AN ATTACK TO BPCS-STEGANOGRAPHY USING COMPLEXITY HISTOGRAM AND COUNTERMEASURE

Michiharu Niimi, Tomohito Ei, Hideki Noda, Eiji Kawaguchi

Kyushu Institute of Technology,
1–1 Sensui–Cho, Tobata, Kitakyushu
804–8550 Japan

Bruce Segee

University of Maine,
5708 Barrows Hall, Orono, ME
04469–5708, USA

ABSTRACT

This paper discusses an attack to BPCS-Steganography (Bit-Plane Complexity Segmentation-Steganography) and presents a countermeasure. BPCS is an image-based steganographic method. BPCS embeds secret data by replacing blocks that appear noise-like on bit-planes. Blocks on bit-planes are categorized as a "noise-like region" or an "informative region" by means of the binary-image feature called complexity. When the complexity distribution of noise-like blocks is different from the complexity distribution of the secret data that replaces those blocks, we can see an unusual shape in the form of a valley in the complexity histogram that represents the relative frequency of occurrence of the various complexities. This would be a signature of BPCS. Because steganography must hide the existence of the secret message, the signature should be removed from steganographic images. We present a method for making embedded binary patterns that quasi-preserves the complexity distribution.

1. INTRODUCTION

BPCS-Steganography (Bit-Plane Complexity Segmentaion-Steganography) [1–4] uses image segmentation based on the measure called complexity. The complexity is defined over a local region within a binary image. Local regions within a binary image can be classified as "informative" or "noise-like" by using the complexity measure. The human eye is unable to perceive the replacement of noise-like regions in an image with random binary data. This property allows us to embed secret data into noise-like regions if the secret data is a random pattern.

BPCS allows the replacement of about 40% of cover images with secret data without any image degradation that can be perceived by humans. Through several experiments, however, we have confirmed that the shape of the complexity histogram of the image with secret data embedded is, in general, different from that of the original one. Here the complexity histogram represents the relative frequency of occurrence of the various complexities in the binary image. The unnatural distribution of complexity histogram, hence, can be used as a signature or a distinguishing mark between natural images and images with information embedded by BPCS. Since the term "steganography" literally means "covered writing," steganographic techniques should not be distinguishable from cover images [5–7].

In this paper, we discuss this possible attack to BPCS and present a countermeasure that removes this distinguishing mark. The problem of BPCS is that all bits in noise-like regions are used for secret data. This causes the the complexity of secret data to be different from that of the original noisy pattern replaced with secret information. In the proposed method, only half of the bits in noise-like regions are used for secret data. The remaining half of the bits are used to adjust the complexity measure in those regions. The adjustment of complexity is performed by changing the pixel values of the bits in the noise-like regions that are not used for encoding secret data.

2. PRINCIPLES OF EMBEDDING USING BPCS[1]

2.1. Complexity Measure

The purpose of a complexity measure is to measure the degree to which a binary image pattern contains significant information for the visual system. In other words, a complexity measure represents the density of the black or white pattern. The complexity measure we use is based on the border length of the binary image, and the border length for a binary pattern depends on the definition of the neighborhood. In this paper, we use four connectivity, so the total length of the black-and-white border is equal to the summation of the number of color-changes along the rows and columns in the interior of the image. We assume the image frame is always a square of size $m \times m$ pixels. Therefore, the minimum border length is 0 (for either an all black or an all white pattern), while the maximum border length is $2 \times m \times (m-1)$ (for a checkerboard pattern). Thus, the

0-7803-8554-3/04/$20.00 ©2004 IEEE.

image complexity measure is defined by the following.

$$\alpha = \frac{k}{2 \times m \times (m-1)} \quad (1)$$

where, k is the total length of the black-and-white border in the image.

2.2. Method to Embed Using Complexity Segmentation

The process of segmenting an image into informative and noise-like regions is performed using the complexity measure. For gray scale cover images, a number of binary images can be produced by bit-plane decomposition, and the complexity segmentation performed on each bit-plane. If the complexity threshold is denoted by α_{TH}, noise-like regions are defined as regions having a complexity value of α_{TH} or greater, and informative regions are defined as regions having a complexity value that is less than α_{TH}. In typical BPCS-Steganography, we replace the noise-like regions with our secret data and leave the informative regions alone.

