Hindawi
Security and Communication Networks
Volume 2019, Article ID 3546367, 13 pages
https://doi.org/10.1155/2019/3546367

Research Article

Security Measure for Image Steganography Based on High Dimensional KL Divergence

Haitao Song, Guangming Tang, Yifeng Sun, and Zhanzhan Gao

Information Science and Technology Institute, Zhengzhou, China

Correspondence should be addressed to Haitao Song; kernelsong@yeah.net

Received 4 December 2018; Revised 9 February 2019; Accepted 26 March 2019; Published 8 April 2019

Academic Editor: David Megias

Steganographic security is the research focus of steganography. Current steganography research emphasizes on the design of steganography algorithms, but the theoretical research about steganographic security measure is relatively lagging. This paper proposes a feasible image steganographic security measure based on high dimensional KL divergence. It is proved that steganographic security measure of higher dimensional KL divergence is more accurate. The correlation between neighborhood pixels is analyzed from the principle in imaging process and content characteristics, and it is concluded that 9-dimensional probability statistics are effective enough to be used as steganographic security measure. Then in order to reduce the computational complexity of high dimensional probability statistics and improve the feasibility of the security measure method, a security measure dimension reduction scheme is proposed by applying gradient to describe image textures. Experiments show that the proposed steganographic security measure method is feasible and effective and more accurate than measure method based on 4-dimensional probability statistics.

1. Introduction

Steganography provides an effective way for covert communication through hiding secret messages in public multimedia covers. Steganography based on image covers gets more attention because images widely existed and are easy to acquire and complex enough. During three key points (robustness, security, and capacity) of steganography, security seems more valued by researchers. So adaptive steganography [1] has become the mainstream because of its high security, and a lot of research results have been achieved. However, research on corresponding steganographic security theory is relatively lagging, and there is no effective steganographic security measure method now. Accurate steganographic security measure method could help to design more secure algorithms, help to enrich steganographic security theory, and promote further development of steganography.

At present, there are mainly two types of steganographic security measure methods. The first type is from the attacker's perspective through blind steganalysis [2, 3], which relies on a large number of training sets, many high-quality features, and good classifier. These security measure methods perform a certain degree of uncertainty and pool availability. The other type is based on information theory, which is the main research direction of steganographic security measure currently.

Zollner [4] first introduced Shannon's information theory to study steganographic security, providing ideas for research on steganographic security theory. The steganographic security theory widely used at present was constructed by Cachin [5] based on statistical security theory and KL divergence. By assuming that covers were independent and identically distributed, Cachin's theory described the changes of 1-dimensional probability statistical distribution between the cover object and its stego object. However, Cachin's theory ignored the correlation between cover elements, resulting in poor accuracy and overestimation of security.

In order to improve the accuracy of the steganographic security measure, Sullivan [6] proposed a method based on the Markov chain model. Then, Zhang [7] proposed a high-order Markov chain model. The "chain" scanning method made these two methods less accurate when applied to images which are 2-dimensional. Image covers (unless specifically

noted, "image" refers to "spatial image" in the paper) are special because there is correlation between neighborhood pixels. And the correlation in 2-dimensional space cannot be described by Markov chain. On the basis of Cachin's theory, Sun proposed a steganographic security measure method of n-dimensional KL divergence, but failed to propose an effective solution for its high computational complexity.

Therefore, the accuracy of image steganographic security measure relies on the accuracy of pixels statistical distribution. Based on the above research, this paper proposes an image steganographic security measure method based on high dimensional KL divergence. It is analyzed and proved that using higher dimensional discrete probability statistics can effectively improve the accuracy of steganographic security measures; we can draw the conclusion that 9-dimensional probability statistics can accurately measure the steganographic security by analyzing the correlation of neighborhood pixels, and we analyze the complexity problem of 9-dimensional probability statistics; to solve the complexity problem of 9-dimensional probability statistics, dimension reduction scheme is proposed to keep the accuracy of measure method, and then the complete steganographic security measure method is depicted; finally, experiment results show the feasibility, validity, and accuracy of the proposed steganographic security measure.

2. Related Work

The steganographic security measure is used to make a reasonable quantification of the steganographic security by means of calculation. In the study of steganographic security, the classical method was proposed by Cachin, which defines steganographic security based on statistical security and KL divergence. Assuming that $P_C(x)$ and $P_S(x)$ are two probability distributions of values of variable x, KL divergence (also known as relative entropy) is an asymmetry measure of differences between the two probability distributions $P_C(x)$ and $P_S(x)$. In general, $P_C(x)$ is the true distribution, and $P_S(x)$ represents the theoretical or approximate distribution. The basic form of KL divergence is

$$D\left(P_C \parallel P_S\right) = \sum_{x\in\Omega} P_C(x) \log \frac{P_C(x)}{P_S(x)} \tag{1}$$

where the logarithmic function defaults to base 2 and Ω is the value space of variable x. For grayscale images, usually $\Omega = \{x | x \in N, x \le 255\}$.

We can use $P_C(x)$ to describe the probability distribution of the original cover image and use $P_S(x)$ to describe the probability distribution of its corresponding stego image. If the KL divergence of the two probability distributions is at most ε,

$$D\left(P_C \parallel P_S\right) = \sum_{x\in\Omega} P_C(x) \log \frac{P_C(x)}{P_S(x)} \le \varepsilon \tag{2}$$

Then the steganography is ε−secure. If $\varepsilon = 0$, the steganography is absolutely secure. In practice, the probability distributions $P_C(x)$ and $P_S(x)$ are difficult to obtain accurately, and accurate steganographic security measure cannot be achieved. In actual application, it is assumed that the pixels are independently and identically distributed, and the probability distribution of the cover can be described by probability statistics.

3. Theoretical Analysis

It is not accurate enough using KL divergence calculated from 1-dimensional probability statistics of pixels to evaluate steganographic security. In order to improve measure accuracy, we naturally get the idea that using high dimensional probability statistics can compensate for the lack of accuracy caused by low dimensional probability statistics. N-dimensional probability statistics used for steganographic security measure is shown as follows:

$$D^{(N)}\left(p_C^{(N)} \parallel p_S^{(N)}\right) = \sum_{x\in\Omega^N} p_C^{(N)}(x) \log \frac{p_C^{(N)}(x)}{p_S^{(N)}(x)} \tag{3}$$

$D^{(N)}(p_C^{(N)} \parallel p_S^{(N)})$ is treated as the final result of the steganographic security measure, and the smaller the value, the higher the steganographic security.

3.1. Theoretical Proof. In this paper, *n-pixel group* is defined as a square region composed of a center pixel and n-1 pixels closely adjacent to it in the spatial image. In the statistical analysis about image, as shown in Figure 1, 2-pixel group, 4-pixel group, and 9-pixel group are often used. When the image is statistically analyzed using n-pixel groups, accordingly, it is assumed that the n-pixel groups are independently and identically distributed.

