Steganography method based on wavelength for images

İbrahim COŞKUN[1], Gamze DOĞALI[2]

[1]Department of Computer Science, Sakarya University, Sakarya, TURKEY
Email: [1]simcoskun@hotmail.com, [2]gamzed@sakarya.edu.tr

ABSTRACT

In this paper, it is aimed to deal with secure communication problem depends on perceptibility. In data hiding process, imperceptibly is much important issue. Perceptibility measure depends on HVS (Human Visual System) in images, videos. In this case, developing software must be sensitive HVS range. Our method proposes to find appropriate pixels using visible light range's edge for embedding hidden data into cover image. Other methods which use visible light methods have some difficulties. Our method tries to satisfy these difficulties. It is known that color transition is most critic point for HVS's perceptibility. So, in our method, first step is finding appropriate pixels which are near visible light range's edge value. And then these pixels can be use for embedding hidden data into cover image. Thus, secure communication problem depends on perceptibility can solve effectively.

Keywords: *Steganography, Data Embedding, Data Hiding, Visible light Wavelength, Human Vision System*

INTRODUCTION

Steganography is an art of secure communication and the science which achieves hiding communication by embedding hidden data into unsuspecting-looking carriers such as digital still images, video files, audio files etc. Steganography is one of the security methods to save secret information against malevolent people. There are various methods are developed to get secret communication (Fig.1). Steganography and Watermarking methods are the most popular methods among the existing methods [1].

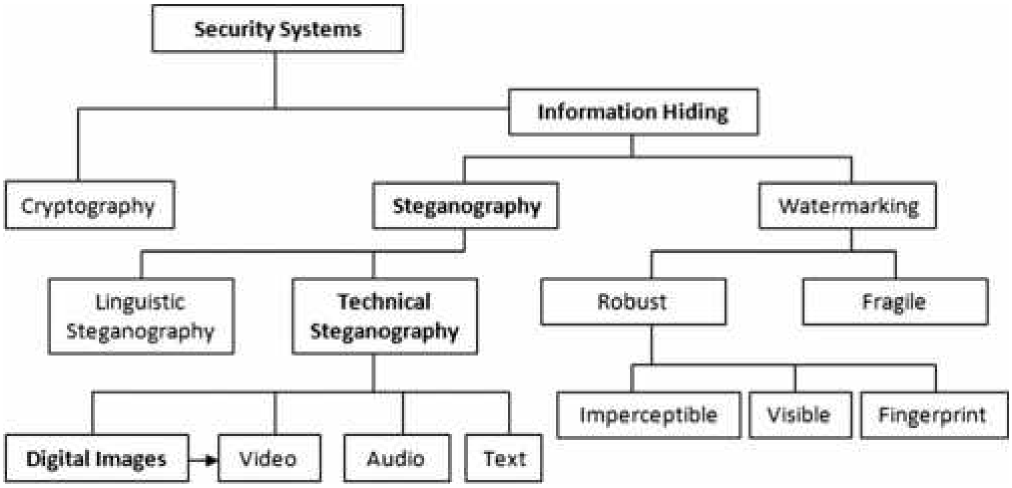

Figure 1 Disciplines of data hiding [2].

At the first glance steganography is useful science to make people's life is easier. However, it can be used as vicious by malevolent people such as terror attacks [3].

Multimedia files are usually chosen to embed secret data because their high capacity and easy share ability.

In the steganography methods, usually color images are used because of their high capacity according to gray-scale images [2].

Image steganography techniques have two different kinds' spatial domain and frequency domain steganography. In the spatial domain, hidden data is embedded into the carrier image's pixels [4, 5, 6, 7]. As for frequency domain, embedding is done into the carrier image's frequency constants [8, 9, 10]. In the frequency method, two different techniques are executed; discrete cosines transform (DCT) and discrete wavelet transforms (DWT).

Potdar et al. [11] have used spatial domain method to embed hidden data into image. Their work is robust against some image processing techniques such as cropping.

In another work, researchers have used Arabic and Farsi [12] alphabet to embed hidden data. While in English just two characters have dot 'i' and 'j', Farsi have 18 characters.

JSteg algorithm is first work which uses JPEG images for embedding hidden data. Even though this method is robust against visual attacks; it is weak under statistical attacks [13].

