An Estimation Approach to Extract Multimedia Information in Distributed Steganographic Images

Li Bai and Saroj Biswas
Temple University
1947 N. 12th Street
Philadelphia, PA 19122
lbai@temple.edu

Erik P. Blasch
Air Force Research Lab
2241 Avionics Cir
WPAFB, OH 45433
erik.blasch@wpafb.af.mil

Abstract – *Distributed image steganography (DIS) [8] is a new method of concealing secret information in several host images, leaving smaller traces than conventional steganographic techniques, and requiring a collection of affected images for secret information retrieval. Fusion system designs of the future will require enhanced security measures for distributed data communication. DIS, compared to other conventional steganographic techniques, can improve security and information hiding capacity because DIS leaves reduced signatures of hidden information in host images. The open literature does not offer effective detection methods and countermeasures for DIS, indicating that it can be potentially usable to criminals for unchallenged covert communication over the Internet and fusion architectures. In this paper, we explore a new information extraction method for both detecting and reversing DIS method by considering images as pseudo-random processes. The key idea is to estimate secret image as a random process, which is corrupted by a noise source (i.e. host image). The secret images may be nonlinear, non-Gaussian and non-stationary in nature, and can be disclosed by using some estimation techniques such as Kalman filtering. Our proposed method demonstrates great promise to reveal a secret image. Consequently, it is useful for intelligence gathering and information extraction in steganographic - images produced by DIS.*

Keywords: distributed image steganography, steganalysis, estimation, image quality matrix

1 Introduction

Steganography is a method that hides secret information within a body of covert communication data such that the secret information is inconspicuous using regular sensing and decoding techniques [4]. Steganography has a long history – an interesting incident has been reviewed by Anderson [1], who claims that in the 1980s, British Prime Minister Margaret Thatcher had word processors programmed to encode cabinet member's identity in the word spacing of official documents in order to determine who leaked information to the press. Needless to say, steganography can also be used for illegitimate purposes. Although steganography is not yet used as widely as cryptography, it has gained renewed interests in recent years by law enforcement agencies. Law enforcement agencies, in particular, are looking for efficient steganalysis techniques to detect, block, or disclose the secret information camouflaged in steganographic images by criminals or terrorists.

Many conventional steganographic schemes hide the secret text in a single host image. These techniques (see more complete references at [2], [3]) include least significant bit (LSB) insertion or transformation domain embedding using the *discrete cosine transform* (DCT), *discrete Fourier transform* (DFT) or *wavelet transform* (WT). Conventional steganographic methods do not have large information payload, which cannot be used to sufficiently hide a secret image. Another emerging image steganographic technique is referred to as *distributed image steganography* (DIS) which uses a (k, n) threshold-based image secret sharing technique [8] for $k \leq n$ and allows large information payload embedding by generating n steganographic images. DIS allows i) k or more steganographic images to reconstruct the secret image, and ii) $(k - 1)$ or fewer cannot reveal the secret image. Its salient features are reliability and security because the hidden information can only be read if an authorized subset of the steganographic images becomes available. Although some countermeasure methods can successfully block conventional steganographic images by altering them, these methods become useless for DIS to prevent criminals from reconstructing the secret unless all possible authorized sets of steganographic images are blocked. More seriously, it gives an alarm to criminals that the covert channel has been compromised, unsecured and untrustworthy because they cannot reconstruct the same secrets from two different sets of authorized steganographic images. Consequently, an effective countermeasure is to decode the secret information rather than to block steganographic images.

In this paper, we propose a countermeasure process for detecting and reversing DIS method by estimating secret information from steganographic images. We regard steganographic images as several pseudo-random processes, which are corrupted by a noise source (i.e. host images). The original secret images may be nonlinear, non-Gaussian and non-stationary in nature, which can be

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An Estimation Approach to Extract Multimedia Information in Distributed Steganographic Images	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Lab,2241 Avionics Cir,Wright Patterson AFB,OH,45433**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
10th International Conference on Information Fusion, 9-12 July 2007, Quebec, Canada.

