一種無警性的文件秘密傳送策略研究

王旭正、呂政國
中央警察大學資訊管理學系

摘要

在現今網際網路普及的時代，爲了建立一個安全的網路傳輸環境，使秘密資訊在網路上能夠被安全的傳輸。先前許多的學者已提出許多的資料保護法，大致上可區分爲兩類，一爲將資料先進行加密傳輸，再進行解密輸出的「資料加密法」，另一類爲將秘密資訊隱藏在備藏資料裡的「資訊隱藏法」。本文試著提出一種新的作法，藉著一張圖片，配合內含之中英文的說明文字，去建立代碼數字索引表格；再將欲隱藏的秘密資訊，轉成代碼的形式。並根據代碼數字索引表格，可將秘密資訊的代碼轉成數字索引檔，最後將其數字索引檔藏入我們傳輸的圖片中。如此一來，在所有的傳輸過程中，傳送的資料都是可見的明文及圖片，不易被非法者懷疑，又可隱藏大量的秘密資訊。

關鍵字：資訊安全、資料加密法、資訊隱藏法

A Scheme of Non-sensible Document in Transit with Secret Hiding

Shiuh-Jeng Wang, Cheng-Kuo Lu
Department of Information Management, Central Police University

ABSTRACT

In now knowledge explosive era, the message transmission is so rapid and convenient via Internet propagation. For the grade of confidential document, however, we need to pay much attention to the message transit in network systems so as to safeguard the secrecy and integrity. Basically, there are two catalogs to encrypt the secret message, one the data encryption cipher, the other one is the information hiding cipher. In this paper, the later one with the information hiding manner is used to embed the secret message into a host image. According to the content of this chosen host image, the bilingual words associated with this image are used to build the index tables which are the relations between the bilingual words and the confidential document. Afterwards, all index tables are embedded into the host image and only this embedded image is required to transit in the network systems. In such a way, all messages transmitted in the network are kind of visible forms, not random-number forms. Comparing to the previous literatures, a general image is transmitted only instead of the cipher documents suspicious to network interceptors. Apparently, the intentional attacks by those who focus on the random-form messages are evitable. Therefore, a novel and efficient scheme aiming at hiding confidential document is achieved in this paper.

Keywords: Information Hiding, Security, Cryptography, Steganography

壹、簡介

隨著網際網路的日益普及，資訊的流通也愈來愈便利，人們也開始習慣利用網路來傳遞重要的文件及資料。但網路環境雖然快速便利，卻仍然存在著許多令網路使用者頭疼的問題。因爲網路爲一開放性的空間，任何一個人，只要具備上網工具，就能輕鬆的在網際網路世界暢通無阻，而我們放在網路上的資料，便有可能遭到非法者的不當截取。過去，在資訊安全的這個領域當中，大部分的學者、專家，已提出並且發展了許多困難又複雜的資料保護法，大致上可分爲兩類，一爲將資料進行加解密的「資料加密法」，另一類爲將秘密資料隱藏在另一資料中的「資訊隱藏法」。這兩種作法都有其缺點，前者爲資料一旦經過加密，易形成一堆雜亂無章的密文，容易遭到非法者的懷疑，當駭客截取到這些表面毫無意義的文字時，便知曉其爲加密過的資料，使其想一探其中究竟，進而想試圖破解取出內含的秘密資訊。而後者將秘密資訊隱藏在另一資料中的作法，往往有無法隱藏大量秘密資訊的問題。

根據文獻 [1]，資料加密法 (Cryptography) 的目標爲傳送加密過的秘密訊息給特定的使用者，爲一種公開的安全訊息模式，我們可以明顯的看出，傳送的結果爲一份可見的加密秘密訊息；而在另外一方面，資訊隱藏法 (Steganography)[6] 爲一種隱蔽的安全隱藏訊息模式，其目的爲將資訊隱藏入存在的資料中，以不會遭受懷疑的明文型式傳送給接收者。

