ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A New Steganography Algorithm for Image Hiding using Gödelization Under Frequency Domain

B.V.Ramadevi
Research Scholar, Department of CS&SE
AUCE(A), Andhra University,
Visakhapatnam,India
bvramadevi@yahoo.com

D.Lalitha Bhaskari*
Associate Professor, Department of CS&SE
AUCE(A), Andhra University
Visakhapatnam,India
lalithabhaskari@yahoo.co.in

P.S.Avadhani
Professor, Department of CS&SE
AUCE(A), Andhra University
Visakhapatnam,India
psavadhani@yahoo.com

Abstract: Steganography, known as the art of hiding information, is a means of embedding data within another data while protecting its secrecy. The proposed method in this paper focuses on hiding the data(image) under frequency domain making use of Modulation technique, which embeds the secret data in the DCT domain of the cover image to increase the robustness of the scheme against JPEG compression. To enhance the security, the secret data is encoded using a technique called Gödelization and compressed using Alphabetic Coding techniques. The encoded compressed data which is obtained is embedded into the DCT domain of the cover image. The proposed methodology is proved to be secure and is resistant to JPEG attacks.

***Keywords*:**Discrete Cosine Transform, Frequency Domain, Gödelization, Alphabetic Coding, Steganography.

I. INTRODUCTION

Steganography, as defined by Kahn[1], is "the art and science of communicating in a way which hides the existence of the communication". Technically speaking, steganography is a covert communication technology, which allows secret information to be embedded into a cover /host message without significantly damaging the content of the cover message. The message usually will be an image and the secret information which is to be embedded is called the stego message. According to their applications, steganography techniques could be roughly divided into two categories: Digital fingerprinting and Digital watermarking. Digital watermarking[2] focuses on the embedding algorithms and serves for the purposes such as copyright protection, authentication, and integrity verification, etc. The hidden information namely watermark in digital watermarking is relatively simple, e.g. a digital signature of the owner or a random pattern generated with a secret key. The main difference between steganography and watermarking is that watermarking techniques are robust when compared to steganographic techniques[8]. The main objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. In simple words, Steganography means hiding one piece of data within another. Usually the cover media will be either image/ text and the secret message can be either text, image or audio. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements-

A. The cover media(C) that will hold the hidden data
B. The secret message (M), may be plain text, cipher text ,image or audio.
C. The stego function (Fe) and its inverse
D. An optional stego-key (K) or password may be used to hide and unhide the message.

The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (S). Steganography and Cryptography are great partners in spite of functional difference. It is a common practice to use cryptography with steganography but cryptography[3] should not be confused with steganography as both have their own merits and demerits.

[a] Modern techniques of Steganography

The common modern technique of steganography exploits the property of the media itself to convey a message. The following media are the candidates for digitally embedding messages[7]. They are Plaintext, Still imagery, Audio,Video and IP datagram.

[b] Plain Text Steganography:

In this technique the message is hidden within a plain text file using different schemes like use of selected characters, extra white spaces of the cover text etc.

[c] Still Imagery Steganography:

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum.

© 2010, IJARCS All Rights Reserved

***[d] Audio & Video Steganography*:**

In audio slight altering of binary sequence of the corresponding audio steganography, secret message is embedded into digitized audio signal which result file. There are several methods are available for audio steganography.

[e] IP Datagram:

This is another approach of steganography, which employs hiding data in the network datagram level in a TCP/IP based network like Internet. Network Covert Channel is the synonym of network steganography. Overall goal of this approach to make the stego datagram is undetectable by Network watchers like sniffer, Intrusion Detection System (IDS) etc[11]. In this approach information to be hidden is placed in the IP header of a TCP/IP datagram. Some of the fields of IP header and TCP header in an IPv4 network are chosen for data hiding.

In this paper we have chosen the approach of still imagery steganography[9] where in we chose to embed an image into a cover which is also an image. Initially we have chosen the cover image to be a gray scale image and the secret image also to be a gray scale image but of smaller size then the cover image.