DIGITAL IMAGE

A digital image becomes n rows and m columns array. Each component is called pixel in this array (Fig.2). Basically, pixels have '0' or '1' binary values. So this image is called binary image. If each pixel presents color value with 16 bit or 24 bit, this image is called color image. In the color image which is presented by 24 bit, each pixel is 3 byte. And each pixel's color is Red, Green, and Blue.

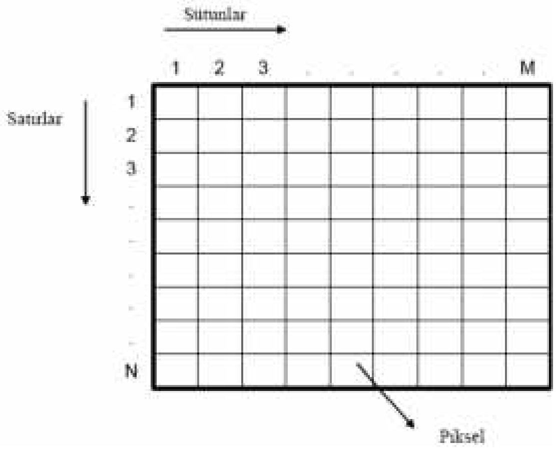

Figure 2 A structure of digital image

Electromagnetic spectrum involves visible light and other electromagnetic forms such as X-Ray, Ultraviolet, and Infrared etc. Human Visual System (HVS) can realize electromagnetic waves which are between 350nm – 780nm in the electromagnetic spectrum.

PROPOSED DATA EMBEDDING ALGORITHM

Until present there are many steganography methods are developed by researchers. But most of them ignore HVS necessities. Lately, some methods which are called Adaptive Steganography consider HVS necessities.

In this paper, a new steganography method is based on HVS is presented [1]. In Fig. 3, the steps of the proposed algorithm are illustrated. According to Fig. 3, secret data can embed to cover image via embedding algorithm. During extraction process, secret data can get from stego image by extraction algorithm.

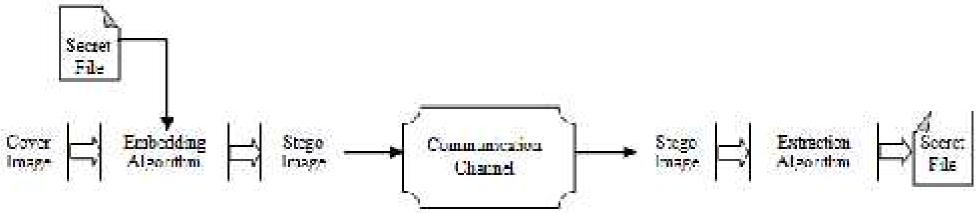

Figure 3 General block diagram for the proposed algorithm.

Embedding process has two steps;

At the first step, pixels which have boundary wavelength value (380nm–700nm) in the electromagnetic spectrum should be chosen carefully. To calculate pixel's wavelength value from RGB value, process can be done in three steps;

1. RGB value should convert to CIE – XYZ form using equations below.

$$\begin{vmatrix} X \\ Y \\ Z \end{vmatrix} = \begin{vmatrix} Xr & Xg & Xb \\ Yr & Yg & Yb \\ Zr & Zg & Zb \end{vmatrix} * \begin{vmatrix} R \\ G \\ B \end{vmatrix} \qquad (1)$$

$$\begin{vmatrix} R \\ G \\ B \end{vmatrix} = \begin{vmatrix} Xr & Xg & Xb \\ Yr & Yg & Yb \\ Zr & Zg & Zb \end{vmatrix}^{(-1)} * \begin{vmatrix} X \\ Y \\ Z \end{vmatrix} \qquad (2)$$

$$\begin{vmatrix} X \\ Y \\ Z \end{vmatrix} = \begin{vmatrix} 0.4124 & 0.3576 & 0.1805 \\ 0.2126 & 0.7152 & 0.0722 \\ 0.0193 & 0.1192 & 0.9505 \end{vmatrix} * \begin{vmatrix} R \\ G \\ B \end{vmatrix} \qquad (3)$$

$$\begin{aligned} X &= 0.4124*R + 0.3576*G + 0.1805*B \\ Y &= 0.2126*R + 0.7152*G + 0.0722*B \\ Z &= 0.0193*R + 0.1192*G + 0.9505*B \end{aligned} \qquad (4)$$

