A Blind Detection Resistant Steganographic Algorithm for Images Based on Texture Complexity and Pixel-value Differencing

Tao Ran

ZhengZhou Information Science and Technology Institute ZhengZhou,China

Zhang Tao

ZhengZhou Information Science and Technology Institute ZhengZhou,China

Abstract—**According to the analysis of the effect of the texture complexity on steganalysis, we propose a data hiding algorithm based on texture complexity and difference pixel value. Firstly, the image is decomposed into blocks, after which the texture complexity of each block is calculated and blocks with high complexity are selected. Then the different pixel values on two directions of the selected blocks are computed to choose the edge areas. The secret messages are only embedded in the pixel-value differencing above the threshold. When compared with several steganographic methods on different image databases, the experimental results show that our method outperforms previous steganographic methods such as LSB matching and Adaptive data hiding in edge areas of images on the capability of resisting universal blind detecting methods, such as wavelet high-order statistics analysis.**

Keywords-Steganography, Universal blind detection, Texture complexity, Edge area, LSB matching

I. INTRODUCTION

With the rapid development of network technology, information security has become a growing problem. Steganography is an important aspect of security communications. Currently, a variety of effective steganalysis brings enormous challenges to the steganography. Universal blind steganalysis is an important element of steganalysis which detects the presence of the messages based on the statistical differences between the cover and stego.

The feature extraction algotirhm based on image quality metrics is a typical blind detection method[1]. Many scholars have extracted image statistics features as classification from the wavelet domain, Fraid[2] has employed a wavelet decomposition and a local angular harmonic decomposition from which they have extracted a statistical feature vector for differentiating between clean and stego. Shi[3] has proposed a method which the statistical moments of characteristic functions of the prediction-error image, the test image, and their wavelet sub-bands are selected as features. Then the probability density functions(PDF) experience moments and the characteristic function(CF) experience moments of sub-band image are extracted in Wang's algorithm[4]. The normalized histogram of the image local linear transformations is used in Li's method[5].

Currently, steganography gives more emphasis on ability of resisting steganalysis, such as Chen[6] has proposed an improved LSB matching with histogram characters reserved method(LSBMHCR) which can resist histogram attack through the establishment of embedding information table that determines the addition and subtraction of the pixel value. Yang[7] has proposed a new adaptive least-significant bit steganographic method(AELSB) using pixel-value differencing that provides a larger embedding capacity and imperceptible stego images. Luo[8] has expanded the LSB matching revisited image steganography and proposed an edge adaptive scheme(EALSBMR) which can select the embedding regions according the size of secret message and the pixel-value differencing which can resist universal blind detection algorithm well.

By analyzing the principle of universal blind detection method and on the basis of block selected by computing texture complexity, a data hiding in edge regions which are chosen according to pixel-value differencing is proposed. The image blocks with maximum complexity are selected, then the secret messages are embeded only in the pixel-value differencing above the threshold which is calculated by the length of the secret message.

II. THE PRINCIPLE ANALYSIS OF UNIVERSAL BLIND DETECTION

According to the analysis from the previous, the PDF moments and CF statistical moments are most widely used in universal blind steganalysis. The analysis of their principles is introduced as follows.

For additive embedding, the relationship between stego signal X, cover signal S, and effective embedding noise Z is given by $X = S + Z$.

Where Z is independent of S and is a function of transmitted messages and secret keys shared between the encoder and decoder. The independence between S and Z leads to the following PDFs and CFs equations:

$$m_{n,X} = E(S+Z)^n \text{ and } \Phi_X(t) = \Phi_S(t)\Phi_Z(t)$$

It is weighted smoothing PDFs of cover signal for additive embedding. We can see that from figure 1. Therefore, it is easy to verify that:

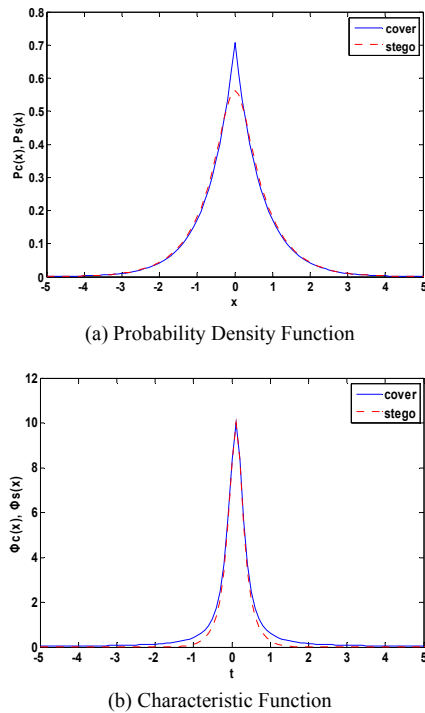$$m_{n,X} \geq m_{n,S} \text{ and } |\Phi_X(t)| \leq |\Phi_S(t)|$$

(a) Probability Density Function

(b) Characteristic Function

Figure1. PDFs and corresponding CFs of a Generalized Gaussian Distributed cover signal S and its stego signal X

So how to maintain the same high frequency coefficients of wavelet sub-band is the key point to resist to universal blind detection algorithm.