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

revealed using estimation techniques. The rest of paper is organized as follows: a review of relevant research to DIS is given in section II. Our proposed countermeasure technique is presented in section III. The conclusion and future work are given in section IV.

2 Reviews of Related Researches

We describe Shamir's (k, n) threshold-based secret sharing scheme (SSS) scheme and Thien and Lin's image secret scheme using shadows. These two schemes are essential processes to protect secret image in DIS.

A. Shamir's Secret Sharing Scheme

Shamir [5] developed the idea of a (k, n) threshold-based secret sharing technique ($k \le n$). The technique allows a polynomial function of order ($k - 1$) constructed as,

$$f(x) \equiv (d_0 + d_1 x + d_2 x^2 + \cdots + d_{k-1} x^{k-1}) \bmod p . \quad (1)$$

where the value d_0 is the secret number. The n shares are (x_1, y_1), (x_2, y_2), …, (x_n, y_n) for $y_i = f(x_i)$, and p is the prime modulus used in the cryptographic computation. The polynomial function $f(x)$ is destroyed after each shareholder possesses a pair of values (x_i, y_i) so that no single shareholder knows the secret value d_0. In fact, no groups of ($k - 1$) or fewer secret shares can discover the secret d_0. On the other hand, when k or more secret shares are available, then we may set at least k linear equations $y_i = f(x_i)$ for the unknown d_i's. The unique solution to these equations shows that the secret value d_0 can be easily obtained by using Lagrange interpolation [5].

Consider a simple example for a (2, 4) threshold-based secret sharing scheme where the secret s is equal to 3. Since the threshold k is 2, we need to construct a polynomial function of the first order and randomly choose a value d_1 (say $d_1 = 2$) as

$$f(x) = 3 + 2\,x \ (mod\ 19).$$

Among four participants, we can choose four random x_i and compute the shares as

$$(1, 5), (3, 9), (4, 11), (9, 2).$$

When any two shareholders collaborate together, they will have two shares (say (1, 5) and (4, 11)). Two equations are constructed as

$$s + d_1 \ (mod\ 19) = 5,$$

$$s + d_1 4 \ (mod\ 19) = 11.$$

Clearly, the secret s can be easily solved as 3. On the contrary, one shareholder does not provide enough information to solve the secret value s. Shamir's method is regarded as *perfect secret sharing* (PSS) scheme because knowing even ($k - 1$) linear equations doesn't expose any information about the secret.

B. Thien and Lin's Image Secret Sharing Scheme

Thien and Lin [7] proposed an image secret sharing method by cleverly using Shamir's secret sharing scheme to generate image shares (also known as *shadow images*) for an $m \times m$ pixels image with image intensity $I(i,j)$, where $1 \le i \le m$, $1 \le j \le m$, and $0 \le I(i,j) \le 255$. The essential idea is to use a polynomial function of the $(k\text{-}1)^{th}$ power to construct n image shares from the secret image as,

$$S_x(i, j) \equiv \left(I(i \times k + 1, j) + I(i \times k + 2, j)x + \cdots + I(i \times k + k, j)x^{k-1}\right) \bmod p$$

where $0 \le i \le \left\lfloor \frac{m}{k} \right\rfloor m$ and $1 \le j \le m$. This method reduces the size of image shares to become $1/k$ of the size of the secret image. Any k image shares are able to reconstruct almost every pixel value in the secret image.

