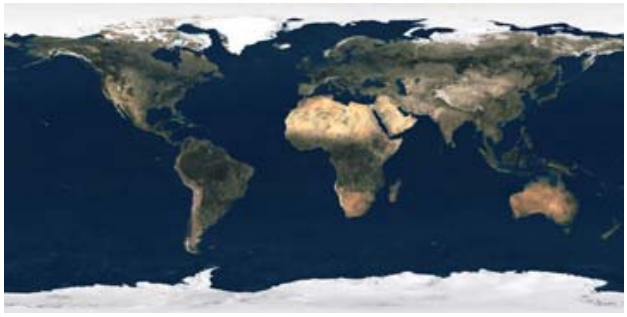

Figure 1: The Earth Image (2400x1200x3 pixels sized).

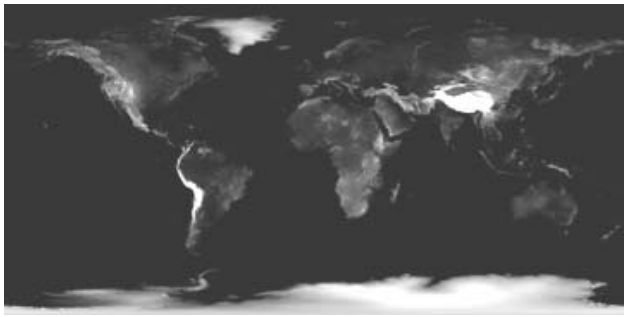

Figure 2: The elevation image of the Earth (2400x1200 pixels sized).

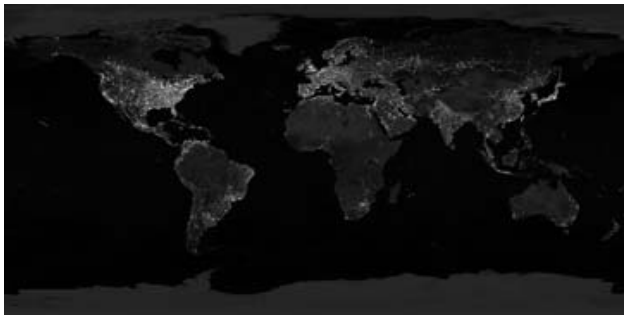

Figure 3: The lights at the night over the Earth image. (2400x1200 pixels sized).

4.1 Image Quality Measures

The well-known image quality measures; Mean Squared Error (MSE), Pearson Correlation Coefficient, and Peak Signal To Ratio (PSNR) have been used in order to objectively evaluate the performance of the proposed method. The quality measure of PSNR is defined with;

$$\text{PSNR}=10\ \log_{10}\left(\frac{{I_{\max}}^2}{MSE}\right)\text{dB} \tag{9}$$

where $I_{\max}$ is equal to 255 for 8 bit gray scale images. The MSE is calculated by using the Eq. (2) given below:

$$\text{MSE}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(Y_{i,j}-S_{i,j})^2 \tag{10}$$

Where M and N denote the total number of the pixels in the horizontal and the vertical dimensions of the image. $S_{i,j}$ represents the pixels in the original image and $Y_{i,j}$ represents the pixels of the stego-image (Chang 1997). Pearson Correlation Coefficient (Corr) is given by;

$$Corr = \frac{\sum\sum (S - \overline{S})\ (Y - \overline{Y})}{\sqrt{\sum\sum (S - \overline{S})^2 \sum\sum (Y - \overline{Y})^2}} \qquad (11)$$

where $\overline{S} = \frac{\sum\sum S}{M\,N}$.

Figure 4: The Sea Mask image (2400x1200 pixels sized).