III. PROPOSED ALGORITHM

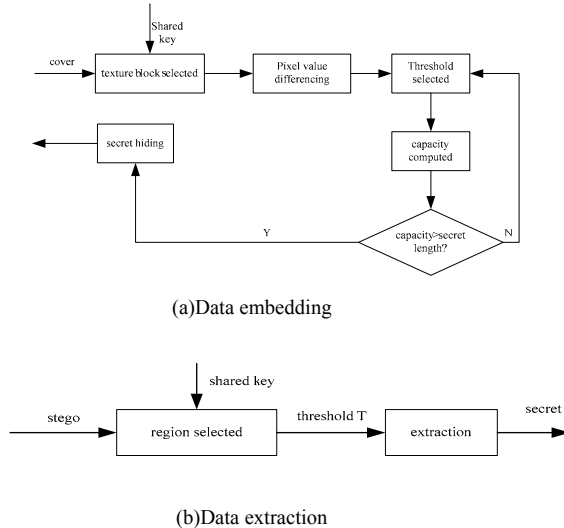The proposed algorithm process is showed in figure 2.

(a)Data embedding

(b)Data extraction

Figure 2. Proposed scheme

A. Texture Block Selected

For the image f of size $M \times N$, we employ the average variance matrix C describing texture complexity of the image：

$$C(i,j) = \frac{1}{8} \times (\sum_{m=-1}^{1} \sum_{n=-1}^{1} (f(i,j) - f(i+m, j+n))^2)$$

$f(i,j)$ denotes the pixel-value of position (i, j) in the image.

For every size of $Bs \times Bs$, calculates the average of $C(i,j)$：

$$CM(k) = \frac{1}{Bs \times Bs} \times (\sum_{i=1}^{Bs} \sum_{j=1}^{Bs} C(i,j))$$

$CM(k)$ denotes block's complexity.

The texture complexity block selected is introduced as follows：

Step 1 The size $M \times N$ of the image is divided into $mb \times nb$, sub-block size of $Bh \times Bh$, and

$$mb = \left\lfloor \frac{M}{Bh} \right\rfloor, nb = \left\lfloor \frac{N}{Bh} \right\rfloor.$$

Step 2 In each sub-block, select many small blocks size of $Bs \times Bs$ according to the difference of the starting point. Calculate their CMs, and record the biggest CM block's starting point in the shared key. The process is showed in figure 3. In this paper $Bh = 10$, $Bs = 8$.

B. Threshold Computing

Generally, the direction of adjacent pixel selected is horizontal. This paper considers the dependence of the image content, the pixel value differencing statistics of horizontal and vertical are recorded. It's show in Figure 4

$Dif(t)$ denotes the pixel value differencing greater than t, assuming the secret message length M, so the threshold T is the integer value which greater than M, when the $Dif(t+1)$ less than M.

According the direction of adjacent pixel value we can get horizontal threshold T_h and vertical threshold T_h, then we can get final threshold T：

$$T = \max(T_h, T_v)$$

When the threshold equals horizontal threshold T_h, then the selected direction of adjacent pixel is horizontal, or it is vertical. From foregoing analysis, the larger the T is, the smaller the capacity is. Experiment shows that $t \in \{0,1,2,3,\cdots 31\}$ can satisfy requirements of security and capacity.
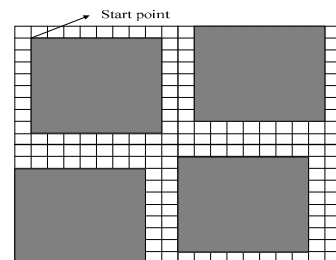
Figure 3. Texture Blocks Selection

(a)selected in horizontal
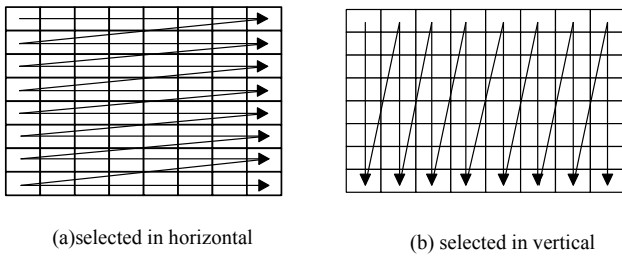
(b) selected in vertical

Figure 4. Direction of Selecting Adjacent pixels

C. Embedding Rules

The message is embedded the pixel value differencing of block above the threshold by LSBM. In order to maintain the correct extraction of the secret message, when the pixel differencing value equals to the threshold T, the value remains or becomes $T+1$.