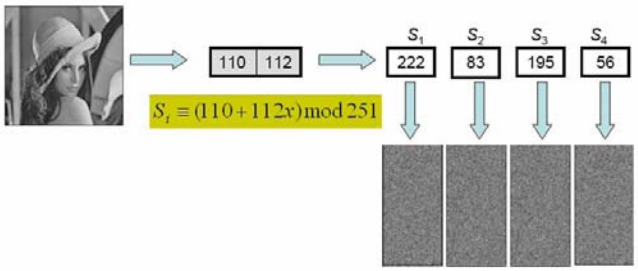

Fig 1. Thien and Lin's (2,4) Image Secret Sharing Method

An example of (2, 4) image secret share construction process is illustrated in Figure 1, where $k = 2$ and $n = 4$. Therefore, a first order polynomial function can be created as

$$S_x(1,1) \equiv (110 + 112x) \bmod 251,$$

where 110 and 112 are the first two pixel values in the Lena image. For our four participants, we can randomly pick four x values, and substitute them into the polynomial function by setting p value to be 251, which is the largest prime number less than 255 (maximum gray image value). Four shares are computed as (1, 222), (2, 83), (3, 195) and (4, 56). They become the first pixel in four image shares. The second pixel is computed in the same manner by constructing another first order polynomial function using next two pixels in the Lena image. This process continues until all pixels are encoded. Four image shares are the bottom right images shown in Figure 1, and the size of each image share is half (1/2) size of the original image.

Neither image share appears to reveal information about the secret image.

C. Distributed Image Steganography

The combination of image secret sharing with image steganography leads to *distributed image steganography* (DIS) [8]. This process is illustrated in Figure 2.

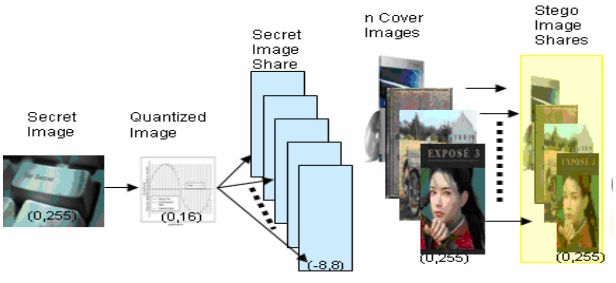

Fig 2. Distributed Image Steganography Process

Wu *et al* [8] referred DIS as a user friendly image secret sharing scheme because image shares are shrunken in innocent looking images, but a serious problem is that the method could be used in the wrong hands. This method currently allows a secret gray colored image of 256 levels (0 to 255) to be quantized into 16 levels (-8 to 8) using a *vector quantization* (VQ) method, and then distributed into several host images. After the quantization process, the secret image has smaller intensity level (16 levels) so that its shadow images, generated from Thien and Lin's image secret sharing method, can hardly alter intensity level in the host images (with 256 levels). The steganographic images are computed by combining the shadow images generated from the quantized image and the corresponding host images.

Figure 3 shows five 128x128 pixel original images (the first row of five images) and their steganographic images (the second row of five images) created from DIS. The steganographic images have a hidden picture invisible to unaided eyes. Any four steganographic images can be used to reconstruct the secret image.

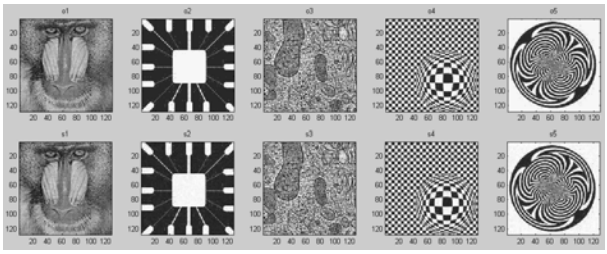

Fig. 3 Five Different Steganographic images

Figure 4 is the original 256x256 pixel secret image (left), and the reconstructed secret image (right) from the first four steganographic images shown in Figure 3. We can see that five steganographic images are almost indistinguishable from the original host images. Also, the size of steganographic images is one fourth of the size of the secret image (large secret information can be hidden in smaller host images) which allows more secret information to be hidden and transmitted in a covert channel. Recall that Thien and Lin's image secret sharing method allows the size of shadow image to become 1/*k* of the secret image (*k* is 4 in this example).