Analyzing steganographic security based on KL divergence, the following theorems (Theorem 1 and Theorem 2) can be derived.

Theorem 1. *Steganography is more secure if embedding modifications occur on pixel groups with smaller statistical probability.*

Proof. When making probability statistical analysis of n-pixel groups, we must use n-dimensional KL divergence $D^{(n)}$ as a criterion for measuring steganographic security. In the proof process, the representation is simplified.

$$\begin{aligned} D^{(n)} &= \sum p(x) \log \frac{p(x)}{q(x)} = E\left(\log \frac{p(x)}{q(x)}\right) \\ &\ge \log\left[E\left(\frac{p(x)}{q(x)}\right)\right] = \log\left[\sum\left(q(x)\cdot\frac{p(x)}{q(x)}\right)\right] \\ &= 0 \end{aligned} \tag{4}$$

The above formula "greater than or equal to" is derived according to the nature of the convex function. $D^{(n)} = 0$ if

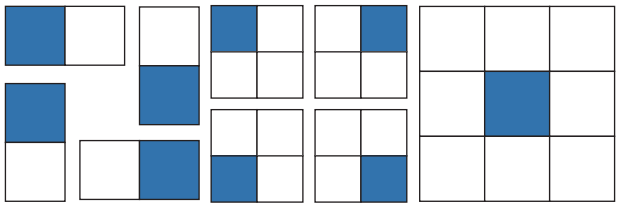

Figure 1: Examples of n-pixel groups.

and only if $p(x) = q(x)$.

$$D^{(n)} = \sum p(x) \log \frac{p(x)}{q(x)} = \sum p \log \frac{p}{p+\Delta} \tag{5}$$

We can get from the above formula that when $p = 0$, $p \log(p/(p+\Delta)) = 0$, and when $\Delta = 0$ $p \log(p/(p+\Delta)) = 0$.

$$\begin{aligned} \frac{\partial D}{\partial p} &= \sum \left(\log \frac{p}{p+\Delta} + \frac{\Delta}{(p+\Delta)\ln 2} \right) \\ \frac{\partial^2 D}{\partial p^2} &= \sum \left(\frac{\Delta^2}{p(p+\Delta)^2 \ln 2} \right) \geq 0 \end{aligned} \tag{6}$$

$\partial^2 D/\partial p^2 = 0$ if and only if $\Delta = 0$, which means that there is no embedding modification.

So, $\partial D/\partial p \geq (\partial D/\partial p)|_{p=0} = 0$, and the equal sign is established if and only if $p = \Delta = 0$.

Therefore, $D^{(n)}$ is a monotonically increasing function of p. If modifying pixel groups with higher statistical probability, KL divergence would be higher and steganography would be less secure; if modifying pixel groups with lower statistical probability, KL divergence would be lower and steganography would be more secure.

Theorem 1 is consistent with the empirical conclusions of current adaptive steganography algorithms. The statistical probability of pixel groups in the image texture areas is relatively low, and modifications of adaptive steganography algorithms with high security occur mostly in the texture pixels. This theorem provides theoretical basis for adaptive steganography algorithms. □

Theorem 2. *Steganographic security measure would be more accurate when using higher dimensional probability statistics.*

Proof. Assuming that pixel groups are independently and identically distributed (different from the assumption that pixels are independently and identically distributed, for that pixel groups with independent and identical distribution conform to the fact that there is a strong and actual correlation between neighborhood pixels), for the same cover image C and stego image S, the N-dimensional KL divergence and n-dimensional KL divergence ($N > n$) are analyzed, respectively, as steganographic security measures, and we have

$$\begin{aligned} D^{(N)} &= \sum_{x_1 \in \Omega} \sum_{x_2 \in \Omega} \cdots \sum_{x_N \in \Omega} P_C^{(N)}(x_1, x_2, \ldots, x_N) \\ &\quad \cdot \log \frac{P_C^{(N)}(x_1, x_2, \ldots, x_N)}{P_S^{(N)}(x_1, x_2, \ldots, x_N)} \\ &= \sum_{x_1 \in \Omega} \sum_{x_2 \in \Omega} \cdots \sum_{x_N \in \Omega} P_C^{(N)}(x_1, x_2, \ldots, x_N) \\ &\quad \cdot \log \frac{P_C^{(N)}(x_1, x_2, \ldots, x_n) \cdot P_C^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N)}{P_S^{(N)}(x_1, x_2, \ldots, x_n) \cdot P_S^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N)} \\ &= \sum_{x_1 \in \Omega} \sum_{x_2 \in \Omega} \cdots \sum_{x_N \in \Omega} P_C^{(N)}(x_1, x_2, \ldots, x_N) \\ &\quad \cdot \log \frac{P_C^{(N)}(x_1, x_2, \ldots, x_n)}{P_S^{(N)}(x_1, x_2, \ldots, x_n)} \\ &\quad + \sum_{x_1 \in \Omega} \sum_{x_2 \in \Omega} \cdots \sum_{x_N \in \Omega} P_C^{(N)}(x_1, x_2, \ldots, x_N) \\ &\quad \cdot \log \frac{P_C^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N)}{P_S^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N)} \\ &= \sum_{x_1 \in \Omega} \sum_{x_2 \in \Omega} \cdots \sum_{x_n \in \Omega} P_C^{(n)}(x_1, x_2, \ldots, x_n) \\ &\quad \cdot \log \frac{P_C^{(n)}(x_1, x_2, \ldots, x_n)}{P_S^{(n)}(x_1, x_2, \ldots, x_n)} \\ &\quad + \sum_{x_{n+1} \in \Omega} \sum_{x_{n+2} \in \Omega} \cdots \sum_{x_N \in \Omega} P_C^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N) \\ &\quad \cdot \log \frac{P_C^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N)}{P_S^{(N-n)}(x_{n+1}, x_{n+2}, \ldots, x_N)} = D^{(n)} + D^{(N-n)} \end{aligned} \tag{7}$$

As obtained in the proof process of Theorem 1, when

$$\begin{aligned} &P_C^{(N-n)} \neq P_S^{(N-n)}, \\ &D^{(N-n)} > 0, \text{ so} \\ &D^{(N)} > D^{(n)} \end{aligned} \tag{8}$$

When we continue to modify the existing stego image S to obtain another stego image S', and use m-dimensional KL divergence to describe differences between C and S, and differences between C and S', the change of KL divergence is

$$\begin{aligned} \Delta D_{KL}^{(m)} &= D' - D_0 = \sum P_C \log \frac{P_C}{P_{S'}} - \sum P_C \log \frac{P_C}{P_S} \\ &= \sum P_C \log \frac{P_S}{P_{S'}} = \sum P_S \log \frac{P_S}{P_{S'}} = D_S^{(m)} \end{aligned} \tag{9}$$

When $N > n$, $D_S^{(N)} > D_S^{(n)} \Longrightarrow \Delta D_{KL}^{(N)} > \Delta D_{KL}^{(n)}$.