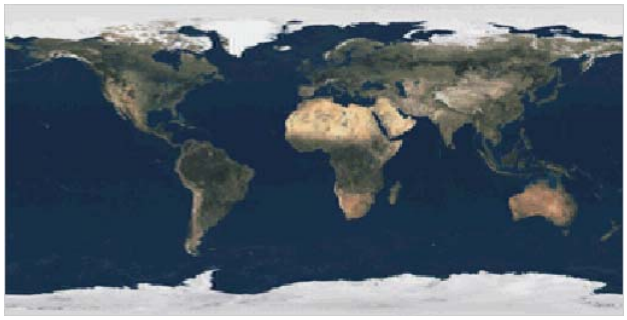

Figure 5: Stego-Image.

Table 1: Objective measure values between Message image and Stego-Image.

MSE	Corr	PSNR
118.866	0.999	27.380

5. RESULTS

Providing data security in spatial information systems has became an important subject due to the widespread use of the communication networks. The use of stenography in spatial information systems provides the following uses:

- Protecting Copyright Infringement of IDs.
- Storing additional data without changing file structures and sizes of the IDs.
- Providing opportunity to develop defense information system applications with high security.
- Storing additional thematic data to the ID without additional space.
- Providing high security in digital geoinformation exchange.
- Providing the security of the multi-level ID by encrypting the data for unauthorized user accessibility.

6. REFERENCES

G., Derrick, (2001), Data watermarking steganography and watermarking of digital data, *Computer Law & Security Report*, 17 (2), 101-104.

D., Gruhl, W., Bender, (1998), Information hiding to foil the casual counterfeiter, Second *International Workshop on Information Hiding*, IH'98, Portland, Oregon, 1-15.

R.J. Anderson, (1996), Stretching the limits of steganography, *Information Hiding: First International Workshop*, 39-48.

R.J., Anderson, F.A.P. Petitcolas, (1998), On The Limits of Steganography, *IEEE Journal of Selected Areas in Communications*, 16 (4), 474-481.

V.I. Arnol'd, (1992), Catastrophe theory, *Springer-Verlag*, Berlin.

C. Cachin, (1998), An information-theoretic model for steganography, *Second International Workshop, Lecture Notes in Computer Science*, 1525, 306-318.

L. Chang, I. S. Moskowitz, (1997), Critical analysis of security in voice hiding techniques, *Information and Communications Security: First International Conference, Lecture Notes in Computer Science*, 1334, 203-216.

I. Csiszar, (1978), Broadcast channels with condential messages, *IEEE Transaction on Information Theory*, 24 (3), 339-349.

D.L. Currie, C.E. Irvine, (1996), Surmounting the effects of lossy compression on steganography, *In National Information System Security Conference*, Baltimore, MD, 194-201.

C. S. Tsai, C.C., Chang, T.S., Chen, (2002), Sharing multiple secrets in digital images, *The Journal of Systems and Software*, 64, 163–170.

M.V., Dijk, (1997), On a special class of broadcast channels with condential Messages, *IEEE Transactions on Information Theory*, 43 (2), 712-714.

J.M., Ettinger, (1998), Steganalysis and game equilibria, Information Hiding: Second International Workshop, *Lecture Notes in Computer Science*, 1525, 319-328.

D. Kahn, The history of steganography, (1996), Information Hiding: *First International Workshop, Lecture Notes in Computer Science*, 1174, 1-6.

C., Kurak, J., McHugh, (1992),onary note on image downgrading, *In Computer Security Applications Conference, San Antonio*, TX, USA, 153-159.

A.J., Menezes, P.C.V., Oorschot, S.A., Vanstone, (1997), Handbook of applied cryptography, CRC Press, Florida.

T. Mittelholzer, (2000), An information-theoretic approach to Steganography and Watermarking, *Information Hiding: Third International Workshop, Lecture Notes in Computer Science*, 1768, 1-16.

B. Ptzmann, (1996), Information hiding terminology, Information Hiding: *First International Workshop, Lecture Notes in Computer Science*, 1174, 347-350.

B. Schneier, (1994), Description of a new variable-length key, 64-Bit block cipher, Fast Software Encryption, *Cambridge Security Workshop Proceedings, Lecture Notes in Computer Science*, 809, 191-204.

C.E., Shannon, (1949), Communication theory of secrecy systems, *Bell System Technical Journal*, 28, 656-715.