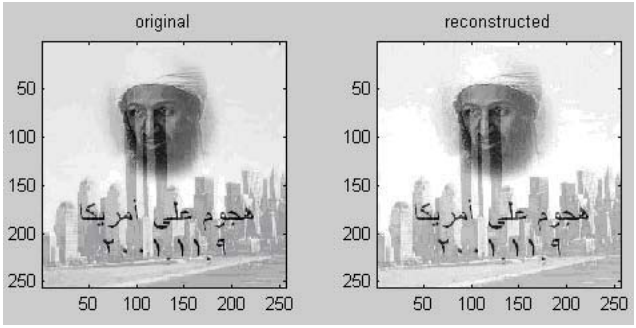

Fig 4. The original and reconstructed secret image

We also note that the reconstructed image is not precisely the same as the original image due to deficiencies in the image vector quantization process, but the method can be upgraded from lossy to become lossless. The method is more reliable and secure than conventional method of disguising the secret image in a single host image. At the same time, it also presents a tough challenge for image steganalysis due to its salient security and reliability features. Capturing one steganographic image is not enough to reconstruct the secret image since the secret image is distributed in a number of host images. In the above example, it is necessary that any four out of five of steganographic images be used to reveal the secret image.

3 Proposed Research

In this research, we study a blind steganalysis technique which no host image is required for detecting and extracting hidden information. To develop this counter-measure for DIS, we have following two assumptions:

i) one secret image hidden in a set of all suspected steganographic images, and
ii) threshold value *k* is known.

We describe our countermeasure process into three modules as shown in Figure 5 as

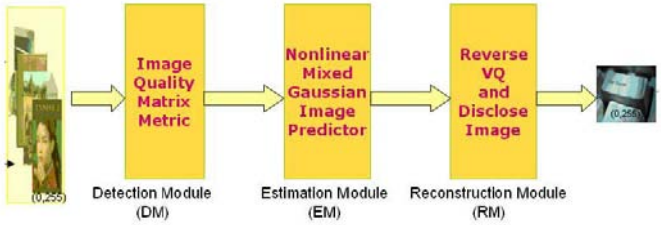

Fig. 5. Countermeasure process for DIS Images

- *Detection Module* (DM) is responsible for detecting possible steganographic images,
- *Estimation Module* (EM) is responsible for extracting image shares embedded in steganographic images, and
- *Reconstruction Module* (RM) is responsible for combining quantized image shares to reconstruct the secret image.

For these three modules, we focus our research efforts in DM and EM modules. In the EM module, a better estimation procedure relies heavily on how successfully we can build a good mathematical model for images. To further explore how we can use these three modules to discover the secret image hidden in DIS images, we detail background information on the DM and EM modules.

A. DM Image Quality Matrix

We know that the neighboring pixels in a natural image often have equal or close values. It is quite evident that the first two pixel values in Lena image (110 and 112) are the first two pixel values in Lena image shown in Figure 1, which are very close to each other. Since steganographic images are often lack of this interesting property, Sullivan *et al.* [6] suggest using an image quality matrix (IQM) to discover such discrepancies in steganographic images.

The basic idea is to construct a random process from an image; we convert two dimensional images into one dimensional data in one of the following two different ways as shown in Figure 6.

Fig. 6. Random Process Constructed from an Image

After this procedure, we determine IQM Q which is also a Markov transition matrix by counting what is the frequency of one pixel value changing to another pixel value. For example, we may observe in the random sequence that there are ten occurrences from pixel value 110 changed to 112. Consequently, the matrix Q has $Q(\lfloor 110/2 \rfloor, \lfloor 112/2 \rfloor) = Q(55,56) = 10$, and it is a 256×256 matrix with one pixel jump in each direction for neighboring elements. We can also construct matrix Q as a 128×128 matrix with a two pixel jump in each direction for neighboring elements. Matrix Q can also be represented in colormap scheme with higher frequency counts showing as white and zero count as black. When we determine IQM from both Lena's image and Lena's image with DIS image share embedding, we can see high frequency count is in the diagonal axis in IQM Q for Lena's image as shown in Figure 7.

