AN EFFICIENT DATA HIDING SCHEME USING DISCRETE WAVELET TRANSFORM

Seyyedi S. A, Ivanov N. N.
Department of Electronic computers, Belarusian state university informatics and radioelectronics
Minsk,Belarus
E-mail: amseyyedi@gmail.com, ivanovnn@gmail.com

Information hiding based on digital images is still the mainstream now. this article represents a new hiding method based on propability of block in frequency domain. we apply discrete wavelet transform through lifting scheme on cover image then divided subband LH to 4x4 non overloaping blocks. Each bit of secret message embedded in cover image with modified entensity value of each block. Experimental results demonstrate that the proposed scheme is robust to common image processing attack like filtering, image compression attack and addaptive noise .

I. Introduction

The rapid growth of Internet and communication networks has led to the tremendous use of digital multimedia like image, audio and video. Furthermore, due to the facility and availability of tools to manipulate digital multimedia especially digital images, tampering of such data has become very easy[1]. In this field, it is important to warrant the integrity of images and protection against unauthorized operation. A common technique for copyright protection is to hide a watermark into digital multimedia to be transmitted. The important requirements of such hiding method are imperceptibility, robustness and security. Imperceptibility means that the watermark should be hidden in the cover image in such a way that it cannot be seen. So it is necessary to exploit the characteristics of the human visual system (HVS) in the secret data embedding process. Robustness is the ability to extract the secret message correctly even if intentional or unintentional attacks are made on the stego image. To ensure security, only the authorized user should be allowed to embed and extract the secret message. This could be achieved by employing a cryptographic methods[1,2].Several digital watermarking algorithms have been proposed in the literature[1,,2,3,4]. these techniques can be divided into two categories namely spatial domain techniques and frequency domain techniques. The secret message can be secret information or another image such as a logo. A novel data hiding scheme based on probability of blockes in frequency domain is proposed. Experimental results demonstrate that the proposed scheme is robust to common image processing attack.

II. Discrete Wavelet Transform

The main theory in wavelet analysis is Multi Resolution Analysis (MRA) that analyzes a signal in frequency domain in detail. Applying one level 2D wavelet transform on image, decompose the cover image in to four non overlapping sub bands by namely LL1, HL1, LH1 and HH 1. The sub bands LL1 include the low pass coefficient and presents a soft approximation of image. Other three sub bands show respectively horizontal, vertical and diagonal details. Approximation sub band is processed further to obtain the next coarser scale of wavelet coefficient until determine scale N is attained. When N scale is attained we will have 3N+1 sub bands.

The lifting scheme is a technique for both designing wavelets and performing the discrete wavelet transform. Actually it is worthwhile to merge these steps and design the wavelet filters while performing the wavelet transform. An advantage of lifting scheme is that they do not require temporary storage in the calculation steps and etc[5]. In this paper biorthogonal Cohen-Daubechies Feauveau (CDF 2/2) lifting scheme was chosen as a case study.

III. proposed embeding method

The main idea behind the proposed algorithm is that secret message bits embed in middle frequency coefficients without visually degrading the quality of the original image. We propose the secret message embedding scheme comprises the following steps:

step A: Read cover image C[MxN]

step B: Take one level 2D discrate wavelet transform through lifting scheme(DWTLS) on cover image.

step C: Select subband LH and divide it to 4x4 nonoverlapping blocks.

step D: Encrypt secret message SM[R,S] and Rearranging its by chaotic function.

step E: For each bits of secret message,coefficients value of block will change as follows:

```
if W=1 then
For all pixel of 4x4 block's
    I'=I+k
if W=0 then
For all pixel of 4x4 block's
    I'=I-k
```

I' denote modifed coefficient,I primary coefficient and k is constant value.

step F: Take inverse transfrom

IV. Extract Modul

The extraction secret image consists of steps as follows:

step A: Take on level 2D DWTLS on both cover image and stego image.

step B: Select subband LHC (cover image) LHS(stego image) and divide them to 4x4 nonoverlapping blocks.

step C: Calculate the Probability of embedded bit 0 (P0) or 1 (P1) with comparison coefficient value in each 4x4 block of cover image (I) and stego image(I') as follow:

P1=P1+1/16 if I'>I
P0=P0+1/16 if I'≤ I

step D: Extract W'(secret messege bits) based on P0,P1 as follow:

W'=1 if P1 $\geq$ P0
W'=0 if P1 $<$ P0

step E: Take reverse chaotic function and decryption to achive secret message.

