行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※

※ 容忍失真壓縮之資訊隱藏技術之研究 ※

※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　□整合型計畫

計畫編號：NSC 89－2218－E－032－027－

執行期間：八十九年八月一日至九十年七月卅一日

計畫主持人：黃仁俊

本成果報告包括以下應繳交之附件：

- □赴國外出差或研習心得報告一份
- □赴大陸地區出差或研習心得報告一份
- □出席國際學術會議心得報告及發表之論文各一份
- □國際合作研究計畫國外研究報告書一份

執行單位：淡江大學資訊工程學系

中　華　民　國　九十年　八月　二十日

行政院國家科學委員會專題研究計畫成果報告

容忍失真壓縮之資訊隱藏技術之研究

The Study of Lossy Compression Tolerant Steganography

計畫編號：NSC 89－2218－E－032－027－
執行期限：八十九年八月一日至九十年七月卅一日

主持人：黃仁俊 淡江大學資訊工程學系

一、中文摘要

本計畫提出一可以容忍失真壓縮的資料隱藏技術。資料隱藏技術提供了傳遞機密資料的安全通道，使攻擊者很難找到攻擊破壞的目標，在今天逐步走向電腦網路化的時代裡，這是一項非常重要的技術。早期許多學者利用各種不同的技術來發展資料隱藏技術，但是這些結果大部份都無法承受失真壓縮技術的破壞。在本篇結案報告中，我們利用相鄰像素間灰階值對比關係，提出一新的資料隱藏技術，經我們技術隱藏資料後所產生的新影像不僅無法從人類的視覺上發現其與未藏資料前影像之差異，同時其經失真性壓縮技術(JPEG)壓縮後，從再還原的影像中仍能正確無誤的還原出被隱藏的資料，這些特性我們都以實驗予以証實，而這是目前許多相關技術做不到的。

關鍵詞：電腦密碼技術，資訊隱藏技術，資訊安全，隱密技術

Abstract

This project proposes a lossy compression tolerant steganography. Steganography hides the confidential data secretly. The unauthorized people are difficult to detect hidden data. It provides a secure channel to transmit confidential information. Nowadays, it is a very important technique when we are progressively going to computer network age. There are many researchers purposed steganographies, but most of their techniques cannot tolerate the destruction of lossy compression. In this project, we propose a novel steganography based on the contrastive relation of the grayscale value of neighboring pixels. It is difficult for the human visual system to detect the difference between original image and one that embedded information based on our steganography. Besides, the embedded data can be extracted correctly from the decompressed stego-image. By our technique, the steog-image can be compressed by the lossy JPEG compression process before transmitting or storing it. This feature will speed up the transmission of the stego-image..

Keywords: Cryptography, Information hiding, Information security, Steganography

二、緣由與目的

With the fast development of Internet technologies, the information and digital age is coming. It is the trend toward each behavior and people must use computer and Internet tools to reduce manpower and raise work efficiency. Moreover, for national defense force, we will be faced with the digital war. The fact that cannot be denied is that all of the information and management, arms system, rear supply system and modernized arms are exchanged with digital mold and transported by the network system. "How to transmit the secret information over the network?" is an important problem. We must prevent peeping, copying and altering the data from conspirators. Of course, using cryptography to encrypt and transmit these data is a good method. However, the cipher texts generated the cryptosystem are meaningless random codes. Transmitting meaningless random codes directly is to tell

other people that there are very important messages in it and remind conspirators to cut, hack or break these confused codes. Therefore, the pure encryption technology cannot solve the problem of transmitting secret data completely. Even if transmitting encrypted secret data, we hope the unauthorized people will think it is a meaningful and its means are independent of the confidential data. Only authorized receivers can extract real secret messages from this meaningful data. This technology is so called steganography.

