Hiding Binary Images behind Noise with Authentication Capability: A New Approach to Covert Communication*

Chih-Hsuan Tzeng
Department of Computer and Information Science,
National Chiao Tung University
Hsinchu, Taiwan 300, Republic of China
Tel: +886-3-5728368
chtzeng@cis.nctu.edu.tw

Wen-Hsiang Tsai♉
Department of Computer and Information Science,
National Chiao Tung University
Hsinchu, Taiwan 300, Republic of China
Tel: +886-3-5728368
whtsai@cis.nctu.edu.tw

Abstract

A new approach to hiding secret binary images behind noise images for covert communication with a capability of secret authentication is proposed. A secret image to be transmitted is transformed into a random noise image at a sender site with a given key, with the aim of both covering the secret and cheating illicit interceptors. Authentication bits are also embedded imperceptibly in the noise image. At the receiver site, the secret image is recovered from the noise image with the same key and verified by checking the existence of the authentication bits. Experimental results show the feasibility of the approach for real applications.

Keywords: covert communication, information hiding, binary noise image, image authentication.

1. Introduction

Covert communication means secret information exchanges between two sites with the purpose of preventing the secret from illicit interceptions. Such communication mechanisms are useful for many business or military applications. Most related studies dealt with the problem from the viewpoint of signal processing or communication theory [1-2]. With the advance of digital multimedia technologies and Internet communication, it is frequently found necessary to transmit secret images between two sites. An intuitive way for this is to use the cryptographic approach in which secret data are encrypted at a sender site and decrypted at a receiver site [3]. However, it is sometimes inconvenient to apply the traditional encryption-decryption approach to images because of the usually large volumes of image data. Thus it is interesting to investigate more specific mechanisms for covert communication of images. In this paper, a new scheme for this purpose is proposed, which is based on a new concept, namely, secret hiding in noise.

The image type we deal with is binary. There were only a few studies [4-7] in the past about hiding information behind binary images, which is usually difficult because of the limited data embedding capacity as well as the low data content complexity of binary images. Wu, et al. [4] embedded bits in image blocks selected by pattern matching. The method can be used for data hiding behind meaningful cover images or for image authentication. Tseng, et al. [5] changed pixels' values in image blocks and mapped block contents into the data to be hidden. The employed cover images again are meaningful. In [6, 7], spacings between words or lines in textural document images were changed to embed watermark signals for copyright protection. In this study, we investigate hiding secret binary images behind noise images from the viewpoint

* This work is supported partially by the MOE Program for Promoting Academic Excellency of Universities under Grant No. 89-1-FA04-1-4.

♉ To whom all correspondence should be sent.

0-7803-7882-2/03/$17.00©2003 IEEE

Authorized licensed use limited to: National Chiao Tung University. Downloaded on March 14, 2009 at 01:51 from IEEE Xplore. Restrictions apply.

of covert communication with an additional capability of checking the authenticity of the recovered secret image.

More specifically, in the proposed method a secret image is hidden at a sender site behind an artificially created image that is full of random noise. This noise image has the effects of both covering the secret and cheating an illicit interceptor or receiver. It will be called a *cover noise image* in the sequel in this paper. The creation of the cover noise image is based on a transformation of the given secret image data into noise through the use of the exclusive-OR bit operation as well as a pre-selected key. Furthermore, some randomly generated bits, called *authentication bits* in this study, are inserted in the cover noise image for the purpose of secret authentication. Such bits also appear to be noise due to their randomness nature. The secret image can be recovered from the cover noise image at a receiver site with their fidelity being authenticated to achieve the goal of secure covert communication.

In the remainder of this paper, we describe the proposed method by giving an algorithm for hiding a secret binary image behind a cover noise image in Section II, and a corresponding algorithm for recovering the secret image from the cover noise image and authenticating the recovered image in Section III. Some experimental results are given in Section IV, followed by some conclusions and discussions on the merits of the proposed approach.

2. Hiding Secret Binary Images behind Cover Noise Images

The proposed algorithm for hiding a given secret binary image processes the image block by block by creating a noise image block from each given secret image block. Each noise block is created to be a little bit larger than the original secret block, allowing extra pixels for embedding authentication bits. The details are as follows. See Figure 1 for illustrations of the intermediate results of the algorithm.

Algorithm 1: Hiding a secret binary image behind a cover noise image that includes authentication bits.

0	1	1
1	1	0
1	0	0

(a) A secret image block B_i.

1	0	1	1
1	0	0	1
0	0	1	0
0	1	0	0

(b) Created noise block B_i'.

①	×	①	①
×	⓪	×	×
×	⓪	×	⓪
×	①	⓪	⓪

(c) Selected pixel sets A_i (×'s) and C_i (circled 1's & 0's) for authentication and secret covering.