Therefore, steganographic security measure adopting higher-dimensional probability statistics can be more sensitive to embedding modification and be more accurate. □

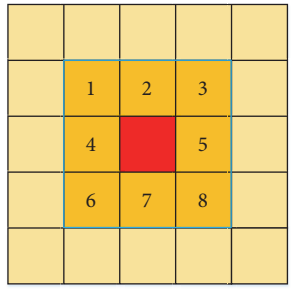

Figure 2: Correlation between central pixel and its neighborhood pixels.

3.2. Determination of Dimensions Used in Steganographic Security Measure. From Theorem 2, it can be concluded that the higher the dimension of probability statistics, the more accurate the corresponding steganographic security measure. But for overall consideration especially for security, computational complexity, and practical feasibility, the conclusion is not absolutely correct. The dimension used in steganographic security measure must be determined obeying the following principles.

Principle 1. Probability statistics should adopt high dimensions to ensure the accuracy of steganographic security measures.

Principle 2. Computational complexity cannot be too high and steganographic security measures are feasible in practice.

Principle 3. The dimension should be determined to conform to actual characteristics of the cover.

The characteristics of the image are mainly reflected in correlation between the central pixel and its neighborhood pixels. We can easily know that Principle 1 is contrary to Principle 2. The key to taking a compromise between the two principles is the consideration of actual characteristics of image which are depicted in Principle 3.

The image library Bossbase 1.01 [8] is often used in image steganography research. It contains 10,000 512∗512 uncompressed spatial images. These images are taken from 8 different cameras, and captured natural images of the raw format are processed (without any compressing operations) to obtain the grayscale image library. Most natural images are interpolated during imaging process [9] which makes the central pixel and its neighborhood pixels have strong correlation. In addition, the inherent content characteristics of natural images also make neighborhood pixels get correlation. It can be found that the pixel closer to the central pixel would have a stronger correlation with the central pixel. Due to interpolation operation and inherent content characteristics, the central pixel has a strong correlation with its 8-neighbor pixels. The correlation between the central pixel and its neighborhood pixels is shown in Figure 2.

After the above analysis, it is not difficult to get the conclusion that it is accurate and reasonable to determine the dimension based on the strong correlation between the central pixel and its 8-neighbor pixels. And it means that steganographic security measure should use 9-dimensional probability statistics, which conforms to Principles 1 and 3. However, for Principle 3, the computation complexity is

$$C_{256}^{9} \times 512 \times 512 \approx 2^{86} \tag{10}$$

Therefore, security measure using 9-dimensional probability statistics is not feasible in practical applications. In order to solve this problem, this paper proposes a dimension reduction scheme based on image texture features, which can convert the 9-dimensional probability statistics to 4-dimensional probability statistics.

4. Steganographic Security Measure

Probability statistics usually ignore image texture features and do not distinguish pixels within a pixel group (9-dimensional probability statistics using 9-pixel group). Empirical conclusion of adaptive steganography and deterministic conclusion of Theorem 1 indicate that local texture features are the focus of most adaptive steganography algorithm, and the processing method to textures is related to steganographic security. Image texture features make dimension reduction in steganographic security measure become possible.

Gradient is a vector with amplitude and direction. The image gradient indicates that the pixel value changes fastest along the gradient direction at a certain pixel. Therefore image gradient can describe image texture features clearly. And it is widely used in edge detection and image enhancement. In this paper, we use gradient to describe texture features in 9-pixel groups and design a "dimension reduction scheme" so as to not only maintain correlation between 9-pixel groups, but also ensure the accuracy, reduce computational complexity, and increase availability of the steganographic security measure.

The overall structure of steganographic security measure method proposed in this paper is shown in Figure 3. The dotted line shows the key content of the proposed method.

4.1. Gradient and Texture Pixels. The preferred choice for obtaining gradient of a 9-pixel group is to use the Sobel operator [10, 11]. As shown in (11), convolving Sobel operator with a 9-pixel group to calculate the horizontal approximate gradient and vertical approximate gradient of the central pixel,

$$G_{ij}^{x} = A_{ij} * \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix}$$
$$G_{ij}^{y} = A_{ij} * \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} \tag{11}$$

G_{ij}^{x} and G_{ij}^{y} are the horizontal gradient and vertical gradient of the central pixel at the position (i, j), respectively. And then the amplitude and direction of the gradient can be

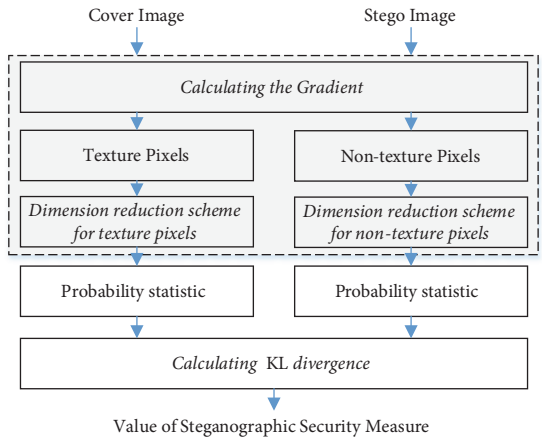

Figure 3: Overall structure of steganographic security measure.

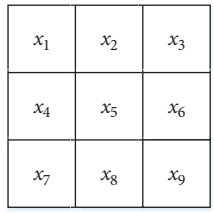

Figure 4: Pixel number within a 9-pixel group.

calculated easily. Gradient amplitude can describe the relative change of the gray value of image pixels. Using gradient amplitude to judge whether the central pixel is a texture pixel is simple, intuitive, and effective. General way to determine whether it is a texture pixel is setting a threshold T (if gradient amplitude is greater than or equal to T, then the pixel studied is a texture pixel). Gradient amplitude is calculated as follows:

$$\left|G\left(I_{ij}\right)\right| = \sqrt{\left(G_{ij}{}^{x}\right)^2 + \left(G_{ij}{}^{y}\right)^2} \tag{12}$$

Because image area where modification occurs and the number of pixels modified differ with different embedding payload, a reasonable threshold T should be closely related to embedding payload. T needs to meet the constraints shown in the following equation:

$$\begin{aligned} |\Xi| &\geq m \cdot n \cdot \alpha \\ \Xi &= \left\{I_{ij} \mid \left|G\left(I_{ij}\right)\right| \geq T\right\} \\ [m, n] &= \text{size of } (I) \end{aligned} \tag{13}$$

where Ξ is a set of texture pixels obtained according to threshold T, I denotes cover image, and α denotes embedding payload.