Steganography hides the transmitted data in a meaningful but not related text or image. Those unauthorized receivers are unable to detect the hidden data while transmitting. Thus, we can avoid attackers painstakingly to break and to intercept. In steganography, we randomly select one image (named cover image [ ]) and embed data into it. This cover image which embedded with secrete data is named stego-image [ ]. The human visual system looks this stego-image similar to cover images. It is difficult to detect the difference between the stego-image and the cover-image by the human visual system. For a conspirator, although the stego-image has important data, he cannot fine it. Therefore, attackers cannot differentiate those that has embedded with secrete data from many of others in the network easily. But for an authorized receiver, he can extract concealed data quickly. In [ ][ ][ ], the authors define the steganography must have the following features:

- Imperceptibly: it is difficult to fine the difference when data embedded in the stego-image.
- Readily Extracted: an authorized receiver can extract concealed data quickly.
- High Capacity: embedding the data into the image as many as possible.
- Resistance Removal: data which be embedded in the stego-image cannot be moved.

In steganography, the most common method is Vector quatization[ ][ ]. It uses codebook which sender and receiver have to process data embedded. First of all, sender cuts the image in which he wants to embed data and the block size is as the same as the size of codebook block. Next, searching the similar block and obtain its index value. After that, encrypt the index value and embed it in the cover image, then transmit it. When receiver receives the stego-image, it will obtain the index value and decryption. Finally, using the index value and codebook to restore data. This method loses data and stego-image cannot resistant lossy compression. It is not suit to embed text.

The other steganographies use image pixels to embed data. In [ ], the authors provide a Fixed Range Equalization method. They divide the gray-level value into sixteen areas: [0~15], [16~31], ..., [240~255]. Depending on index value, their method determines a suitable area of the embedded data and selects one value to replace the embedded data. The selected value cannot repeat. For instance, data value is 25, select one point in area 16 to 31 and exchange its value. The other common steganographies are LSB[ ][ ]. It embeds the data in lower bit that can reduce the influence on image after embedded data. This method is the simplest and most directly one. Moreover, it has biggest embedded capacity. However, the previous methods cannot tolerate lossy compression, for example JPEG. In this project, we propose a novel steganography. The stego-image based on our method can satisfy the previous features. Besides, although stego-image is processed by lossy compression, the embedded data still can be extract correctly from the decompressed stego-image.

三、結果與討論

This section will introduce our steganography based on the contrastive relation of gray-level values of the neighbor pixels. In steganography, there are two important data, one is the embedded data and the other is cover image. In accordance with each embed data bit, we select one

correspond pixel in the cover image. We use the contrastive relation of gray-level values of the selected pixel and its top, bottom, left and right neighbor pixels to keep this embedded data. Some of the contrastive relations of gray-level values do not destroy after lossy compression and decompression process. We can extract them correctly based on the contrastive relations. Without loss of the generality, this project assumes the cover image C is an m×n gray-level image and the gray-level is 256. The data D, which is embedded in C, we assume it is a g bits stream. We use below expressions to express image C, data D and each pixel separately.

$C=\{c_{ij} \mid 0 \leqq i < m, 0 \leqq j < n, c_{ij} \in [0,255]$

$D=\{d_i \mid 0 \leqq i < g, d_i \in [0,1]\}$,

We introduce our method in the following two phases:

[Embedded data Phase]

Step-E1:Randomly select one number S.

Step-E2:Generate g different numbers named $A = \{a_1, a_2, ..., a_g\}$ based on the seed S. Each value a_i ranges between 1 and $m \times n$. For any two different integer numbers a_i and a_j in A, their top, bottom, left and right neighbor pixels should be different.

Step-E3:Decide a threshold value t. According to the value of each d_i bit, we alter some pixels in C as the following steps. C' is the stego-image embedded the data D in C.

Step-E3-1:Compute $k = a_i$ DIV n and $l = a_i$ mod n. The "X DIV Y" means the quotient of Y dividing X, and "X mod Y" means remainder of Y dividing X.

Step-E3-2:Compute the average value v of the pixel c_{kl} in cover image C and its top, bottom, left and right neighbor pixels' gray-level as $(c_{k-1,l} + c_{k,l-1} + c_{kl} + c_{k,l+1} + c_{k+1,l}) / 5$.

Step-E3-3:If $d_i = 0$; when $v - c_{kl} \geqq t$, keep c_{kl} value, otherwise simultaneously alter c_{kl} value and its top, bottom, left and right neighbor pixels value by the same difference until $v - c_{kl} \geqq t$.