2. After first step, x, y, z choromaticity coordinates are calculated by equation which is below using X, Y, Z.

$$\begin{aligned} x &= \frac{X}{X+Y+Z} \\ y &= \frac{Y}{X+Y+Z} \\ z &= \frac{Z}{X+Y+Z} = 1 - x - y \end{aligned} \qquad (5)$$

3. At the last step, each wavelength value's can be decided using Algorithm 1 below.

Algorithm 1

```
NM_TO_XYZ converts a light wavelength to CIE xyz chromaticities.
!      x = X / ( X + Y + Z ), y = Y / ( X + Y + Z ), z = Z / ( X + Y + Z )
Input, real W, the wavelength of the pure light signal, in nanometers.
Input wavelengths outside this range will result in X = Y = Z = 0.
Output, real X, Y, Z
implicit none
integer, parameter :: ndat = 81
real, save, dimension ( ndat ) :: ldat = (/ &

..


..

real w
  real x
  real, save, dimension ( ndat ) :: xdat = (/ &
..


..

real y
  real, save, dimension ( ndat ) :: ydat = (/ &
..


..

real z
 real, save, dimension ( ndat ) :: zdat = (/ &

..


..

if ( w >= 380.0E+00 .and. w <= 780.0E+00 ) then
    call interp ( ndat, w, ldat, x, xdat )
    call interp ( ndat, w, ldat, y, ydat )
    call interp ( ndat, w, ldat, z, zdat )
  else
    x = 0.0E+00
    y = 0.0E+00
    z = 0.0E+00
  end if
  return
end
```

At the second step, after embedding process, each pixel which is used for embedding should be checked if its wavelength value is still in boundary value in the electromagnetic spectrum. This requirement should be done to do successful embedding.

CONCLUSION

In this work, we have presented a new steganography method based on utilizing HVS for digital still images. In the method, HVS is considered and it makes this method distinctive in the others. According to security level, secret files size can be determined changing wavelength space in the Algorithm 1. So this option gives a big flexibility to users when they want more secret file size or high level security.

Acknowledgment

This study is a part of a research project which is supported by Sakarya University Commission Scientific Research Projects.

REFERENCES

1. O. Cetin, "A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach" Ph.D. dissertation, Dept. Elect. Eng., Sakarya Uni., Sakarya, Turkey, 2008.
2. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods" Elsevier, Signal Processing, pp.727-752,2010.
3. Brent T. McBride, Gilbert L. Peterson, Steven C. Gustafson, "A new blind method for detecting novel steganography" Elsevier, Digital Investigation, pp. 50-70, 2005.
4. C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (2004) 469–474.
5. Chih-Ching Thien, Ja-Chen Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on odulusfunction, Pattern Recognition 36 (2003) 2875–2881.
6. C.C. Chang, T.S. Chen, L.Z. Chung, A steganographic method based upon JPEG and quantization table modification, Information Sciences 141 (2002) 123–138.
7. H. Noda, J. Spaulding, M.N. Shirazi, E. Kawaguchi, Application of bit-plane decomposition steganography to JPEG2000 encoded images, IEEE Signal Processing Letters 9 (2002) 410–413.

8. M.H. Shirali-Shahreza, M. Shirali-Shahreza, A new approach to Persian/Arabic text steganography, in: Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006), 10–12 July 2006, pp. 310–315.
9. A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, A new genetic algorithm approach for secure JPEG steganography, in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22–23 April 2006, pp. 1–6.
10. P. Wayner, Disappearing Cryptography, second ed, Morgan Kaufmann Publishers, 2002
11. A.A. Abdelwahab, L.A. Hassan, A discrete wavelet transform based technique for image data hiding, in: Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, March 18–20, 2008, pp. 1–9.
12. T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group Depertment of Computer Science, universty of Pretoria, Sourth Africa.
13. O. Cetin, A.T. Ozcerit, M. Cakiroglu, "A New Data Embedding Method into Motion Pictures" The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, June 26-29, 2006, Las Vegas, USA.