4.2. Dimension Reduction Scheme. Dimension Reduction Scheme is different for texture pixels and nontexture pixels.

(1) Dimension Reduction Scheme for Texture Pixels. If $|G(I_{ij})| \geq T$, then the central pixel is a texture pixel. In this case, in order to reduce 9-dimensional probability statistics to 4-dimensional probability statistics, we must pick out pixels that are greatly deviated from the 9-pixel group to minimize the overall impact.

(1) It is necessary to determine which pixel is the most deviated from the 9-pixel group. The easiest way is to compare $|x_i - \overline{x}|$ which means difference between each pixel and the mean of pixels in the group. Pixel number within a 9-pixel group is shown in Figure 4.

The mean $\overline{x}$ can be obtained in the following way:

$$\overline{x} = \frac{1}{9} A_{ij} * \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{14}$$

(2) Based on $|x_i - \overline{x}|$, look for the target pixel x_m with the largest deviation,

$$x_m \in \left\{x_i \mid \max\left(\left|x_i - \overline{x}\right|\right\}\right. \tag{15}$$

By comparison to get the maximum value of $|x_i - \overline{x}|$ and its corresponding target pixel x_i, if there is more than one pixel satisfying the requirement, then select the pixel having weak correlation with the central pixel (correlation of D-neighbor pixel is weaker than 4-neighbor pixel) as the target pixel (if there are still more than one, the target pixel is determined by a random selection method). According to the position of target pixel x_m, we can get the dimension deduction scheme for texture pixels, which is shown in Figure 5.

If the target pixel is the upper left pixel x_1 of the 9-pixel group, the lower right 4 pixels (x_5, x_6, x_8, x_9) are counted, as shown in Figure 5(a).

If the target pixel is the upper pixel x_2 of the 9-pixel group, the lower left 4 pixels (x_4, x_5, x_7, x_8) are counted, as shown in Figure 5(b).

If the target pixel is the upper right pixel x_3 of the 9-pixel group, the lower left 4 pixels (x_4, x_5, x_7, x_8) are counted, as shown in Figure 5(c).

If the target pixel is the left pixel x_4 of the 9-pixel group, the lower right 4 pixels (x_5, x_6, x_8, x_9) are counted, as shown in Figure 5(d).

If the target pixel is the central pixel x_5 of the 9-pixel group, no statistics are performed.

If the target pixel is the right pixel x_6 of the 9-pixel group, the upper left 4 pixels (x_1, x_2, x_4, x_5) are counted, as shown in Figure 5(e).

If the target pixel is the lower left pixel x_7 of the 9-pixel group, the upper right 4 pixels (x_2, x_3, x_5, x_6) are counted, as shown in Figure 5(f).

If the target pixel is the lower pixel x_8 of the 9-pixel group, the upper right 4 pixels (x_2, x_3, x_5, x_6) are counted, as shown in Figure 5(g).

If the target pixel is the lower right pixel x_9 of the 9-pixel group, the upper left 4 pixels (x_1, x_2, x_4, x_5) are counted, as shown in Figure 5(h).

The purpose of the above processing is to weaken the influence of texture pixels to steganographic and reduce the loss of measure accuracy caused by 9-dimensional probability statistics being reduced to 4-dimensional probability statistics.

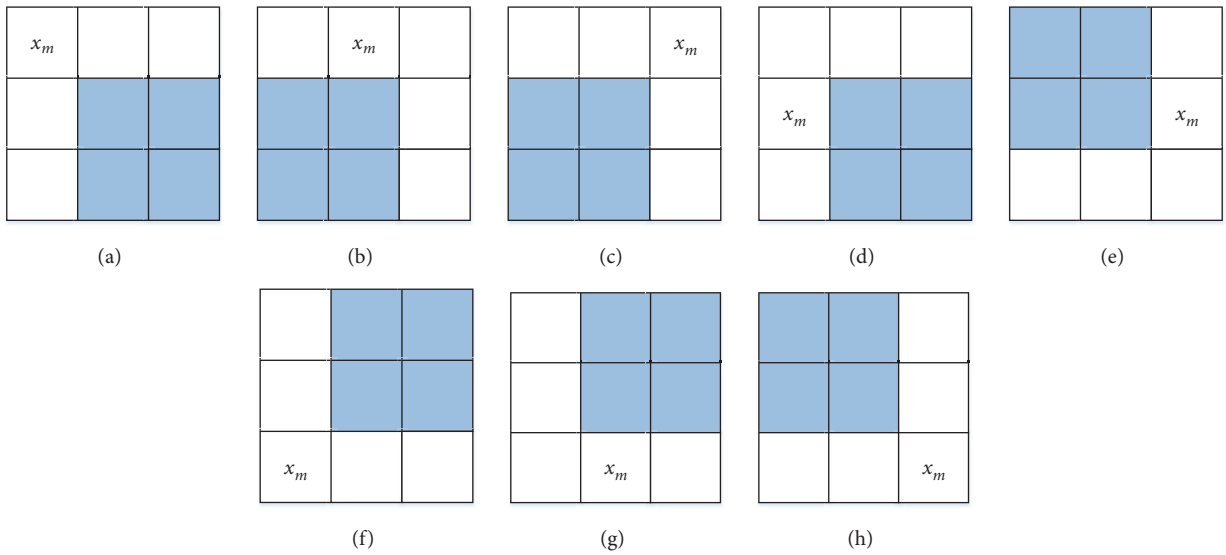

Figure 5: Target pixel and dimension reduction scheme for texture pixels.

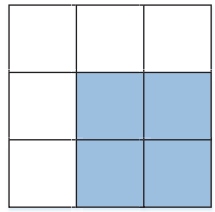

Figure 6: Probability statistical object when $|x_5 - \overline{x}| > T_z$.

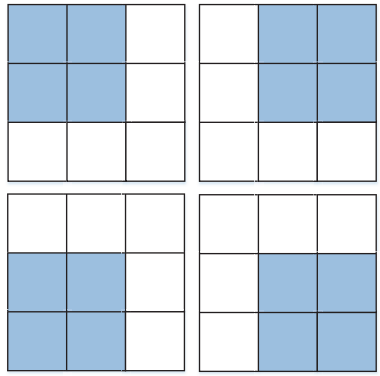

Figure 7: Four probability statistical objects when $|x_5 - \overline{x}| \leq T_z$.

(2) Dimension Reduction Scheme for Nontexture Pixels. If $|G(I_{ij})| < T$, then the central pixel is a nontexture pixel. In this case, it is necessary to determine whether the central pixel is a singular pixel, that is, whether the central pixel is far away from its neighborhood pixels:

If $|x_5 - \overline{x}| \gg 0$ (setting a threshold T_z, it is equivalent to $|x_5 - \overline{x}| > T_z$) meaning the central pixel is a singular pixel, the lower right 4 pixels (x_5, x_6, x_8, x_9) are counted, as shown in Figure 6. The probability of this situation is extremely low.