本文試著引用 1998 年，由 Lin et al.[9] 所提出的作法，結合文獻 [12, 13] 的作法，提出一種新的做法，其中的文獻 [13]，是以十六進制的數字型式爲資料的對應關係以達到秘密隱藏的效果。我們利用一篇簡單的雙語說明文字，加上其圖檔，再傳送給接收者，改進先前研究者所存在的缺點：加密過所形成之亂碼，將遭受懷疑，而有被攻擊的高風險性。在我們的方法中，唯一的限制爲，所使用的雙語說明文字轉成的代碼，必須至少包含所有我們欲傳送的中英文秘密訊息所轉成的代碼，然這方面的限制，很容易得到解決，因爲在一般的訊息傳送裡，中英文字的重覆使用性很高，如此一來，便能夠同時隱藏大量的中英文資訊。而且不同於先前的研究，在文獻 [9,12] 中，其爲將文件數字索引檔案加密直接放置於網路上傳輸，其密文的外表易遭到非法者的質疑，增加被攻擊、破壞的風險；然我們取而代之的是將其隱藏入圖片中，這樣一來，所有網路傳輸的資料都是可見的明文，不易造成非法者的懷疑，而且透過一張圖片及其說明文字，就能隱藏大量的中英文字。另外在文獻 [9,12] 的作法中，需傳輸數張的掩護文件，如此的方式，明顯地增加網路資料傳輸的負擔。而反觀在我們所提的方法中，僅一份掩護的文件即可達到保護的效果，而在整體所需空間的傳輸上，經評估並未增加過多輔助性資料量傳輸的疑慮。

我們所提出的方法，其基本的作法乃透過一篇內含雙語的翻譯文件，將實際的中英文秘密訊息轉成代碼型式，再隱藏入圖片中。而這個作法事實上可爲資訊隱藏方法的一種應用，由文獻 [5] 可說明之；而且我們的數字索引檔案，需先經過加密處理，減少被破解的風險，因此可說是集合資訊隱藏與資料加密之更安全與加強性之方法。

在我們的文件秘密傳送系統中，由於秘密訊息的數字索引檔案是非常重要的，所以我們得有加密的機制處理，而我們使用的方法爲 *IDEA*[3, 8]，用以加密數字索引檔案。*IDEA* 是一種區塊密碼 (Block cipher)，它使用了一把 128 位元的加密金

鑰去加密 64 位元的明文區塊，並且產生 64 位元的密文區塊。這種加密過程，類似於 *DES*[4, 10]，但它的安全性比 *DES* 還高。最明顯的例子爲金鑰的長度比較長，*DES* 的金鑰長度爲 56 位元，而 *IDEA* 的金鑰則爲 128 位元。而且在最近的幾年，*DES* 已經遭受到很多的攻擊，尤其是 "Known-Plaintext Attack"[7]。基於這些可能性攻擊及金鑰長度的安全性，因此我們延續 [9] 裡使用 IDEA 的方法將我們秘密訊息的數字索引檔案進行加密；當然這 *IDEA* 的方法並不是唯一的加密方法，最適合的方法應該取決於我們所應用的密碼系統。

在本文的其它安排方面，在接下來的第二節，我們提供了三個相關的研究文獻以爲比較與應用的依據。另在第三節中，我們隨即介紹我們所提出來的方法，並以一個範例作說明，當然我們亦增附整個研究的處理流程於文末。至於第四節則爲關於本研究的相關比較與分析。最後於第五節中爲我們的結論。

貳、相關研究探討

● *Review I*：

Lin et al. 於 1998[9] 年提出的方法，主要是用來隱藏大量的英文字。文中提到，只要所要隱藏的秘密訊息能夠以 ASCII 碼表示，就能將其轉換成數字代碼，隱藏在掩護的文件當中。其執行之演算法簡述如下：

輸入：

(1)一份欲傳送的明文。

(2)幾份有具體內容的掩護文件，其中一份文件所用到的字元必須至少包含欲傳送明文所用到的字元。

(3)兩把加密金鑰。一把用來加密明文的索引檔案 (Plaintext Index File, PIF for short)，一把用來加密掩護文件的代號 (Identity, ID for short)。

輸出：

(1)加密過的 PIF。

(2)包含 ID 的掩護文件。

步驟一：根據欲建立索引代碼之掩護文件，將每一個用到的字元，建立每個字元的數字代碼，以產生字元位置對應表格 (Character's Position Table, CPT for short)。