II. ISCRETE COSINE TRANSFORM

According to literature survey, embedding of secret data into the digital images can be done in two domains. One is spatial domain where the intensity values(pixels) of the image are manipulated and data is hidden in the intensity values of the images. The second method is frequency domain where the frequency components of the digital images are considered. The secret data is embedded into the frequency components of the image. It is observed that spatial domain manipulations are easy when compared to frequency domain, yet frequency domain provides more security when compared to spatial domain techniques. So in this paper, frequency domain is chosen as the media and discrete cosine transforms (DCT)[5,10] are considered. The discrete cosine transform helps to separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform where it transforms a signal or image from the spatial domain to the frequency domain as shown below.

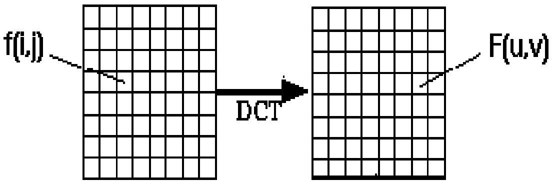


Figure 1. DCT Encoding

In the above figure, f(i,j) i.e., the pixel value of the image in spatial domain is transformed into F(u,v) in the frequency domain after applying DCT. The general equation for a 1D (N data items) DCT is defined by the following equation:

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] f(i)$$

and the corresponding inverse 1D DCT transform is simple $F^{-1}(u)$,where

$$\Lambda(i) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

The general equation for a 2D (N by M) image DCT is defined by the following equation:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

and the corresponding inverse 2D DCT transform is simple i.e. $F^{-1}(u,v)$ where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

DCT is similar to the Fast Fourier Transform (FFT), but can approximate lines well with fewer coefficients.

III. ROPOSED METHOD

The proposed method in this paper follows a three step procedure as given below:

[a] The secret data is transformed into strings of Gödel numbers(GNS) using Gödelizaton technique[6], the size of each string obtained after Gödelization is compressed using the proposed alphabetic coding (AC) technique[6] which encodes the string like run length encoding scheme.

[b] The encoded compressed string now is embedded into a cover image Middle-band Coefficient Exchange[4] encoding process.

[c] The output is a stego image and a string termed as ‘key’ which is of fixed length of 256 bits. The sender transmits the stego image and the key alone is again transmitted via any public key encryption algorithm[3].

[d] At the decoding end, the receiver receives the key and the stego image and follows the inverse process of embedding and obtains the secret data.

The proposed scheme for embedding the data is depicted as follows in figure 2.

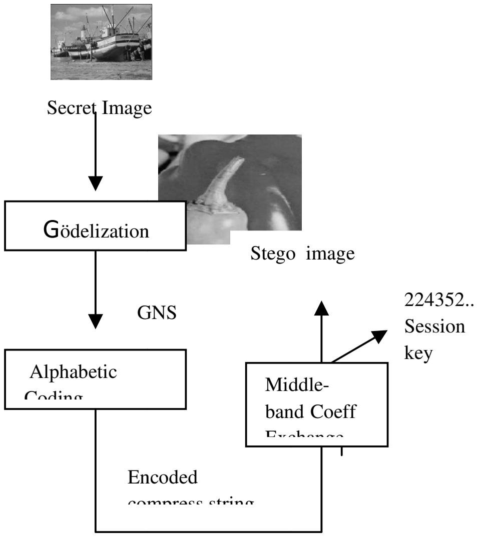


Figure 2. Embedding data

The secret image or data which is the input, is converted into Gödel number string(GNS) through the process of Gödelization[6] which is explained later. This string is then converted into an encoded string through alphabetic coding technique and later this encoded compressed string is embedded into the original image by using the Middle-band Coefficient Exchange method[4]. After this process the output will be a stego image and a key which is a number array is required at the receiver end for decoding process. The key (array) is then transmitted using any public key encryption algorithm (like RSA encryption algorithm). At the decoding end, based on the key the stego image is read and the values are retrieved according to the decoding algorithm for Middle-band Coefficient Exchange method. The output will be a compressed string, for which reverse alphabetic coding is applied to obtain Gödel string. After obtaining the Gödel string, reverse Gödelization is applied to obtain the values of the secret data and then the image is reconstructed at the receiver's end.