If $|x_5 - \overline{x}| \leq T_z$, then according to the method shown in Figure 7, four groups of 4 pixels are counted. Through counting multiple times, it can compensate for the disadvantages of low dimensional statistics and emphasize that embedding modification occurring on nontexture pixels has a great influence on steganographic security.

Associate threshold T_z with threshold T defined in Section 4.1, $T_z \geq 2T$. Generally, $T_z = 2T$.

4.3. Algorithm Description for Proposed Measure Method. See Algorithm 1.

5. Experiments

The experiments use BOSSBase 1.01 [8] as the image library, and MATLAB R2016a as the experimental platform. The processor is Intel(R) Pentium(R) CPU G2130 @ 3.20 GHz. In the experiment, three spatial image steganography algorithms including two adaptive steganography algorithms (HOGO [12] and HILL [13]) and LSBM (Least Significant Bit Matching) are selected for experimental analysis. Besides, we also select a JPEG image steganography algorithm J-UNIWARD [14] for experimental analysis. Sections 5.1–5.3 are experiments for spatial image steganography; and Section 5.4 is for J-UNIWARD.

5.1. Effectiveness of the Proposed Measure Method. Two different images (Image 1 and Image 2, as shown in Figure 8) are selected from the image library. We make three comparative experiments to demonstrate the effectiveness of the proposed measure method.

(1) Comparing the differences of the steganographic security measures of the two images with the same embedding rate ($\alpha = 0.4$) and the same spatial image steganography algorithm, the results are shown in Figures 8(a) and 8(b).

Image 1

$\alpha = 0.4$, D_{KL} (HILL)=2.19878

$\alpha = 0.4$, D_{KL} (HUGO)=2.34387

$\alpha = 0.4$, D_{KL} (LSBM)=4.71428

(a)

Image 2

$\alpha = 0.4$, D_{KL} (HILL)=0.20011

$\alpha = 0.4$, D_{KL} (HUGO)=0.25344

$\alpha = 0.4$, D_{KL} (LSBM)=0.30240

(b)

Image 1

$\alpha = 0.4$, D_{KL} (HILL)=2.19878

$\alpha = 0.2$, D_{KL} (HILL)=1.05996

(c)

Figure 8: Settings and results of the effectiveness experiments.

Input: Payload α, Cover image C, Stego image S
Output: Value of steganographic security measure D

Initialize target-image $I = C$; $f(x_k, x_m, x_n, x_r) = 0$
[m,n]= size of (I)
calculate gradient Gx, Gy using *Equ.*(11)
$T_0 = 6$
while $|\Omega| - m \cdot n \cdot \alpha > \varepsilon$ $(\Omega = \{I_{ij} \mid |G(I_{ij})| \geq T_i\})$
  $k++, T_k = T_{k-1} + 2$
end
$T = T_{k-1}, T_z = 2T$
for i=1:511
  for j=1:511
  if $|G_{ij}| = \sqrt{Gx_{ij}{}^2 + Gy_{ij}{}^2} \geq T$ //*texture pixels*
    calculate $\overline{x}^{ij}$ using *Equ.*(14)
    $|x_h^{ij} - \overline{x}^{ij}|, h = 1, 2, ..., 9$
    look for $x_{h'}^{ij}$ make max $|x_{h'}^{ij} - \overline{x}^{ij}|$ established
    if $h' = 1 or 4$ $f(x_5, x_6, x_8, x_9) + +$ end
    if $h' = 2 or 3$ $f(x_4, x_5, x_7, x_8) + +$ end
    if $h' = 6 or 9$ $f(x_1, x_2, x_4, x_5) + +$ end
    if $h' = 7 or 8$ $f(x_2, x_3, x_5, x_6) + +$ end
    else if $|x_5 - \overline{x}| > T_z$ //*non-texture pixels*
      $f(x_5, x_6, x_8, x_9) + +$
      else
        $f(x_1, x_2, x_4, x_5) + +$
        $f(x_2, x_3, x_5, x_6) + +$
        $f(x_4, x_5, x_7, x_8) + +$
        $f(x_5, x_6, x_8, x_9) + +$
      end
    end
  end
end
calculate $P_C(x_k, x_m, x_n, x_r) = f(x_k, x_m, x_n, x_r) / \sum f(x_\lambda, x_\eta, x_\tau, x_\mu)$
let $I = S$ repeat step 2-30 to get $P_S(x_k, x_m, x_n, x_r)$
return D using *Equ.*(3).

Algorithm 1

(2) Comparing the differences of the steganographic security measures of the same image with the same embedding rate ($\alpha = 0.4$) but with different steganography algorithms (HUGO, HILL, LSBM), the results are shown in Figure 8(a) or Figure 8(b).

(3) Comparing the differences of the steganographic security measures of the same image with the same steganography algorithm (HILL) but with different embedding payloads ($\alpha = 0.2$ and $\alpha = 0.4$), the result is shown in Figure 8(c).

Table 1: Some experimental results of the HILL algorithm.

	Measure Value of 4 dimensional probability statistics			Measure Value of proposed method			Difference of Chang Ratio
	HILL (0.2)	HILL (0.4)	Change Ratio	HILL (0.2)	HILL (0.4)	Change Ratio	
1	1.02092	2.08164	103.90%	0.73296	1.53317	109.18%	5.28%
2	0.89417	1.71277	91.55%	0.63163	1.23047	94.81%	3.26%
3	1.34281	2.32159	72.89%	0.76800	1.37687	79.28%	6.39%
4	1.43922	2.66047	84.86%	0.78199	1.48413	89.79%	4.93%
5	0.90536	1.52810	68.78%	0.61658	1.05371	70.90%	2.11%
6	1.10897	2.12113	91.27%	0.95001	1.86434	96.24%	4.97%
7	1.25125	2.44827	95.67%	1.04682	2.10483	101.07%	5.40%
8	0.98012	1.66209	69.58%	0.45888	0.79972	74.28%	4.70%
9	0.44683	0.88066	97.09%	0.27333	0.54846	100.66%	3.57%
10	0.70805	1.02537	44.82%	0.24943	0.38313	53.60%	8.79%
11	0.31410	0.47564	51.43%	0.12727	0.20011	57.23%	5.80%
12	0.91659	1.63704	78.60%	0.75807	1.40109	84.82%	6.22%
13	1.16346	2.17729	87.14%	0.75297	1.45461	93.18%	6.04%
14	1.32227	2.57819	94.98%	0.84763	1.70640	101.31%	6.33%
15	0.62734	1.14779	82.96%	0.28477	0.53467	87.75%	4.79%
16	1.29864	2.53750	95.40%	0.65260	1.30918	100.61%	5.21%
17	1.22362	2.06343	68.63%	0.70746	1.20782	70.73%	2.09%
18	1.17480	2.40565	104.77%	1.05996	2.19878	107.44%	2.67%
19	1.33475	2.55500	91.42%	0.90483	1.76291	94.83%	3.41%
20	0.84656	1.50879	78.23%	0.61633	1.11217	80.45%	2.22%

Figures 8(a) and 8(b) show that when the payload is 0.4, the value of steganographic security measure of Image 2 is lower than that of Image 1 for all three steganography algorithms, and the steganographic security of Image 2 is higher. Comparing Image 1 with Image 2, they all have a high texture complexity and texture pixels in Image 1 distribute widely, which causes embedding modification to Image 1 more scattered. Therefore, more pixel groups would be modified and final measure values would be higher. It can be seen from the results of Figure 8 that the proposed steganographic security measure method can effectively quantify steganographic security and can accurately quantify the relationship of steganographic security with algorithm, cover image features, and embedding payload.