步驟二：將我們欲傳送的明文，將其每一個字元，根據 CPT 隨機地選取其相對應的數字代碼，稱其爲明文索引檔案 (PIF)。

步驟三：使用任何一種壓縮方法，壓縮 PIF 檔。

步驟四：爲我們欲傳送的所有掩護文件隨機地建立代號 (ID)。

步驟五：使用第一把加密金鑰，加密壓縮過的 PIF 檔。

步驟六：使用第二把加密金鑰，加密建立索引代碼之掩護文件代號 (ID)，將其結果放置在步驟五所產生之加密壓縮過的 PIF 檔前頭。

步驟七：送出所有包含代號的掩護文件，i.e. 即多份掩護文件，及步驟五、步驟六所產生之加密壓縮過的 PIF 檔及加密過的 ID。

就 [9] 所提出之方法而言，基本上似乎能夠隱藏大量的秘密訊息在文件中；但如果是應用在中文的系統中，就會發生較難尋找出一份掩護文件。其理由爲我們所要傳輸的是中文字，而中文字不像英文單字裡的處理：只有二十六個字母下去變化。在英文文件中，隨便一篇英文文章，就能輕易包含我們所要傳輸的英文訊息。因爲有此項缺點，因此在文獻 [12] 所提出的方法可以執行中文環境下的處理，說明

如下：

● *Review II*：

在 [12] 所提出的作法，乃是引用 [9] 的基本觀念，利用中文內碼的特性，將我們的中文字轉成 BIG-5 碼的十六進位碼型式，十六進位碼只有 0 到 9；A 到 F 共十六個元素，而每一個中文字又都需要四個十六進位碼表示，如此一來，就能在一篇中文文章中，輕易的建立包含十六個元素的編碼表；故很容易就能將我們所要隱藏的秘密文件之中文轉成十六進位碼的代碼，用掩護的中文文件產生的十六進位碼編號來表示。

其步驟及方法如下：

輸入：

(1)欲傳送的秘密文字。

(2)幾份有具體內容的掩護文件。

(3)對稱式加密金鑰。

輸出：

(1)數份含文件代號與內容的掩護文件。

(2)加密過的掩護文件代號與已經壓縮加密過的秘密文字索引檔案。

步驟一：將欲建立索引代碼的掩護文件，將其轉成 BIG-5 碼型式，進而將每個十六進位碼編號，建立十六進位碼索引表格。

步驟二：將我們已轉成 BIG-5 碼的秘密文字，去比對其每一個十六進位碼與十六進位碼索引表格，隨機選取十六進位碼索引表格中相對之一個數字紀錄，建立該秘密文字之文件索引檔案 (Chinese Document Index File ,CDIF for short)。

步驟三：將秘密文字之文件索引檔案 (CDIF) 進行壓縮。

步驟四：針對每一份掩護的文件，隨機產生一個固定長度的文件代號。

步驟五：使用對稱式之加密金鑰，加密建立索引代碼的掩護文件代號 (ID) 與已經壓縮加密過的秘密文字文件索引檔案 (CDIF)。

解密步驟爲，當接收者接收到所有的掩護文件時，先將其儲存，再利用對稱式解密金鑰，將加密過之索引代碼掩護文件代號與已經壓縮加密過的秘密文字文件索引檔案解密，根據文件代號，找出欲對照之掩護文件，將其轉成 BIG-5 碼後，建立十六進位碼索引表格；將秘密文字文件索引檔案所代表的十六進位碼解出，還原成中文內碼，再拼成內含的中文訊息。

● *Review III*：

我們使用 [11] 所提出的方法，將無論中 / 英文資料進行處理，其主要的精神和特色在於萃取和重建重要機密資訊時，不需要使用原先的掩護圖作爲基底，而是以藏有重要機密資訊的僞裝圖下去做萃取的工作。而對於欲隱藏的秘密資訊位元資料，係透過一個門檻值及預先選定的兩個模組數，進行模的運算，去輕微調整工作像素中部分組成位元，將這些位元取代成我們欲隱藏的位元值，達到資訊嵌入的功用。其精神乃基於人類對於些微的圖像改變，並無法有效辨識出其不同，如此一來，具有重要機密的僞裝圖，能夠不易遭受懷疑，進而遭受攻擊。而隱藏及萃取步驟如下：