Conversely, when we extract the secret information, we rely on the fact that the simple regions (informative regions of low complexity) do not contain secret data, and the complex regions (noise-like regions of high complexity) do. All secret data must therefore be of high complexity so we can identify it. If the binary pattern of the secret data mapped on a local region is simple, we need to apply the conjugation operation [1] to it. This operation transforms a simple pattern into a complex pattern. We also need to keep track of which complex data patterns had such conjugation applied to them. We call this information a *conjugation map*.

2.3. Changes in Complexity Histograms

Let P_{ORG} be a block replaced with secret data and P_{EMB} be a squared binary pattern mapped from secret data. From a principle of embedding in BPCS, the complexity of P_{ORG} and P_{EMB} satisfies the following conditions

$$\alpha_{TH} \leq \alpha(P_{ORG}) \quad \text{and} \quad \alpha_{TH} \leq \alpha(P_{EMB}) \quad (2)$$

where "$\alpha(P_{ORG})$" means the complexity of P_{ORG} and α_{TH} represents the threshold used to determine whether the subimage is noise-like or not. However the following equation is not always satisfied.

$$\alpha(P_{ORG}) = \alpha(P_{EMB}) \quad (3)$$

This causes a change in the shape of the complexity histogram. In order to explain this fact, we will look at the complexity histogram in greater detail. As mentioned above, the complexity histogram used in this paper represents the relative frequency of occurrence of the various complexities in a binary pattern. Because the complexity of an original binary pattern is rarely equal to that of a binary pattern mapped from secret data, a change in shape in the complexity histogram will generally occur. Binary patterns having a complexity value that exceeds the threshold are substituted for noise-like binary patterns (secret data) having the complexity distribution described below.

One might assume that the complexities of random binary patterns of size $n \times n$ would follow a normal distribution, and indeed, this has been experimentally verified. [1]. Thus, for BPCS, patterns in bit-plane images that are replaced by secret information generally have a normal distribution of complexities, because the secret information is noise-like.

We embedded pseudo random data into the gray scale image called GIRL (256 $\times$ 256, 8 bit/pixel) using BPCS with $\alpha_{TH} = 0.36$. Local regions on all bit-planes having more than the threshold in complexity were substituted with pseudo random data. Fig. 1 shows complexity histograms of the bit-planes using BPCS with $\alpha_{TH} = 0.36$. We can see an unusual shape in the form of a valley near the threshold. The distribution of the substituted pattern (complexities greater than the threshold) is a normal distribution. In the middle bit-planes, noise-like patterns and non noise-like patterns are mixed. In embedding in these planes, patterns that are above the threshold change to the normal distribution and a discontinuity in the complexity measure histogram around the threshold becomes noticeable.

3. PROPOSED METHOD

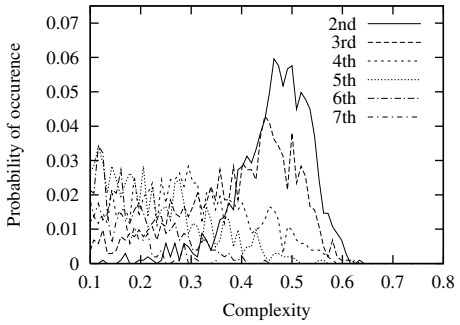
In BPCS, binary patterns for the replacement of noisy blocks are generated from only secret data. In the proposed method, on the other hand, binary patterns are generated both from secret data and the bits used to adjust the complexity.