5.2. Accuracy of the Proposed Measure Method. In order to show that the steganographic security measure method proposed is more accurate, compare it with the measure method of calculating KL divergence by directly using 4-dimensional probability statistics. 50 images were randomly selected from the image library, and adopt these two measure methods to get their KL divergence values between each cover image and its stego image processed by HILL or HUGO. Since the total number of 4 pixel groups used in probability statistics of two measure method is different, the measure values cannot directly reflect each method's accuracy. Change ratio which can avoid this problem can be used to evaluate measure accuracy. In the experiment, we adopt the change ratio of payload changed from 0.2 to 0.4 as direct data for evaluating the accuracy of each measure method. Change ratio can be calculated in the following way:

$$CR = \frac{D(\alpha = 0.4) - D(\alpha = 0.2)}{D(\alpha = 0.2)} \tag{16}$$

where CR denotes change ratio and D indicates measure value at a certain payload.

In the experiment, we compared the difference of measure value and the difference of change ration between the two measure methods under algorithms HILL, HUGO, and LSBM. Some experimental results of HILL algorithm are shown in Table 1. Some experimental results of HUGO algorithm are shown in Table 2. And Some experimental results of LSBM algorithm are shown in Table 3 (only 20 of them are listed due to paper space limitations).

The effectiveness of the steganographic security measure method proposed in the paper can also be demonstrated from the data in Tables 1, 2, and 3. From the comparison between the proposed method and the method based on 4-dimensional probability statistics in change ratio when embedding payload is changed from 0.2 to 0.4, it can be clearly found that change ratio of the proposed method is larger. And it indicates that the proposed method is more sensitive to embedding modifications and is more accurate. At the same time, the two measure methods sometimes show different conclusions due to the data shown in Tables 1 and 2. For example, as for the 18th data and 19th data in Table 2,

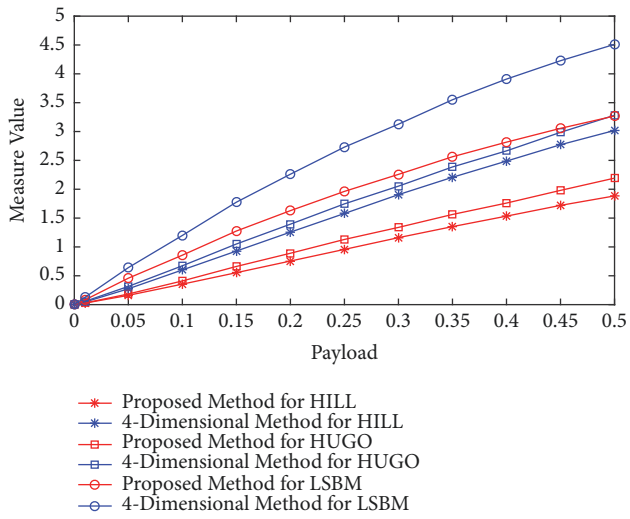

Figure 9: Changes of measure values with embedding payload.

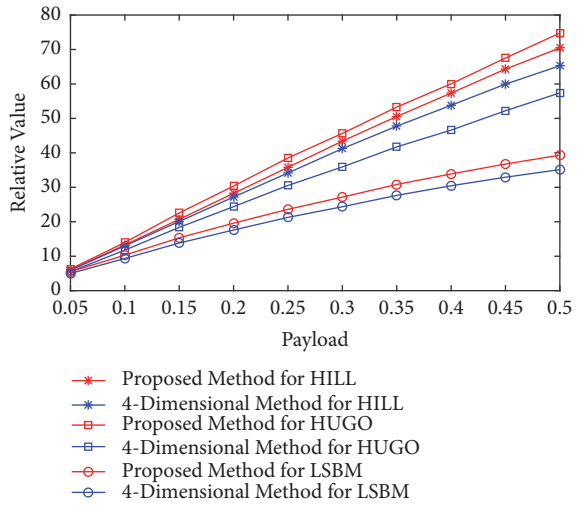

Figure 10: Changes of relative values with embedding payload.

the proposed method shows that steganography of 19th image is more secure while the method based on 4-dimensional probability statistics shows that steganography of 18th image is more secure.

5.3. Changes of Steganographic Security Measure with Embedding Payload. This experiment is designed to compare the values of the proposed steganographic security measure method and the method based on 4-dimensional probability statistics at different embedding payload. 100 images in Bossbase 1.01 image library were randomly selected as experimental database, and average measure values of HILL, HUGO, and LSBM were calculated when the embedding payloads were 0.01, 0.05, 0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4, 0.45, and 0.5. Average measure values at selected payloads are shown in Table 4 and Figure 9.

Both the proposed method and the method based on 4-dimensional probability statistics adopt the frequency statistics to approximate the probability. Total number of frequency counts (total number of pixel groups) of the two methods are different. So, in view of the same cover and the same measure method, the total number of frequency statistics is the same, so we can take a "relative value" to show the accuracy of the security measure method. "Relative value" can be calculated as follows:

$$R_M^A(\alpha) = \frac{D_M^A(\alpha)}{D_M^A(0.01)} \tag{17}$$

where $R_M^A(\alpha)$ represents relative value at payload α using steganography algorithm A and measure method M; $D_M^A(\alpha)$ represents measure value at payload α using steganography algorithm A and measure method M.

Changes of relative values with embedding payload are shown in Figure 10.

Figure 9 shows that both two methods can describe the change of steganographic security with the embedding payload. Figure 10 shows that relative values of proposed method for the same steganographic schemes are all larger than that of the method based on 4-dimensional probability statistics, which indicates that measure method based on low dimensional (4-dimensional) probability statistics overestimates the steganographic security and is less accurate. At the same time, the results indicate that the proposed measure method is more sensitive to the change of the embedding payloads and the proposed measure method is more accurate.

The above results show that the proposed method is more accurate and performs much better.