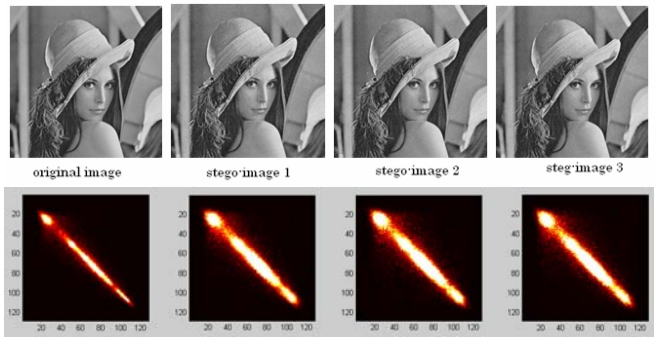

Fig. 7. Image Quality Matrices

In contrast, we see in Figure 7, that steganographic images have a wider band for the higher frequency count. Generally speaking, DIS image shares are white and uncorrelated, their image quality matrices are spread evenly, and there is no greater probability for values near the main diagonal. When image shares are superimposed on host image, hiding secrets in natural images weakens the dependencies between pixels in the host images, which cause spreading from the main diagonal of the image quality matrices in steganographic images. Therefore, IQM is an effective method to determine which images are steganographic images.

B. EM Mixed Gaussian Model

Zhang and Ma [9] developed a nonlinear predictor for Gaussian mixture image model. In this model, the prediction of each pixel is a linear combination of neighboring pixels. It is nonlinear because the combination coefficients are functions of the neighboring pixels, not constants. Nonetheless, it is important to derive a mixture of Gaussian models for steganographic images which we can then use to estimate pixel values for host images. In this example, we use the last four steganographic images (shown in Figure 3) to compute the mixed Gaussian models from histograms of their pixel

values. Figure 8 shows approximated mixed Gaussian model curves in solid line.

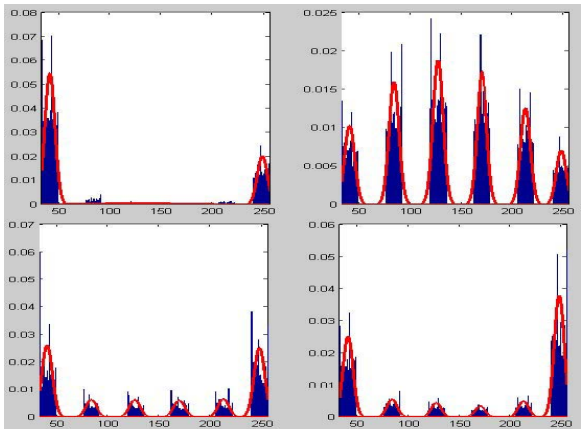

Fig. 8. Histograms of Steganographic Images

As a result, we can determine predicted values for all pixels in host images from steganographic images. Since image shares are superimposed on host images, we regard the dispersion difference with predicted values and true pixel values in the host image as result of image share values and some observation noises. Consequently, we can approximate a random sequence model *s(n)* as an autoregressive (AR) system similar as

$$s(n) = s(n-1) + u(n), \qquad (3)$$

where u(n) is process noise with zero mean, and it is uniformly distributed [-8, 8]. As image shares are embedded into the host images to produce steganographic images, we can get another random process in similar manner as for any one steganographic image as

