УДК 004.056.5

AN ADAPTIVE STEGANOGRAPHY BASED ON PARTITIONING APPROACH

S.A. SEYYEDI, N.N. IVANOV

Belarusian State University of Informatics and Radioelectronics
6, P. Brovki Str., Minsk, 220013, Republic of Belarus
amseyyedi@gmail.com, ivanovnn@bsuir.by

Steganography is a branch of information hiding. A tradeoff between the hiding payload and quality of digital image steganographic schemes is major challenge of steganographic methods. This article presents high payload and imperceptible steganography technique based on integer wavelet transform. The cover image is partitioned into 8×8 non overlapping blocks, then each transformed block divided into two subsets and secret message is embedded into the proper one. Experimental results indicate low degrading the quality of stego image by hidden high volume of secret message.

Keywords: Steganography, Integer Wavelet Transform, Embeddable Subset, Rounding Method and LSB.

Nowadays the digital communication channels and Internet play important role in data transmission and sharing, hence there is a great need for security of information to prevent unauthorized access. Steganography is technique of hiding confidential data in any form of media in such a way that no one, except the intended recipient knows the existence of secret data [1]. The main difference between steganography and cryptography is the suspicion factor. The digital images, videos, audios and other digital files can be used as a carrier to embed the information. The important requirements of such steganographic method are payload, security and fidelity. Payload refers to the amount of information that can be hidden in the cover image. Security refers to impossibility of successful attack to detect hidden information. Fidelity (imperceptibility) refers to inability of human eyes to distinguish between cover image and stego-image. Increasing payload rate is in conflict with fidelity and security. The major goal of steganographic techniques is to enhance communication security by increasing embedding rate [2].

An adaptive steganography technique based on integer wavelet transform (IWT) for hiding a large volume of data is proposed. The cover image is partitioned into 8×8 non overlapping blocks and 2D IWT applied to each block. The coefficients in each block divided into embeddable (E) and unused (U) subsets. The subset partition is based on local threshold (T2) where:

$$T_0 = 2^{\lfloor \log_2 \max(temp) \rfloor} \tag{1}$$

$$T_1 = \frac{T_0}{2}, \tag{2}$$

max (temp) denotes as maximum value of coefficients in a block.

The embeddable subset E for each block is undergone for embedding a secret message. The data hiding length (L) is computed based on absolute value of coefficient in E with the aid of following decision factor:

$$L = \begin{cases} 1 & \text{if } \mathrm{E_i} = 0{,}1 \\ \lfloor \log_2 E_i \rfloor & \text{otherwise} \end{cases} \tag{3}$$

The embedding method is determined based on L value. If L=1 then use LSB to embed secret message bits else use rounding method. Rounding method is one a way for embedding secret message bits in cover image. The pixel value is modifying into the nearest integer with the last LSB bits equal to the input bits. The mathematical representation of rounding method is [3]:

$$y = x + A \times (A \le B) - B \times (B < A), \tag{4}$$

$$A = \mathrm{mod}(m - x, 2^c), \tag{5}$$

$$B = \mathrm{mod}(x - m, 2^c), \tag{6}$$

Where y, x, m, and c denote the output value, input value, secret message and capacity respectively.

In order to evaluate the performance of the proposed steganographic method, experimental results simulated using Matlab platform. Various experiments are carried out to access the performance of proposed method in the terms of Payload and fidelity (by measuring several quality metrics peak signal to noise ratio, mean square error and cross correlation). The secret message is generated randomly and four well know 512×512 gray scale image «Lena», «Baboon», «peppers», «Jet» used as cover image. Tab. 1 is shown the results in term of payload and imperceptibility.

Tab. 1. Comparison of maximum payload and fidelity metrics

Image	*Max Payload (bit)*	*Metrics*	*Length of embedding message(Byte)*		
			20000	**30000**	**50000**
Lena	***406040***	**PNSR**	43.35	41.29	39.96
		MSE	3.006	4.835	6.568
		CC	0.9993	0.9990	0.9986
Baboon	***616365***	**PNSR**	39.21	37.8964	36.978
		MSE	7.805	10.554	13.0381
		CC	0.9978	0.9971	0.9964
Peppers	***418187***	**PNSR**	42.77	41.16	40.18
		MSE	3.436	4.979	6.238
		CC	0.9994	0.9992	0.9990
Jet	***386830***	**PNSR**	43.54	40.52	N/A
		MSE	2.877	5.763	N/A
		CC	0.9993	0.9986	N/A

An adaptive and secure steganography scheme has been proposed. Proposed method has integrated blocking approach, wavelet transform, rounding method and LSB into steganography scheme. The main advantage of proposed method is high hiding payload with acceptable level of perceptual quality of stego-image. Also there are several parameters which have an impact in aspect of proposed method such as level of decomposition, level of thresholds. This parameters lead to change the number of elements in subset E. With increasing the elements of E, payload increased. The sender must make the best tradeoff between requirements.

References

1. *Cheddad A., Condell J., Curran K. and Kevitt P.M.* // Digital Signal Processing. 2010. No.3 (90), pp.727-752.

2. *Chandramouli R. and Memon N.D.* // SPIE Security Watermarking Multimedia Contents. 2003. Vol.5020, pp.173–177.

3. *Sarreshtedari S., Ghobi M. and Ghaemmeghami S.* // the 7th annual IEEE consumer communications and networking conference. USA, January 9-12 2010. pp.1-5.