(1)資訊前置處理程序

首先，將其欲隱藏的位元值，利用 DES-like 的密碼系統進行加密編碼的工作，使其變成一堆雜亂無章的亂碼，外人無法從中獲取資訊，了解其意涵。

(2)資訊嵌入程序

在掩護圖中，透過虛擬亂數產生器，選定一個工作像素，計算其像素值，設定一個門檻值 T，依據門檻值 T 與工作像素的大小關係決定選取的兩個模組數 m_u 和 m_l，推得我們可以取代改變的位元數

目，即如果像素值大於門檻值，則可以取代 $\lfloor log_2^{m_u} \rfloor$ 個位元；反之，如果像素值小於門檻值，則可以取代代 $\lfloor log_2^{m_l} \rfloor$ 個位元，再根據嵌入資訊的位元內容，透過模 *(modulo)* 的運算，把位元值嵌入，假設門檻值 T 取 *160* 、兩個模組數 m_u ， m_l 分別取 8 與 4 ，那麼原則上當像素值大於門檻值者，透過模組數 8 來處理嵌入 3 位元的雜亂位元串列，小於門檻值者，則透過模組數 4 來處理嵌入 2 位元的雜亂位元串列，最後形成僞裝圖。而此方法爲以 256 色灰階圖爲主要的研究對象，所以其掩護圖的像素數值分布爲 0~255 。

(3)資訊萃取程序

在萃取重建重要機密資訊的過程中，僅需要使用到僞裝圖及一些相關的參數。我們先利用亂數產生器，在僞裝圖中，找到其工作像素，接著推估嵌入資料的數量，萃取出嵌入的資料，再解密出機密資訊的原始值，便可眞正獲得重要、機密資訊。

參、無警性的文件秘密傳送研究

由於 [9,12] 所提的方法，最後都是將秘密訊息的數字索引檔案加密處理形成密文傳送給接收者。在他們的處理中皆於網路傳輸資料時，先傳送幾份掩護文件，中間再夾雜眞正欲對照的掩護文件及加密過的秘密訊息索引檔案，雖然初期駭客一開始先看到幾份有具體內容的掩護文件，並不會因此產生懷疑，但等到一旦看到加密過的秘密訊息的索引檔案，即會懷疑內藏玄機而予以非法截取，雖然此時已無法截取原先欲對照的掩護文件，而無法解出其訊息。但在這裡其研究忽略了一點，假若駭客一次將所有傳輸的資料全部截取或直接中斷傳送，則上述兩篇所提的方法，便有其風險性存在。因此本篇我們提出一種新的作法，將加密過的秘密訊息數字索引檔案，轉成二進位碼的型式，應用 [11] 的資訊隱藏技巧，再將其隱藏入我們所傳輸的圖片中。如此一來，所有在網路傳輸的文字或圖片，都是可見的明文，不易遭到駭客的注意與刻意攻擊。以下我們介紹我們的演算法與實例說明之：

【演算法】無警性的文件秘密傳送之加解密

輸入：

(1)一張具有圖片及其雙語說明文字的資料檔。這雙語說明文字所用到的字元代碼，必須至少包含所有欲傳送的秘密中英文字所用到的所有字元代碼。

(2)欲傳送的秘密中英文訊息。

(3)對稱式的加密金鑰。

輸出：隱藏秘密中英文訊息代碼資料的圖片及其雙語說明文字檔。

執行步驟如下：

步驟一：將欲傳送的秘密訊息之中文字，以 BIG-5 碼的型式表示。

步驟二：將傳送圖片之中文說明文字，轉成 BIG-5 碼。

步驟三：檢查圖片之中文說明文字，轉成 BIG-5 碼後，是否至少包含所有欲傳送的秘密中文訊息轉成 BIG-5 碼的所有十六進位碼。

步驟四：檢查圖片之英文說明文字，是否至少包含所有欲傳送的秘密英文訊息所用到的所有英文字元，包括標點符號。

步驟五：根據圖片之中文說明文字所產生之 BIG-5 碼，將所有十六進位碼由左至右依序由 1 開始編號，以建立十六進位碼索引表格 (Hexadecimal Code Index Table, HCIT for short) 。

步驟六：根據圖片之英文說明文字，將每個字元（包含空格）由左至右由1開始編號，以建立英文字元對應表格(English Character's Position Table, ECPT for short)。