5.4. The Performance of Steganographic Security Measure on JPEG Image Steganography. The experiment in this section still uses the Bossbase 1.01 as the image library. Images are JPEG-compressed to obtain the corresponding JPEG images (Quality=75, bitDepth=8). Adopting a typical JPEG image steganography algorithm J-UNIWARD [14], the compressed JPEG images are modified to obtain stego images in JPEG format. Since the proposed security measure is carried out through statistical analysis of pixel values, it is necessary to read the cover images and stego images in spatial discrete pixel values when evaluating the steganographic security of the JPEG image steganography. In short, JPEG images need to be inversely transformed into spatial images before steganographic security measure. We perform experiments similar to previous sections, and the results are shown in Table 5 and Figure 11.

From the data in Table 5, it can be seen that measure value of J-UNIWARD is higher than HILL or HUGO. This is because JPEG image steganography modifies the DCT coefficients of the image block, and each embedding modification affects more pixels. It can be seen from Table 5 and Figure 11 that the proposed security measure can effectively measure the changes of steganographic security of JPEG images with image features and payload, and it is slightly more accurate than 4-dimensional probability statistics.

Table 2: Some experimental results of the HUGO algorithm.

	Measure Value of 4 dimensional probability statistics			Measure Value of proposed method			Difference of Chang Ratio
	HUGO (0.2)	HUGO (0.4)	Chang Ratio	HUGO (0.2)	HUGO (0.4)	Chang Ratio	
1	1.30987	2.48358	89.60%	0.84043	1.69914	102.18%	12.57%
2	1.24200	2.14255	72.51%	0.70168	1.30778	86.38%	13.87%
3	1.44736	2.53561	75.19%	0.78758	1.44846	83.91%	8.72%
4	1.45431	2.87307	97.56%	0.74110	1.53700	107.39%	9.84%
5	1.27310	2.29136	79.98%	0.80768	1.48351	83.68%	3.69%
6	1.34469	2.57513	91.50%	1.04682	2.10384	100.97%	9.47%
7	1.39926	2.76546	97.64%	1.06538	2.21430	107.84%	10.20%
8	1.16290	1.91906	65.02%	0.51397	0.88650	72.48%	7.46%
9	0.93269	1.57508	68.87%	0.52490	0.91122	73.60%	4.72%
10	1.19879	1.62380	35.45%	0.39717	0.56526	42.32%	6.87%
11	0.48139	0.63090	31.06%	0.18233	0.25344	39.00%	7.94%
12	1.13675	1.95546	72.02%	0.88165	1.57983	79.19%	7.17%
13	1.33889	2.43350	81.75%	0.81350	1.54125	89.46%	7.70%
14	1.42714	2.85344	99.94%	0.81764	1.73621	112.34%	12.40%
15	1.24942	2.25357	80.37%	0.53311	0.97934	83.70%	3.33%
16	1.46831	2.80853	91.28%	0.67017	1.36130	103.13%	11.85%
17	1.36486	2.53497	85.73%	0.74542	1.42298	90.90%	5.17%
18	1.33739	2.69973	101.87%	1.11746	2.34387	109.75%	7.89%
19	1.42747	2.83689	98.74%	0.90182	1.87308	107.70%	8.96%
20	1.14644	2.06412	80.05%	0.79610	1.45723	83.05%	3.00%

Table 3: Some experimental results of the LSBM algorithm.

	Measure Value of 4 dimensional probability statistics			Measure Value of proposed method			Difference of Chang Ratio
	LSBM (0.2)	LSBM (0.4)	Chang Ratio	LSBM (0.2)	LSBM (0.4)	Chang Ratio	
1	2.3620	4.0083	69.70%	1.8435	3.1582	71.32%	1.62%
2	1.5050	2.5938	72.35%	1.0403	1.8095	73.94%	1.59%
3	1.5571	2.6633	71.04%	0.9881	1.6993	71.98%	0.93%
4	1.9854	3.3944	70.97%	1.1598	2.0167	73.88%	2.90%
5	1.6512	2.8346	71.67%	1.1484	1.9933	73.58%	1.92%
6	2.5666	4.3860	70.89%	2.3622	4.0406	71.05%	0.16%
7	2.8742	4.9373	71.78%	2.5766	4.4360	72.16%	0.38%
8	1.0682	1.8674	74.82%	0.5608	0.9976	77.87%	3.05%
9	1.0515	1.8061	71.77%	0.6704	1.1520	71.84%	0.08%
10	0.7674	1.3572	76.86%	0.3412	0.6426	88.33%	11.47%
11	0.3166	0.5782	82.62%	0.1519	0.3024	99.05%	16.43%
12	1.6482	2.8817	74.83%	1.4669	2.5623	74.67%	-0.16%
13	1.8257	3.1334	71.63%	1.2902	2.2171	71.84%	0.21%
14	2.5363	4.3696	72.28%	1.7830	3.0952	73.59%	1.31%
15	1.2773	2.2376	75.19%	0.6221	1.1279	81.31%	6.12%
16	1.8769	3.2131	71.19%	1.0351	1.7893	72.86%	1.67%
17	1.7534	3.0413	73.45%	1.0460	1.8486	76.74%	3.29%
18	2.9332	5.0360	71.69%	2.7375	4.7143	72.21%	0.52%
19	2.1540	3.7006	71.80%	1.5181	2.6244	72.87%	1.08%
20	1.4750	2.5593	73.51%	1.0913	1.8978	73.91%	0.40%

Table 4: Average measure values at selected payloads.

Payload	Proposed Method (HILL)	Method based on 4-Dimensional Statistics (HILL)	Proposed Method (HUGO)	Method based on 4-Dimensional Statistics (HUGO)	Proposed Method (LSBM)	Method based on 4-Dimensional Statistics (LSBM)
0.01	0.026748	0.04624	0.029323	0.057184	0.083131	0.128378
0.05	0.16085	0.274677	0.184445	0.31584	0.458272	0.641383
0.1	0.355073	0.601163	0.410599	0.673072	0.85707	1.199006
0.15	0.553858	0.928578	0.661722	1.050773	1.275703	1.7755
0.2	0.755488	1.256531	0.890548	1.394526	1.629017	2.260528
0.25	0.957277	1.579468	1.129779	1.74628	1.96266	2.730451
0.3	1.160906	1.906298	1.338445	2.053393	2.257668	3.127282
0.35	1.352058	2.207212	1.562899	2.38607	2.562883	3.550725
0.4	1.533851	2.487873	1.760218	2.664928	2.816241	3.908961
0.45	1.720401	2.7717	1.980265	2.98618	3.055427	4.227427
0.5	1.884053	3.018689	2.192547	3.282173	3.269811	4.510741

Table 5: Some experimental results of the J-UNIWARD algorithm.