$LSB(x_i)$ denotes the least significant bit of x_i, $dif(i) = x_{i+1} - x_i$, m_i is the secret message, T is the threshold，the rules is given in following:

$$Case1: dif(i) \bmod 2 = m_i$$
$$(y_i, y_{i+1}) = (x_i, x_{i+1})$$
$$Case2: dif(i) \bmod 2 \neq m_i \& dif(i) = T \& dif(i) > 0$$
$$(y_i, y_{i+1}) = (x_i + 1, x_{i+1}) or (x_i, x_{i+1} - 1)$$
$$Case3: dif(i) \bmod 2 \neq m_i \& dif(i) = T \& dif(i) < 0$$
$$(y_i, y_{i+1}) = (x_i - 1, x_{i+1}) or (x_i, x_{i+1} + 1)$$
$$Case4: dif(i) \bmod 2 \neq m_i \& dif(i) \neq T$$
$$(y_i, y_{i+1}) = (x_i + 1, x_{i+1}) or (x_i, x_{i+1} - 1) or (x_i - 1, x_{i+1}) or (x_i, x_{i+1} + 1)$$

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Image Quality Analysis

Five sizes of 512×512 which standard test images' peak signal-to-noise ratio(PSNR) are showed in table1. The ratio embedded in each image is 0.2:

B. Statistical Attack

In this subsection, in order to validate the performance of our method, we experiment in different image sets. First, 1400 high-precision original uncompressed scanning images which are stored as TIFF in NRCS are selected and sampled from 2100×1500 to 700×500, then converted to gray images which are recorded as image Set 1. The images in Set 1 are compressed in quality factor 80 to standard JPEG images, and then extracted to the gray images, denoted Set 2. Set 3 is constituted of 1338 uncompressed size of 512×384 or 384×512 gray images.

Secret messages are embedded in each image of sets using five algorithm by embedding rate 0.2. There are 400 images(338 in set 3) randomly selected as training sets in Set 1, 2. The rest 1000 are used as test sets. Four universal blind algorithms are used to classify the covers and stegos. In order to reduce the impact of the randomly samples selected, the experimentations are repeated 20 times, and the average of the results is employed.

The performance of four universal blind algorithm is showed in Table2, "TP_E" is used to measure the ability of blind detection resistant which means the probability of detection when the probability of non-detection equals to the probability of false.

From these different tables, we can see that our method owns better ability to blind detection resistant than other methods.

V. SUMMARIES

Based on analysis of the principles of blind detection techniques, a data hiding algorithm by selecting the highest texture complex block is proposed. The highest texture complex block is selected in which the message is embedded by pixel value differencing. The defect of proposed embedding rate is low. Future research direction is used to maintain security while increases the embedding capacity.

REFERENCES

[1] TOMÁŠ PENVÝ, PATRICK BAS, AND JESSICA FRIDRICH. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 215-224.

[2] LYU S, FARID H. Steganalysis using higher-order image statistics[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(1): 111-119.

[3] SHI YUNQING, XUAN GUORONG, ZOU DEKUN, GAO JIANJIONG. Image Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and Neural Network[C]// Proceedings of IEEE ICME, 2005: 269-272.

[4] WANG YING, PIERRE MOULIN. Optimized feature extraction for learning-based image steganalysis[J]. IEEE Transaction on Information Forensics and Security, 2007, 2(1): 31-45.

[5] LI BIN, HUANG JIWU, SHI YUNQING. Textural feature based universal steganalysis[C]// Proceedings of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents X, 2008,6819:12.1-12.12.

[6] CHEN ZHIZHONG, LIU WENYAO. Improved LSB Matching with Histogram Characters Reserved[C]// Proceedings of the SPIE, Information optics and Photonics Technologies II, 2007,6837.

[7] YANG C H, WENG C Y, WANG S J, SUN H M. Adaptive data hiding in edge areas of images with spatial LSB domain systems[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(3): 488-497.

[8] LUO WEIQI, HUANG FANGJUN, HUANG JIWU. Edge Adaptive Image Steganography Based on LSB Matching Revisited[J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 201-214.

TABLE I. PSNR OF FIVE IMAGES WITH DIFFERENT STEGANOGRAPHIC ALGORITHMS(DB)

Image	Steganographic Algorithms				
	AELSB	LSBM	LSBMR	EALSBMR	Proposed
Baboon	44.57	61.13	62.40	67.29	69.01
Lena	45.57	61.11	62.46	67.21	74.83
Gold	45.01	61.08	62.37	67.25	73.68
Peppers	45.72	61.14	62.44	67.22	75.51
Barbara	44.50	61.10	62.41	67.22	68.67

TABLE II. THE PERFORMANCE OF RESISTING BLIND DETECTION ALGORITHMS

Embedding rate	Steganographic Algorithms	Fraid	Shi	Wang	Li
Set 1	LSBM	0.544	0.561	0.545	0.600
	LSBMR	0.534	0.540	0.586	0.576
	AELSB	0.927	0.722	0.746	0.603
	EALSBMR	0.516	0.506	0.511	0.504
	Proposed	0.500	0.501	0.500	0.502
Set 2	LSBM	0.608	0.806	0.984	0.943
	LSBMR	0.584	0.758	0.975	0.937
	AELSB	0.564	0.621	0.747	0.557
	EALSBMR	0.508	0.580	0.838	0.539
	Proposed	0.515	0.516	0.521	0.501
Set 3	LSBM	0.608	0.806	0.984	0.943
	LSBMR	0.584	0.758	0.975	0.937
	AELSB	0.564	0.621	0.747	0.557
	EALSBMR	0.508	0.580	0.838	0.539
	Proposed	0.515	0.516	0.521	0.501