①	1	⓪	⓪
1	①	0	1
1	①	1	⓪
0	⓪	⓪	⓪

(d) Final noise block B_i' covering the secret and including authentication bits.

Figure 1. Illustrations of intermediate results of Algorithm 1.

Authorized licensed use limited to: National Chiao Tung University. Downloaded on March 14, 2009 at 01:51 from IEEE Xplore. Restrictions apply.

Input: A given secret binary image I of $M\times M$ blocks, with each block of size $n\times n$, and a selected secret key K.

Output: A cover noise image I' of $M\times M$ blocks, with each block of size $m\times m$ and including authentication bits, where $= m\times m - n\times n > 0$.

Steps.

1. For each image block B_i of I where $i = 1, 2, \ldots, M\times M$, perform the following steps until all blocks of I are processed.
2. **(Generating a key for use in each block)** Use a random number generator g_1, with the input key K as the seed, to create a key K_i for B_i.
3. **(Creating a random noise block)** Use another random number generator g_2, with K_i as the seed, to generate sequentially $m\times m$ random binary values (0's or 1's) to create a noise image block B_i' of I'.
4. **(Selecting pixels for secret covering and authentication)** Use a third random generator g_3, with K_i as the seed again, to select randomly pixels in B_i' as a set A_i for embedding authentication bits later. And collect the remaining $n\times n$ pixels as another set C_i for covering the secret data of B_i later.
5. **(Covering the secret by noise)** In a manner of raster-scanning the secret image block B_i and the noise pixel set C_i, apply the exclusive-OR operation to the binary values of every pair of corresponding pixels, one pixel p_1 from B_i and the other p_2 from C_i, and fill the resulting value into p_2. Collect all the resulting bits in C_i in a raster scanning sequence to form an $n\times n$-bit binary number X_i.
6. **(Creating the authentication bits)** Use a fourth random number generator g_4, with X_i as the seed, to generate an -bit binary number Y_i, and fill the bits of Y_i in a raster scanning sequence into the pixels of A_i as the authentication bits.

3. Secret Image Recovering and Authentication

The process of secret image recovering and authentication, described as Algorithm 2 below, is basically a reverse process of the secret hiding process described by Algorithm 1. Also, if any image block is checked to be tampered, the entire image is claimed to be unauthentic and the algorithm is stopped.

Algorithm 2: Recovering a secret image from a cover noise image and checking its authenticity.

Input: A cover noise image I' of $M\times M$ blocks with each block of size $m\times m$, and the selected secret key K used in secret hiding.

Output: A recovered secret image I with each block of size $n\times n$, and the authenticity of I, where $m\times m - n\times n =$.

Steps:

1. For each block B_i' of I' where $i = 1, 2, \ldots, M\times M$, perform the following steps until all blocks of I' are processed.
2. **(Generating a key for use in each block)** Use the random number generator g_1 employed in Algorithm 1, with the input key K as the seed, to create a key K_i for B_i'.
3. **(Selecting pixels for extracting authentication bits and recovering the secret)** Use the third random generator g_3 employed in Algorithm 1, with K_i as the seed, to select pixels in B_i' as a set A_i for extracting authentication bits later. And collect the remaining $n\times n$ pixels as another set C_i for recovering the secret data later.
4. **(Extracting the authentication bits)** Collect the values of the pixels of C_i in a raster scanning sequence to form an $n\times n$-bit binary number X_i, and use the fourth random number generator g_4 employed in Algorithm 1, with X_i as the seed, to generate an -bit binary number

Authorized licensed use limited to: National Chiao Tung University. Downloaded on March 14, 2009 at 01:51 from IEEE Xplore. Restrictions apply.

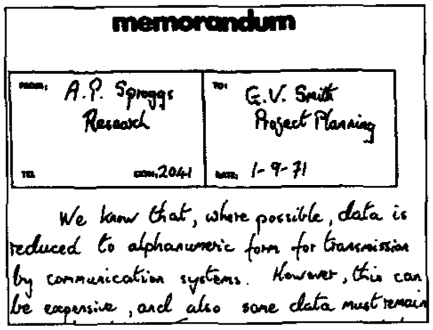
Y_i.

5. **(Checking the authenticity of the secret image block)** Collect the values of the pixels of A_i in a raster scanning sequence to form an -bit binary number Y_i', and compare Y_i' with Y_i. If they are not identical, report that the corresponding secret image block B_i is tampered and stop the algorithm; otherwise, perform the following steps to recover B_i.
6. **(Creating a random noise block)** Use the random number generator g_1 employed in Algorithm 1, with K_i as the seed, to yield a sequence of random binary values (0's or 1's) to create an $m\times m$ noise image block R_i.
7. **(Recovering the secret image block)** In a manner of raster-scanning the noise blocks R_i and C_i, apply the exclusive-OR operation to the values of every pair of corresponding pixels, one pixel p_1 from R_i and the other p_2 from C_i, and fill the resulting binary value into p_2. Collect all the resulting bits in C_i to form an $n\times n$ block B_i in the recovered secret image I.