If $d_i = 1$; when $v - c_{kl} \leqq -t$,keep c_{kl} value, otherwise simultaneously alter c_{kl} value and its top, bottom, left and right neighbor pixels value by the same difference until $v - c_{kl} \leqq -t$.

Step-E4:Stego-image C' is the image generated by Step-E3.

Step-E5:Send the seed S by the secret channel.

〔Extract Embedded data Phase〕

When receiver receives image $C' = \{c'_{ij} \mid 0 \leqq i < m, 0 \leqq j < n, c'_{ij} \in [0,255]\}$, he extracts the embedded data by the following steps.

Step-D1:Generate the set A based on the seed S as Step-E3.

Step-D2:Extract each bit d_i based on its correspondence value a_i as the following steps.

Step-D2-1:Compute $k = a_i$ DIV n and $l = a_i$ mod n.

Step-D2-2:Compute the average gray-level value v of the image pixel c_{kl} and its top, bottom, left and right neighbor pixels as $(c'_{k-1,l} + c'_{k,l-1} + c'_{kl} + c'_{k,l+1} + c'_{k+1,l}) / 5$.

Step-D2-3:If $v > c'_{kl}$ then $d'_i = 0$, otherwise $d'_i = 1$.

Step-D3:Integrate all the bits d'_i extracted by Step-D2, and make up the embedded data D'.

四、計畫成果自評

In this project, we propose a steganography based on the contrastive relation of the gray-level values of the neighbor pixels. Some of the contrastive relation among the values of the neighbor pixels does not alter after the JPEG lossy compression process. The proposed steganography does not only contain the features as the other steganography, but also can tolerated JPEG lossy compression. When receiver receives the stego-image, he can decompress stego-image and extract the embedded data correctly from it. The transmissions of lossy compressed stego-images are more efficient than the original stego-image. The proposed steganography is more practical than the other steganography. Thus, this result achieves the subject of this project. It is success. This result is published in the international conference: *The International Conference on The Human Society and the Internet.* [10]

五、參考文獻

[1] The New Testament Revised Standard Version And Chinese Union Version: The Gospel According to Matthew Chapter3, pp. 5-7 (1985)..

[2] E. Adelson (1990), "Digital Signal Encoding and Decoding Apparatus," *U.S. Patent, No.4939515.*

[3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu (1996), "Techniques for Data Hiding," *IBM Systems Journal*, Vol. 35, Nos 3 and 4, pp.313-336.

[4] T. S. Chen, C. C. Chang, and M. S. Hwang (Oct.1998), "Virtual Image Cryptosystem Based upon Vector Quantization," *IEEE Transactions onf Image Processing*, Vol. 7, No. 10, pp.1485-1488.

[5] T. S. Chen, and Y. H. Hsu (1997), "Image Camouflage and Encryption Method Using Vector Quantization," *The Second Conference of Information Management and Its Application in Law Enforcement*, Taipei, R.O.C., pp.97-106.

[6] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon (September 1996), "Secure Spread Spectrum Watermarking for Images, Audio and Video," *Proceedings of the IEEE International Conference on Image Processing , Lausanne, Switzerland*, ,pp.243-246.

[7] N. F. Johnson and S. Jajodia (Feb. 1998), "Exploring Steganography: Seeing the Unseen," *IEEE Computer Magazine*, Vol. 31, NO. 2, pp.26-34.

[8] M. S. Liaw and L. H. Chen (Nov. 1997), "An Effective Data Hiding Method," *Proceeding of the Sixth National Conference on Science and Technology of National Defense*, Vol. 2, Taoyuan, Taiwan, pp.534-540.

[9] Lisa M. Marvel, Charles T. Retter and Charles G. Boncelet (1998), "Hiding Information in Images," *in Proceedings of ICIP.*

[10] R. J. Hwang, T. K. Shih, C. H. Kao, and T. M. Chang (2001), "Lossy Compression Tolerant Steganography," *The Human Society and the Internet,* LNCS 2105, Springer-Verlag, 2001,pp.427-435.