A. Gödelization & Alphabetic Coding Techniques

In the proposed Gödelization method the intensity values at a point f(x,y) in the image are transformed into the power of its primes. Consider a pixel value 198 which can be factorized as $2^1\times3^2\times11^1$. The Gödel number sequence of 198 = GN (1,2,0,0,1). The sequence 1,2,0,0,1 can be encoded as $2^1\times3^2\times11^1$ as GN(0) = 2, GN(1)=3,GN(2)=5 and so on. Now here the maximum gray level we can have is 255 which can be factorized as $5^1\times3^1\times17^1$ and the sequence is GN (0,0,1,0,0,0,1). These sequences are stored in an array and each sequence is separated by a special character apart from these numbers where the special character acts as the delimiter. This will help us at the decoding end. The second part is, the Gödel string obtained from the above said procedure is again encoded using AC technique. The main idea of using this technique is to reduce the length of the string obtained in the first step. As we have a sequence of more 0's and 1's in the string, we represent 0's with 'A' , 1's with 'B' , 2's with 'C' and so on. If we encounter more than 3 same characters then we represent as the number of occurrences first and then the character. So the string 0110001000$1200100000$0000100010$ becomes ABB3AB3A$BC2AB5A$4AB3ABA$.

The length is reduced to 25 from 33.With AC technique the length is reduced as well as second level of security is also provided. After this the string obtained from AC technique is embedded into the host image using Middle-band Coefficient Exchange method which is a method under frequency (DCT domain) domain.

B. iddle-band Coefficient Exchange Method

This method in the frequency domain is based on modulating the relative size of two DCT coefficients within in one image block. During encoding process, the sender splits the cover-image in 8*8 pixel blocks; each block encodes exactly one secret message bit. Before the communication starts, both sender and receiver have to agree on the location of the two DCT coefficients, which will be used in the embedding process; let us denote these two coefficients by (u1,v1) and (u2,v2). One block encodes a "1", if B_i (u1,v1) > B_i(u2,v2), otherwise a "0". In the encoding step, the two coefficients are swapped if their relative size does not match with with the bit to be encoded.

To decode the data, by comparing the two coefficients of block, the information can be restored.

[a] Steps in the Middle-band Coefficient Exchange encoding process

```
Step 1: for i=1,…,(M) do
Step 2: choose one cover-block $b_i$
Step 3: $B_i$=D{$b_i$}.
Step 4: if mi=0 then
          If $B_i$ (u1,v1) >$B_i$ (u2,v2) then
          Swap $B_i$ (u1,v1) and $B_i$ (u2,v2).
          End if.
Step 5: else
          If $B_i$ (u1,v1) < $B_i$ (u2,v2) then
          Swap $B_i$ (u1,v1) and $B_i$ (u2,v2).
          End if.
Step 6: Adjust both values so that $|B_i (u1,v1)-B_i (u2,v2)| > x$.
Step 7: $b_i' = D^{-1}\{B_i\}$
Step 8:End for.
Create stego-image out of all $b_i'$.
```

[b] Steps in the Middle-band Coefficients Exchange decoding process (Key)

```
Step 1: for i=1,…,l(M) do
Step 2: using key get cover-block associated with bit i
Step 3: $B_i$=D{$b_i$}.
Step 4: if $B_i$ (u1,v1)<=$B_i$ (u2,v2) then
          $m_i$=0 else $m_i$=1 end if
Ste 5: end for
```

The above technique is widely used and is effective for embedding data under frequency domain.

C. Decoding Process

The decoding process is as follows:

Step1) Once the key and the stego image are received, the receiver retrieves the data from the key which is obtained while embedding process.

Step2) Apply reverse Alphabetic coding on the obtained data. The result of this step is a string in encoded form.

Step3) Apply reverse Gödelization process to obtain the data in its original form.

Step4) Reconstruct the image from the data obtained in step 3.

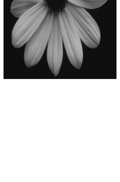
IV. RESULTS FOR EMBEDDING

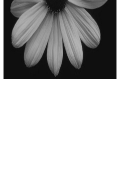
The proposed algorithm is implemented on a set of 50 images and few results are shown below. The algorithm proves to be efficient as there is no perceptual difference between the cover image and the stego image.