步驟七：根據十六進位碼索引表格，比對秘密中文訊息之每一個十六進位碼與十六進位碼索引表格中相對的對應數字索引值，隨機選取一數字代表，以建立秘密中文訊息之 BIG-5 碼數字索引檔案(Chinese Index File, CIF for short)。

步驟八：根據英文字元對應表格，比對秘密英文訊息之每一個英文字元與英文字元對應表格中相對之對應位置數字值，隨機選取一數字代表，以建立秘密英文訊息之數字索引檔案(English Index File, EIF for short)。

步驟九：利用加密金鑰，將步驟七及步驟八所產生之數字索引檔案分別進行加密。

步驟十：將加密過的中英文秘密訊息數字索引檔案轉成二進位碼的型式。

步驟十一：將所得之二進位碼，應用[11]所提之方法，隱藏入我們所使用的灰階圖之每一像素中。

【範例】

假設我們欲傳送的中英文秘密訊息分別爲："一種無警性的文件秘密傳送研究"及"non-sense document in transit with secret hiding."。

而我們傳送的圖片說明文字檔如圖1，而其文字說明亦如下：

"端午節前夕，陳水扁總統向一群高中畢業生分發粽子。"英文譯文爲：

"Before the Dragon Boat Festival, President Chen Shui-bian gives away wrapped rice dumplings to a crowd of high school graduates."

圖一、範例說明圖

其處理步驟如下：

步驟一：我們先將欲傳送的秘密中文訊息"一種無警性的文件秘密傳送研究"改以 BIG-5 碼型式，表示如下：

A440 BAD8 B54C C4B5 A9CA AABA A4E5 A5F3 AFB5 B14BB6C7 B065 ACE3 A873

步驟二：將圖片之中文說明文字"端午節前夕，陳水扁總統向一群高中畢業生分發粽子。"，亦轉成 BIG-5 碼型式，表示如下：

BADD A4C8 B860 AB65 A469 A141 B3AF A4F4 ABF3 C160 B2CE A656 A440 B873 B0AA A4A4 B2A6 B77E A5CD A4C0 B56F BAEA A46C A143

步驟三：檢查圖片之中文說明文字，轉成 BIG-5 碼後，其十六進位碼是否至少包含所有欲傳送的秘密中文訊息轉成 BIG-5 碼後所有的十六進位碼。

步驟四：檢查圖片之英文說明文字，其英文字元是否至少包含所有欲傳送的秘密英文訊息所用到的所有英文字元，包括標點符號。

步驟五：根據圖片之中文說明文字"端午節前夕，陳水扁總統向一群高中

表1：十六進位碼索引表格(HCIT)

十六進位碼	對應數字索引值
0	12,40,52,58,80
1	22,24,38,94
2	42,66
3	26,36,56,96
4	6,18,23,30,32,50,51,62,64,78,90,95
5	16,47,74,82
6	11,15,19,39,46,48,68,83,91
7	55,70,71
8	8,10,54
9	20
A	2,5,13,17,21,27,29,33,45,49,59,60,61,63,67,73,77,86,88,89,93
B	1,9,14,25,34,41,53,57,65,69,81,85
C	7,37,43,75,79,92
D	3,4,76
E	44,72,87
F	28,31,35,84

畢業生分發粽子。"，所產生之BIG-5碼，如下所示：

BADD A4C8 B860 AB65 A469 A141 B3AF A4F4 ABF3 C160 B2CE A656 A440 B873 B0AA A4A4 B2A6 B77E A5CD A4C0 B56F BAEA A46C A143

將所有十六進位碼由左至右依序由1開始編號，建立十六進位碼索引表格，如下表1：

步驟六：根據圖片之英文說明文字，如下所列：

Before the Dragon Boat Festival, President Chen Shui-bian gives away wrapped rice dumplings to a crowd of high school graduates.