3.1. Approach to adjust complexity

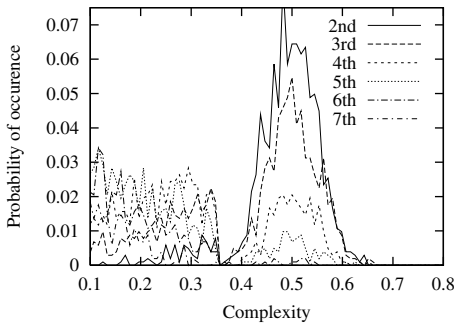
In order to adjust the complexity of blocks in binary images, we use only half of the pixels in the image. The remaining half of the pixels are used for adjusting complexity. Pixels of the images are divided into two groups, *group A* and *group B*. Pixels in *group A* are used for secret information and pixels in *group B* are used for adjusting complexity. The pixels of group A are the pixels for secret data, and are termed *PSD*. The pixels of group B are the pixels for adjusting complexity, and are termed *PAC*. The locations of the PSD and PAC correspond to a checkerboard pattern. Fig. 2 shows the bit assignment of PSD and PAC in the images.

In the proposed method, we redefine noisy patterns as

$$0.5 - \delta \leq \alpha(P) \leq 0.5 + \delta. \quad (4)$$



(a) Before embedding



(b) After embedding

Fig. 1. Complexity histograms of natural image and those of the image with secret data embedded

where P is a binary image and δ is a constant coefficient satisfying $0 < \delta \leq 0.5$.

Next, to generate the binary patterns for embedding, we divide a bit-plane of the cover image into $m \times m$ size blocks. Let $P^i(i = 1, 2, \cdots, N)$ be the noise-like blocks and $C^i(= \alpha(P^i))$ be the complexity of P^i. The complexity histogram of blocks that are replaced with secret data is denoted by $h_{ORG}(c), (0.5 - \delta \leq c \leq 0.5 + \delta)$. $h_{ORG}(c)$ is the number of blocks of complexity c. In order to represent the complexity histogram of blocks that have been replaced with secret data, we define the another histogram denoted by $h_{EMB}(c), (0.5-\delta \leq k \leq 0.5+\delta)$, and initialize $h_{EMB}(c)$ to "0."

Firstly, we map a binary sequence having the size of $(m \times m)/2$ extracted from secret data on PSD in P^i. Then, we set the target complexity of P^i by the following steps.

a-1) C_{org} and e are initialized as C^i and 0 respectively.

a-2) Let k_c and k_s be $C_{org} + e$ and $C_{org} - e$. The k_c is the target complexity if the following condition is satisfied.

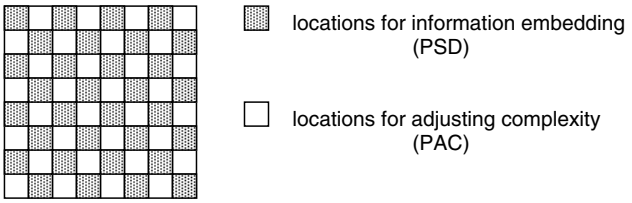


Fig. 2. information assignment

$$h_{ORG}(k_c) > h_{EMB}(k_c) \quad \text{and} \quad k_c \leq 0.5 + \delta \quad (5)$$

The k_s is also the target complexity if the following condition is satisfied.

$$h_{ORG}(k_s) > h_{EMB}(k_s) \quad \text{and} \quad 0.5 - \delta \leq k_s \quad (6)$$

If both k_c and k_s are the the target complexity, we choose one of them randomly. If k_c and k_s do not satisfy the above conditions, then the value of e is changed by

$$e \leftarrow e + \frac{1}{2 \times m \times (m-1)}, \quad (7)$$

and the above conditions are re-checked. The target complexity is denoted by C_t in the following.

The complexity of P^i is adjusted by the following steps using the target complexity and h_{EMB} and h_{ORG}. In PAC on P^i, there are pixels having the property that the complexity of P^i becomes larger by reversing its value. We denote the set of pixels having the property as B^+. There are also pixels having the property that the complexity of P^i becomes smaller by reversing its value. We denote the set of pixels having the property as B^-.

b-1) Go to the step **b-2** if P^i satisfies the following condition.

$$\alpha(P^i) < c. \quad (8)$$

Go to the step **b-3** if P^i satisfies the following condition.

$$\alpha(P^i) > c \quad (9)$$

Go to the step **b-4** if the above conditions are not satisfied, this means $\alpha(P^i) = C_t$.