$$x(n) = h(n) + s(n) + w(n), \qquad (4)$$

where *h(n)* is determined from mixture Gaussian model developed by Zhang and Ma [9], *w(n)* is a white Gaussian noise with zero mean and standard derivation of one. Clearly, equations (3) and (4) are none other than the processing and measurement equations in a dynamic model for sequential estimation. Our proposed countermeasure technique is based upon Bayesian sequential estimation problem to determine

$$\theta = s(n), \text{ and}$$

to minimize mean square error in Bayesian criterion as

$$Bmse(\hat{\theta}) = E(|s(n) - \hat{s}(n)|^2).$$

Accordingly, some nonlinear, non-Gaussian, and non-stationary based adaptive estimation methods such as Un-scented Kalman filter or particle filters can be used to extract the image shares from the steganographic images.

C. RM Reversing DIS

Here, we assume that we can detect *k* steganographic images using DM module and extract *k* image shares using EM module. The reversing process is to i) reconstruct quantization image using Thien and Lin's method, ii) decode the secret image from quantization image. In this example, we use the last four steganographic images (shown in Figure 3) to reconstruct the secret image (on the right) as shown in Figure 9.

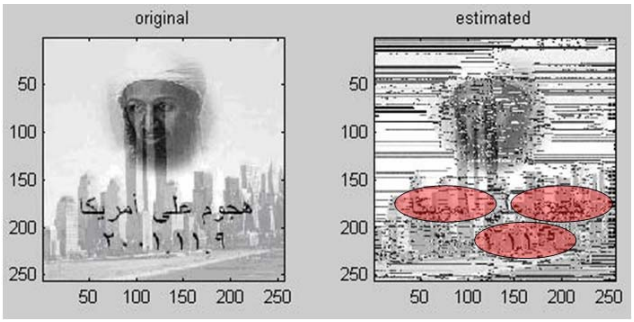

Fig. 9. Original and Estimated Images

Note, it is interesting that we can almost see numbers 9 and 11 in the estimated secret image in the lower oval. Undoubtedly, such information can be extremely useful in intelligence gathering for the law enforcement agencies and military analysts.

4 Conclusion and Future Work

In this paper, we present an estimation approach to detect and disclose what a secret image or message is hidden among several steganographic images using DIS. We demonstrate an estimation approach which can be used successfully to discover the secret image. From this preliminary attempt to disclose what secret image is hidden, we still need more validation procedures and performance metrics to show how effective this method is to countermeasure DIS. Also, we made the following two assumptions i) threshold value (*k*) is known and ii) the same secret image is hidden in all suspected steganographic images. Although these two conditions are difficult to determine, but we can see its potential for disclosing all possible hidden secret images if we can utilize some high speed parallel processing systems in order to discover secrets in suspected steganographic images. With great confidence in this research, we think it can provide an excellent intelligence gathering tool for law enforcements and military analysts with an immense amount of information extraction capability to prevent criminals from communicating by using DIS.

References

[1] R. Anderson, “Stretching the limits of steganography,” presented at the IWIH International Workshop on Information Hiding, vol. 1174. Springer Lecture Notes in Computer Science, 1996, pp. 39–48.

[2] N. F. Johnson, Z. Duric, and S. Jajodia, Information hiding: Steganography and watermarking attacks and countermeasures. Kluwer Academic Publisher, 2000.

[3] N. Johnson and S. Katzenbeisser, A survey of steganographic techniques in information hiding. Norwood. MA: Artech House, 2000.

[4] D. Kahn, The codebreakers the story of secret writing. New York, New York, USA: Scribner, 1996.

[5] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

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

[7] C.C. Thien and J.C. Lin, “Secret image sharing,” Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.

[8] Y.S. Wu, C.C. Thien, and J.C. Lin, “Sharing and hiding secret images with size constraint,” Pattern Recognition, vol. 37, no. 7, pp. 1277–1385, 2004.

[9] J. Zhang and D. Ma, “Nonlinear prediction for Gaussian mixture image models,” IEEE Trans. Image Processing, vol. 13, no. 6, pp. 836–847, 2004.