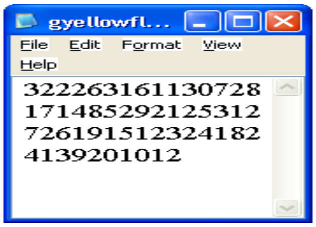
A. Testcase1:

Here the size of the cover image is 1024 x 1024, the size of secret image is 28 x 28 and the size of the stego image is 1024 x 1024.

Cover image Secret image Stego image







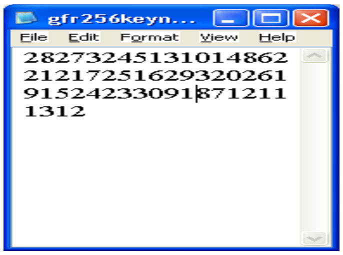
```
322263161130728
171485292125312
726191512324182
4139201012
```

Key File for test case 1

B. Test Case 2:

Here the size of the cover image is 256 x 256, the size of secret image is 8 x 8 and the size of the stego image is 256 x 256.

Cover image Secret image Stego image



```
28273245131014862
21217251629320261
91524233091871211
1312
```

Key file for test case 2

V. CONCLUSIONS & FUTURE WORK

The method proposed in this paper is a combination of an encoding scheme termed as Gödelization, a compression technique known as Alphabetic coding. After encoding and compressing the secret data,it is embedded into a cover image using middle band coefficient exchnage algorithm under frequency domain. Later the key and stego image are securely transmitted using any public key transmission algorithm. The results have proved that it is efficient and secure. The proposed methodology has been tested on various test images and the results are very encouraging and effective. Here for each set of cover and secret image a different key is generated and so the key generated for one image cannot be used for any other image except for its corresponding stego image. The length of the key is also fixed. The proposed methodogy can be extended to RGB images under frequency domain as future work where in more informartion can be embedded in all the components of the color image. The security of the algorithm can still be enhanced by increasing the size of the key.

VI. REFERENCES

[1] Kahn. D, ‘ Codebreakers- The Story of secret writing’, The Macmillan Company, NewYork, U.S.A., 1996, pp 1-5.

[2] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., “Information hiding – A survey”, Proc. of IEEE, Vol.87, No.7, 1999, pp.1062-1078.

[3] A.J.Menezes, P. C. Oorschot, S.A.Vanstone ‘Handbook of Applied Cryptography’, Boca Raton, FL: CRC Press, 1996, Available online http://www.cacr.math.uwaterloo.ca/hac/about/chap1.pdf

[4] Stefan Katzenbeisser, F.A. Petitcolas, ‘Information Hiding–Techniques for Steganography and Digital watermarking’, London, Boston: Artech House, 2000, pp 98.

[5] Discrete cosine transform. [online] 2003. Available at http://www.hyperdictionary.com/computing/discrete+cosine+transform

[6] P.S.Avadhani, D.Lalitha Bhaskari, ‘A Blind Scheme Watermarking Technique Using GÖdelization Technique for RGB images under spatial domain’, International Conference on i-warfare (ICIW-2010), Dayton,USA, 8th -9th April 2010, pp 373-377.

[7] Bret Dunbar, ‘A detailed look at Steganographic Techniques and their use in an Open-Systems Environment’, The Information Security Reading Room, SANS Institute, 2002. http://www.sans.org/reading_room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment_677

[8] Anderson, R.J. and Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, 16(4),May 1998, pp 474-481.

[9] Wolfgang, R.B. and E.J. Delp, ‘Watermark for digital images’, Proceeding of the IEEE International Conference on Image Processing, Sep. 16-19, IEEE Computer Society, 1996, pp 219-222.

[10] D. Tzovaras, N. Karagiannis, M. G. Strintzis, ‘Robust image watermarking in the subband or discrete cosine transform domain’ , 9th European Signal Processing Conference (EUSIPCO’98), Greece, 8–11, Sept. 1998, pp 2285–2288.

[11] Alan McCarty, ‘Distributed NIDS: A HOW-TO Guide’, The Information Security Reading Room, SANS Institute, 2002. http://www.sans.org/reading_room/whitepapers/detection/distributed-nids-how-to-guide_1249

© 2010, IJARCS All Rights Reserved