b-2) Choose a pixel from B^+, reverse the its value and remove it from B^+. Choose a pixel randomly if there

are pixels having the same property. This step is repeated until $\alpha(P^i)$ is equal to C_t or greater, or B^+ is empty. In oder for P^i to satisfy noisy pattern, the pixel value of the last pixel that has been reversed is reversed if the following condition is satisfied.

$$\alpha(P^i) > 0.5 + \delta \tag{10}$$

Go to **b-4** if this step is finished.

b-3) Choose a pixel from B^-, reverse the its value and remove it from B^-. Choose a pixel randomly if there are pixels having the same property. This step is repeated until $\alpha(P^i)$ is equal to C_t or smaller, or B^- is empty. In oder for P^i to satisfy noisy pattern, the pixel value of the last pixel that has been reversed is reversed if the following condition is satisfied.

$$\alpha(P^i) < 0.5 - \delta \tag{11}$$

Go to **b-4** if this step is finished.

b-4) $h_{EMB}(c)$ is changed by the following equation.

$$h_{EMB}(\alpha(P^i)) \leftarrow h_{EMB}(\alpha(P^i)) + 1. \tag{12}$$

4. EXPERIMENTS AND DISCUSSIONS

We investigated the relation between δ and the accuracy of the adjusted complexity histogram. In the experiments, all of noise-like blocks in the cover image are replaced with random binary sequences representing secret data. In order to evaluate the accuracy in adjusting the shape of the complexity histogram, we defined the measure of the accuracy as follows.

$$\text{error} = \sum_i |h_o(i) - h_e(i)| \tag{13}$$

where $h_o(i)$ and $h_e(i)$ represent the histograms of the cover image and the stego image, respectively.

The error was calculated from $\delta = 0.04$ to 0.36 with 0.02 increments. The result is shown in Fig. 3. As can be seen, the shape of the complexity histogram with $0.1 \leq \delta \leq 0.25$ is virtually identical before embedding and after embedding.

5. CONCLUSIONS

We have proposed an improved BPCS-Steganography technique that removes an identifying signature that can be found in conventional BPCS-Steganography. The improved BPCS is robust against attacks using complexity histogram because the complexity distribution is quasi-preserved by adjusting the complexity of the embedded patterns.

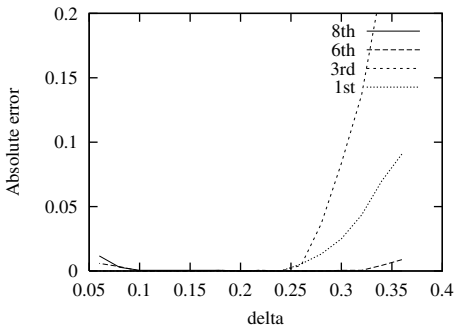


Fig. 3. Error of histogram adjustment

6. REFERENCES

[1] M. Niimi, H. Noda and E. Kawaguchi, "Steganography based on region segmentation with a complexity measure," Systems and Computers in Japan, Vol.30, No.3, pp.1–9 (1999).

[2] M. Niimi, R. O. Eason, H. Noda and E. Kawaguchi: "A method to apply BPCS-steganography to palette-based images using luminace quasi-preserving color quantization", IEICE Trans. on Fundamentals, Vol.E85-A, No.9, pp.2141–2148 (2002).

[3] R. Ouellette, H. Noda, M. Niimi and E. Kawaguchi: "Topological ordered color table for BPCS-steganography using indexed color images", IPSJ Journal, Vol.42, No.1, pp. 110–113 (2001).

[4] H. Noda, J. Spaulding, M. Shirazi and E. Kawaguchi: "Application of bit-plane decomposition steganography to JPEG2000 encoded images", IEEE Signal Processing Letters, Vol.9, No.12, pp. 410–413 (2002).

[5] S. Katzenbeisser and F. A. Petitcolas Eds.: "Information Hiding : Techniques for Steganography and Digital Watermarking", Artch House, Inc, pp.79–93 (2000).

[6] N. F. Johnson, Z. Duric and S. Jajodia: "Information Hiding : Steganography and Watermarking - Attacks and Countermeasures", Kluwer Academic Publishers, pp.47–76 (2001).

[7] P. Wayner: "Disappearing Cryptography second edition:Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, pp.303–314 (20 02).