It is noted here that the exclusive-OR operations conducted in Step 7 above indeed will recover the original secret bit because of the following property of the operation (denoted as $\oplus$): if $b_1\oplus b_2 = b_3$ (computed in Step 5 in Algorithm 1), then $b_3\oplus b_2 = (b_1\oplus b_2)\oplus b_2 = b_1\oplus(b_2\oplus b_2) = b_1\oplus 0 = b_1$ (computed in Step 7 in Algorithm 2), where b_1, b_2, and b_3 are binary values, and b_1 is the secret bit.

4. Experimental Results

Some binary images have been tested in our experiments. An example of the results is shown in Figure 2. Figure 2(a) shows a secret binary image of size 1024×768 to be transmitted in a covert communication session, and Figure 2(b) shows the cover noise image of size 1152×864 resulting from Algorithm 1 with a key $K = 1234$, which can be seen to be random enough to cover the original secret image effectively. The block sizes adopted in the algorithms are $n\times n = 8\times 8 = 64$ and $m\times m = 9\times 9 = 81$, so that the number of extra authentication bits in each block is $= 81 - 64 = 17$. This number may be reduced if the requirement for each block in the cover noise image to be square is relaxed. In this case, we may take a block in the noise image, say, to be $n\times m$, so that $= n = 8$ here. The recovered secret image after applying Algorithm 2 to the image of Figure 2(b) is exactly that shown in



memorandum

A.P. Spriggs
Research

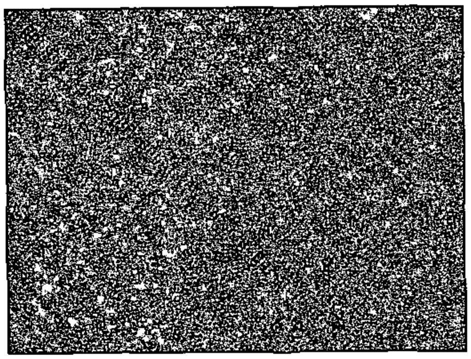
G.V. Smith
Project Planning

2041

1-9-71

We know that, where possible, data is reduced to alphanumeric form for transmission by communication systems. However, this can be expensive, and also some data must remain

(a) A secret binary image.



(b) Cover noise image resulting from Algorithm 1.

Figure 2. An example of experimental results.

Authorized licensed use limited to: National Chiao Tung University. Downloaded on March 14, 2009 at 01:51 from IEEE Xplore. Restrictions apply.

Figure 2(a). When an erroneous key is input to Algorithm 2, the algorithm will stop at Step 5 with no output.

5. Conclusions

A new approach to covert communication has been proposed, which may be employed to hide secret binary images behind noise ones with an additional capability of secret authentication. There is no need to seek a meaningful cover image for hiding the secret; instead, the cover image, which is full of random noise, is created directly from the secret image itself. This provides an alternative way for steganography. Since noise images tend to be ignored when they are intercepted in a communication process, hopefully more steganographic or cheating effect can be achieved in covert communication applications. Another merit of the proposed approach is that a larger data-embedding capacity can be provided by the cover noise image, because *each* pixel of a cover noise image can be utilized to hide a secret data bit imperceptibly. This merit is not found in other approaches dealing with binary data. Furthermore, differing from most data hiding techniques by which secret binary images cannot be recovered perfectly after they are embedded, the proposed method ensures full recoverability of hidden secret data from cover noise images.

References

[1] R. Orr, et al., "Covert communications employing wavelet technology," *The Twenty-Seventh Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, California, November 1993.

[2] J. T. Wittbold, "Controlled signaling systems and covert channels," *Proceedings of the 1989 Computer Security Foundations Workshop II*, Franconia, N. H., June, 1989, pp. 87-104.

[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley & Sons, New York, 1995.

[4] M. Wu, E. Tang, and B. Liu, "Data hiding in digital binary images," presented at the *IEEE International Conference on Multimedia and Expositions*, New York, 2000.

[5] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," *IEEE Transactions on Communications*, vol. 50, no. 8, August 2002, pp. 1227-1231.

[6] S. H. Low, N. F. Maxemchuk, and A. M. Lapone, "Document identification for copyright protection using centroid detection," *IEEE Transactions on Communications*, vol. 46, no. 3, March 1998, pp. 372-383.

[7] D. Huang and H. Yan, "Interword distance changes represented by sine waves for watermarking text images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 12, pp. 1237-1245, December 2001.

Authorized licensed use limited to: National Chiao Tung University. Downloaded on March 14, 2009 at 01:51 from IEEE Xplore. Restrictions apply.