將每個字元（包含空格），依序由左至右由1開始編號，以建立英文字元對應表格，如下表2：

表2：英文字元對應表格(ECPT)

英文字元	對應位置數字值
B	1,19
e	2,6,10,25,35,39,45,61,74,80,125
f	3,104
o	4,16,20,93,99,103,114,115
r	5,13,34,70,77,98,119
'space'	7,11,18,23,42,47,57,63,68,76,81,91,94,96,102,105,110,117
t	8,22,27,41,92,124

英文字元	對應位置數字值
h	9,44,49,106,109,113
D	12
a	14,21,30,55,64,66,71,95,120,123
g	15,58,89,108,118
n	17,40,46,56,88
F	24
s	26,36,62,90,111,126
i	28,37,51,54,59,78,87,107
v	29,60
l	31,86,116
,	32
P	33
d	38,75,82,101,121
C	43,79,97,112
S	48
u	50,83,122
-	52
b	53
w	65,69,100
y	67z
p	72,73,85
m	84
.	127

步驟七：比對步驟一之秘密中文訊息"一種無警性的文件秘密傳送研究"，所產生之每一個十六進位碼"A440 BAD8 B54C C4B5 A9CA AABA A4E5 A5F3 AFB5 B14BB6C7B065 ACE3 A873" 與十六進位碼索引表格（表一）中相對的對應數字索引值，隨機選取一數字代表，建立秘密中文訊息之 BIG-5 碼數字索引檔案(CIF)，得下表 3。

表3：秘密訊息中文字BIG-5碼索引檔案(CIF)

17,18,50,40,9,13,4,10,34,74,23,7,79,51,1, 74,45,20,79,27,2,5,53,59,88,90,44,82,33, 16,28,26,13,31,41,16,9,22,95,14,57,39,43, 70,34,58,68,47,27,7,72,96,77,10,55,36

步驟八：比對秘密英文訊息 "non-sense document in transit with secret hiding." 之每一個英文字元（包含空格）與英文字元對應表格（表二）中相對之對應位置數字值，隨機選取一數字代表，建立秘密英文訊息之數字索引檔案(EIF)，得下表 4。

表4：秘密訊息英文字索引檔案(EIF)

17,20,56,52,62,6,17,90,10,11,38,4,43,50, 84,25,46,22,18,51,40,63,27,70,14,56,62, 51,41,81,69,28,41,106,1,62,35,97,13,39, 22,63,9,54,82,51,56,15,127

步驟九：利用加密金鑰，將步驟七與步驟八所產生之數字索引檔案加密。

步驟十：將加密過的數字索引檔案轉成二進位碼的 0 與 1 型式。

步驟十一：將所得之二進位碼，應用 [11] 所提之方法，隱藏入我們所使用的灰階圖之每一像素中。

至此我們已經完成了所有的數字索引代碼藏入動作。而當接收端收到相關處理訊息後，可執行下列的萃取秘密訊息步驟，介紹如下：

步驟一：將經由網路傳輸收到的圖片檔，利用 [11] 所提之方法，將每一 Pixel 所隱藏入之二進位碼萃取出，以一個位元組爲一個單位，還原成數字檔。

步驟二：利用解密金鑰，解密前一步驟所得到之數字檔，還原成我們所隱藏之中英文秘密訊息的 CIF 與 EIF。

步驟三：將我們所收到之圖片中文說明，先自行轉成 BIG-5 碼型式。

步驟四：利用圖片中文說明所轉成之 BIG-5 碼，將所有十六進位碼由左至右依序由 1 開始編號，建立十六進位碼對照索引表格。

步驟五：利用步驟二所得之秘密中文訊息之 CIF，配合十六進位碼對照索引表格，找出所代表之十六進位碼後，再以四個十六進位碼爲單位，還原解出隱藏之中文秘密訊息。

步驟六：將我們所收到之圖片英文說明，將每個字元（包含空格），依序由左至右由 1 開始編號，建立英文字元對應表格 (ECPT)。

步驟七：以步驟二所得之秘密英文訊息的 EIF，配合 ECPT，還原解出我們隱藏之英文秘密訊息。

在文末所附圖 2 與圖 3 裡，可藉由流程圖來清楚說明本論文實際的處理方式。

肆、安全性分析與效果評估

本篇方法最主要的設計精神，乃爲了避免駭客的非法不當截取，爲了欺騙駭客，我們使用了欺人的雙語說明文字，及一張說明圖片，完全用明文的型式傳輸秘密訊息；一旦駭客看到一張圖片，及其說明文字，並不會加以懷疑，與進行攻擊。如此的方式，不僅欺騙了駭客之耳目，也達到了資訊安全的目的。而且駭客若想試圖解出其中的秘密訊息，將會遭遇到以下的兩個基本問題。