	Measure Value of 4-dimensional probability statistics			Measure Value of proposed method			Difference of Chang Ratio
	LSBM (0.2)	LSBM (0.4)	Chang Ratio	LSBM (0.2)	LSBM (0.4)	Chang Ratio	
1	2.3980	3.8116	58.95%	1.7478	2.8700	64.20%	5.25%
2	1.5503	2.5022	61.40%	1.0278	1.7299	68.31%	6.91%
3	1.8447	2.6529	43.81%	1.0771	1.5964	48.21%	4.40%
4	2.1020	3.0682	45.97%	1.1829	1.7872	51.08%	5.12%
5	1.3284	2.2791	71.56%	0.9469	1.6698	76.34%	4.78%
6	2.6214	4.2552	62.33%	2.2499	3.7877	68.35%	6.02%
7	2.9595	4.7336	59.95%	2.5685	4.2482	65.40%	5.45%
8	1.3384	1.9594	46.40%	0.6621	1.0006	51.13%	4.73%
9	0.9555	1.5528	62.52%	0.6048	1.0036	65.93%	3.41%
10	0.7076	1.1481	62.24%	0.2512	0.4259	69.56%	7.32%
11	0.3445	0.5069	47.12%	0.1264	0.1964	55.35%	8.24%
12	1.6758	2.5975	55.00%	1.3909	2.2457	61.46%	6.46%
13	1.9713	3.0271	53.56%	1.2981	2.0635	58.96%	5.41%
14	2.9178	4.5013	54.27%	1.8871	3.0126	59.64%	5.36%
15	0.8939	1.7379	94.41%	0.4174	0.8262	97.96%	3.55%
16	2.3003	3.4792	51.25%	1.2138	1.8955	56.16%	4.91%
17	1.3965	2.3239	66.41%	0.8405	1.4308	70.23%	3.82%
18	3.3994	5.4091	59.12%	3.0998	5.0776	63.81%	4.68%
19	2.3899	3.9014	63.25%	1.6657	2.7949	67.80%	4.55%
20	1.6447	2.6120	58.81%	1.2476	2.0352	63.13%	4.32%

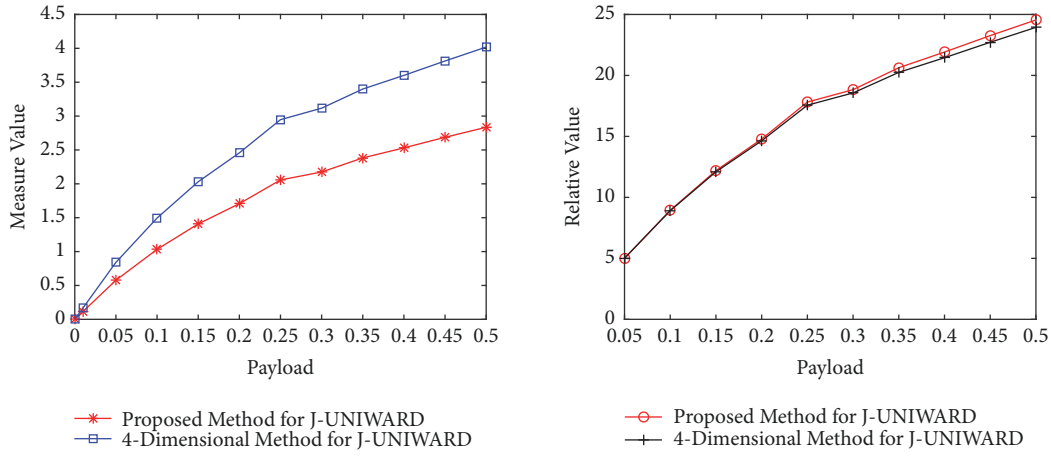

Figure 11: Results of J-UNIWARD with embedding payload.

6. Conclusions

In this paper, a feasible steganographic security measure method based on high dimensional KL divergence is proposed. The proposed steganographic security measure is considered from the perspective of stegan (the sender) to conduct a reference steganographic security measure. It is proved that embedding modification to the pixel groups with small statistical probability could get higher steganographic security, and higher dimensional probability statistics is more accurate for steganographic security measure. It is reasonable to use 9-dimensional probability statistics in security measure by analyzing the imaging principle. And dimension reduction scheme is proposed to obtain a feasible steganographic security measure method. Experiments on spatial image steganography and JPEG image steganography show the effectiveness and accuracy of the proposed measure method. However, the threshold determination of the proposed method needs to be further improved in terms of complexity and rationality. We will make further study

on the relationship between image texture complexity and steganographic security.

Data Availability

The image data supporting this Systematic Review are from previously reported studies and datasets, which have been cited. The processed data are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation under grant 61601517.

References

[1] J. Fridrich, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," *Proceedings of SPIE - The International Society for Optical Engineering*, 2015.

[2] R. R. Chhikara, P. Sharma, and L. Singh, "An improved dynamic discrete firefly algorithm for blind image steganalysis," *International Journal of Machine Learning and Cybernetics*, vol. 9, no. 5, pp. 1–15, 2018.

[3] P. Zhong, M. Li, K. Mu, J. Wen, and Y. Xue, "Image steganalysis in high-dimensional feature spaces with proximal support vector machine," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 11, no. 1, pp. 78–89, 2019.

[4] J. Zöllner, H. Federrath, H. Klimant et al., "Modeling the security of steganographic systems," in *Proceedings of the International Workshop on Information Hiding*, pp. 344–354, 1998.

[5] C. Cachin, "An information-theoretic model for steganography," *Information and Computation*, vol. 192, no. 1, pp. 41–56, 2004.

[6] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Steganalysis for Markov cover data with applications to images," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 275–287, 2006.

[7] Z. Zhang, F. Qu, G.-J. Liu, J.-W. Wang, Y.-W. Dai, and Z.-Q. Wang, "A novel security evaluation method for digital image steganography based on higher-order markov chain model," *Information and Control*, vol. 39, no. 4, pp. 455–461, 2010.

[8] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system: the ins and outs of organizing BOSS," in *Information Hiding*, vol. 6958, pp. 59–70, Springer, Berlin, Germany, 2011.

[9] M. Gupta, J. Dosad, and P. Goyal, "Performance analysis of median filter demosaicking algorithm using new extended bilinear demosaicking," in *Proceedings of the 2nd International Conference on Computer Vision & Image Processing*, vol. 704, pp. 47–63, 2018.

[10] X. Ma and Y. Nie, "Optimized approach of Sobel operator of image edge detection using model-based design," *RISTI: Revista Iberica de Sistemas e Tecnologias de Informacao*, vol. e6, pp. 401–412, 2016.

[11] N. Mathur, S. Mathur, and D. Mathur, "A novel approach to improve sobel edge detector," *Procedia Computer Science*, pp. 431–438, 2016.

[12] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," *Lecture Notes in Computer Science*, vol. 6387, pp. 161–177, 2010.

[13] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proceedings of the IEEE International Conference on Image Processing*, pp. 4206–4210, 2014.

[14] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 1, pp. 1–13, 2014.