V. Experimental results

In order to evalute the performance of the proposed data hiding method, Matlab platform is used. Various experiments are carried out to access the performance of the proposed algorithm, in terms of robustness against attacks and imperceptibility.Standard gray scale image Barbara of size 512x512, shown in figure 1 is used as host images and BSUIR logo 64x64 is used as secret message(watermark) and k=5, shown in figure 2.

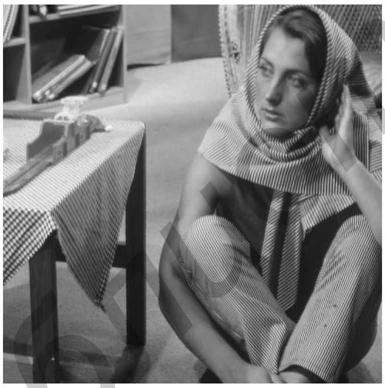

Рис. 1 – Coverimage Barbara

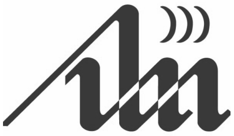

Рис. 2 – Secret image logo BSUIR

PSNR (Peak Signal To Noise Ratio) is used in this paper to analyze imperceptibility of stego image S in comparrison with the cover image C. PSNR is defined as:

$$PSNR = 20log_{10}\left(\frac{255}{\sqrt{MSE}}\right).$$

where MSE is the mean squared error between the cover image C and the stego image S given by:

$$MSE = (\frac{1}{MN})\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[C(i,j) - S(i,j))^2.$$

The performance of extracted secret messege W' (i,j) with orignal secret messege W(i,j) is evaluted by calculating the Normalized Cross Correlation, which is given by:

$$NCC(W,W') = \frac{\sum_{i=1}^{R}\sum_{j=1}^{S}(W(i,j).(W'(i,j))}{\sum_{i=1}^{R}\sum_{j=1}^{S}(W(i,j))^2}.$$

Таблица 1 – Experimental results for test image Barbara

Attacks	PSNR	NCC
No attack	40.1720	1
Jpeg Q80	38.2930	1
Jpeg Q70	35.7930	1
Jpeg Q65	35.2972	0.9830
Median filter3x3	37.1445	0.9619
Saltandpepper 0.01	24.6299	1
Saltandpepper 0.1	17.5505	0.9921
Saltandpepper 0.3	12.7381	0.9526

VI. Conclusion

In this paper an efficient and non blind data hiding scheme has been proposed. We have integrated wavelet transform ,chaotic function and probability of intensity value of blocks into hiding scheme. The main advantage our scheme high imperceptiblity and robust against common image processing attacks. Security of scheme also increase by applying choatic function beffor embedding.

VII. References

1. Hartung, F. Multi media watermarking techniques / M. Kutter,M. Kuhn // proceeding of the IEEE. – 1999. – Vol. 87,№ 10. – P. 1079–1107.
2. Petitcolas, F. Information hiding a survey / R. Anderson // proceeding of the IEEE. – 1999. – Vol. 87,№ 7. – P. 1062–1078.
3. Vleeschouwar, C. De. Invisibility and application function in perceptual watermarking an overview / J. F. Delaigle, B. Macq // proceeding of the IEEE. – 2002. – Vol. 90, № 1. – P. 64–77.
4. Krishnamoorthi,R.Image adaptive watermarking with visual model in orthogonal polynomial based transform domain / P. D. Sheba Kezia Malarchelvi // International journal of information and communication engineering. – 2009. – Vol. 5, № 2. – P. 146–153.
5. Win, S.The lifting scheme: A construction of second generation wavelets / // SIAM journal on matematical analysis. – 1997. – Vol.29, № 2. – P. 511–546.