(1)如何將隱藏在圖片中每一像素的二進位碼萃取出，而且如何判斷一個像素中到底隱藏入多少個二進位碼？

藉由在 [11] 的研究，由於最高容量的資訊隱藏技術乃是根據每一像素的像素值與門檻值相比較去判斷欲在每一個像素中，取代多少個二進位碼。由於每一像素值不同，取代的位元個數也不盡相同，如此的安排增加駭客解讀出正確數字索引值的困難度；另外在所選用的門檻值及預先選定之兩個模組數，亦使得讀得所隱藏的像素位置更增添困難度。

(2)一旦其成功的由影像中猜出秘密訊息的數字索引檔案，但其如何將加密過的數字索引檔案進行解密，還原成原始數字檔？

由於我們所使用的加密方法爲 IDEA，不管駭客使用何種攻擊方法，他都必須將 128 位元的加密金鑰進行破解動作，並且花費計算時間去解密還原截取到的數字索引檔，如此的方式在計算時間有限下，仍是不可行的 [3]。

另外由於我們所產生的秘密訊息數字索引檔案，乃是隨機產生的，縱使是相同

的秘密訊息，也有不同的索引檔案，如此安排亦增加了系統的安全性。至於如何找出合適的雙語說明文字爲掩護的訊息方面，由於我們中文字，乃是使用 BIG-5 碼的十六進位碼的型式，而英文字元亦只有二十六種字母的變化，所以只要在網路上任意截取一篇雙語文章，都能夠同時擁有所有的十六進位碼，及英文秘密訊息所用到的字元。並且透過安排使得它們擁有不同的數字變化，如此一來，以不易遭到質疑的圖文傳送，隨即完成秘密文件傳送的目的。

另外在實際的資料空間傳輸量方面，由於我們所提方法裡的中英文秘密資料需要四種相關索引表格輔助，分別爲十六進位碼索引表格、英文字元對應表格、 秘密訊息中文字 BIG-5 碼索引檔案與秘密訊息英文字索引檔案等，才得以進行最後的隱藏資料回復演算。也就是說，爲能實現秘密資料傳送目的，於傳送前，需另外至少四倍於原秘密資料的輔助索引表格產生。而在文獻 [9, 12] 的研究中，除這些多倍於原秘密資料的輔助索引表格得傳送外，爲加強＂掩人耳目＂的效果得再選擇多份完全不同於秘密文件的其他明文文件伴隨壓縮處理的索引表格一起傳送，因此在資料空間傳輸量方面將爲原秘密文件資料空間的數多倍空間需求與網路頻寬傳送，即需以較多於原秘密文件的空間需求換取＂掩人耳目＂的文件傳輸效果。若考慮本文中我們所提的方法，由於我們的資料隱藏方式爲空間域 (Spatial Domain) 形式，在人類視覺可接受的範圍內，一般可取用的灰階圖像像素最多爲最後的 4 或 5 個位元 [2] ，即綜合所有的取用空間約爲原圖像的一半空間。爲能完全隱藏至少四倍於原秘密資料的產生輔助索引表格，使得本方法中所取用的僞圖 (Cover Image) 得有至少八倍於原秘密資料的圖像。若以一般所常使用的 512(512 像素分佈的灰階圖像爲例，則可容納約 8192 個位元組資料隱藏，即 8KB 的資料量。此資料對於一般的四至五頁內的機密文件傳送應可足夠，即爲本文所強調的無警性文件傳送的效果。尙且在傳送的過程中，本方法已完全免除了在 [9, 12] 裡得有額外的多份其他明文文件與伴隨壓縮處理的索引表格傳送（所有資料亦爲數多倍於原秘密文件的空間需求量），僅需一般的圖像傳送，即可於接受端進行機密資料的演算法回復，得到實際的原秘密文件。此性質使得在常態下的經常性幾頁機密文件處理傳送裡，我們不可察覺性的隱藏訊息圖像傳送可確實發揮效果。當再考慮更大量的文件資料量處理，在文獻 [9, 12] 裡的所需多份額外掩護性質的明文與索引資料檔的空間需求與傳送量亦隨之增大；我們的方法亦得依資料量增加而以不同張的掩藏圖像 (Stego-image) 傳送。然就整體性而言，在空間需求上，比較先前文獻的相關伴隨資料傳送，我們所提方法在圖形傳送先天限制上（空間需求）得略多於先前研究的所有傳送資料，但並不需過度增加傳輸負擔，且實際應用上，亦實現無密碼形式的機密性文件傳送的效果。

綜合得知，我們所提出之“無警性的文件秘密傳送研究” 與之前所提之方法 [9 ,12] ，有以下之不同之處：

㈠ [9] 與 [12] 是透過於網路上傳輸數張之掩護文件，而我們所提出之方法，只需傳輸一張圖片說明檔，包括中英文之雙語說明文字。如此一來可以減少於網路上傳輸的量。

㈡本篇所提之方法，最大的不同之處在於，我們放在網路傳輸的資料都是可見的明文，不易引起駭客的懷疑，而遭受攻擊。較先前所提之方法，將秘密文件索引檔案經過加密，放於網路上傳輸，容易遭受駭客的攻擊，具有一定的風險性。

㈢至於我們所提之方法，能夠同時隱藏大量的中英文訊息，亦是不同於先前文獻所提之方法，各僅處理中文或英文的資料。

㈣當然在本研究裡也並非無缺點，即我們仍然必須將我們所傳輸的資料，先行建立索引表格，這樣如果我們傳輸的量多的話，較費時間。而且如果是中文字，則必須再透過 BIG-5 碼的轉碼程序，將其轉成代碼的型式，不管是傳送端的轉碼或者是接收端的還原，都得經歷這個步驟，爲其所潛在的問題。然有關表格建立與轉碼程序在程式的處理只是一種對應關係式的處理，就時間的執行上，尤其是硬體的實作，將是非常的快速，而不會降低系統的開發價值。

伍、結論

本文所提出之方法，乃是改良 [9] 與 [12] 所提出的方法，他們所提的方法在傳送過程中有密文夾雜於其中易遭刻意截取與破壞爲最大的缺點；而本文最大的特色在於所有傳輸的過程都是可見的明文，僅透過一張圖片及其說明文字檔，就能夠隱藏大量的中英文訊息，減少傳輸多份掩護文件檔案的量及被非法攻擊的機率。這對於利用有意義的文件去隱藏秘密資訊的安全性問題，提供了一個新的思考方向。我們期望在不久的未來，能夠有類似的方法被提出，且使用有意義的明文，去隱藏大量需保密性的文件資訊。

參考文獻

1. F.L. Bauter, Decrypted Secret: Methods and Maxims of Cryptography, Spring-Verlag, Berlin, pp. 8-9, 1997.
2. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," IBM System Journal, Vol. 35, No. 3&4, pp. 313-336, 1996.
3. A. Curiger and B. Stuber, "Specifications for the IDEA Chip," Technical Report No 92/03, ETH Zurich, Institute for Integrate System, 1992.
4. R.M. Davis, The Data Encryption Standard in Perspective, Computer Security and the Data Encryption Standard, National Bureau of Standards Special Publication, February 1978.
5. H.J. Highland, "Data Encryption: a Non-mathematical Approach-Part 5," Computers & Security, 14(2), pp. 93-97, 1995.
6. D. Kahn, The Codebreakers, Macmillan, New York, 1967.
7. C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a Public World, Prentice Hall Series in Computer Networking and Distributed Systems, Englewood Cliffs, NJ, 1995.
8. X. Lai and J. Massey, "A Proposal for a New Block Encryption Standard," Proceedings of Eurocrypt '90, Spring-Verlag, Berlin, pp. 389-404, 1991.
9. C.H. Lin and T.C. Lee, "A Confused Document Encrypting Scheme and its Implementation," Computers & Security, Vol.17, No. 6, pp. 543-551, 1998.
10. B. Schneier, Applied Cryptography, Wiley, New York, 1994.
11. S.J. Wang and K.S. Yang, "A Scheme of High Capacity Embedding on Image Data Using Modulo Mechanism," The Second International Workshop on Information Security Applications (WISA), Korea, pp. 299-309, Sept., 2001.

12. W.H. Yeh and J.J. Hwang, "A Scheme of Hiding Secret Chinese Information in Confused Documents," Journal of Information Management, Vol. 7, No. 2, pp. 183-191, Jan., 2001.

13. W.H. Yeh and J.J. Hwang, "Hiding Digital Information Using a Novel System Scheme," Computers & Security, Vol. 20, No. 6, pp. 533-538, 2001.

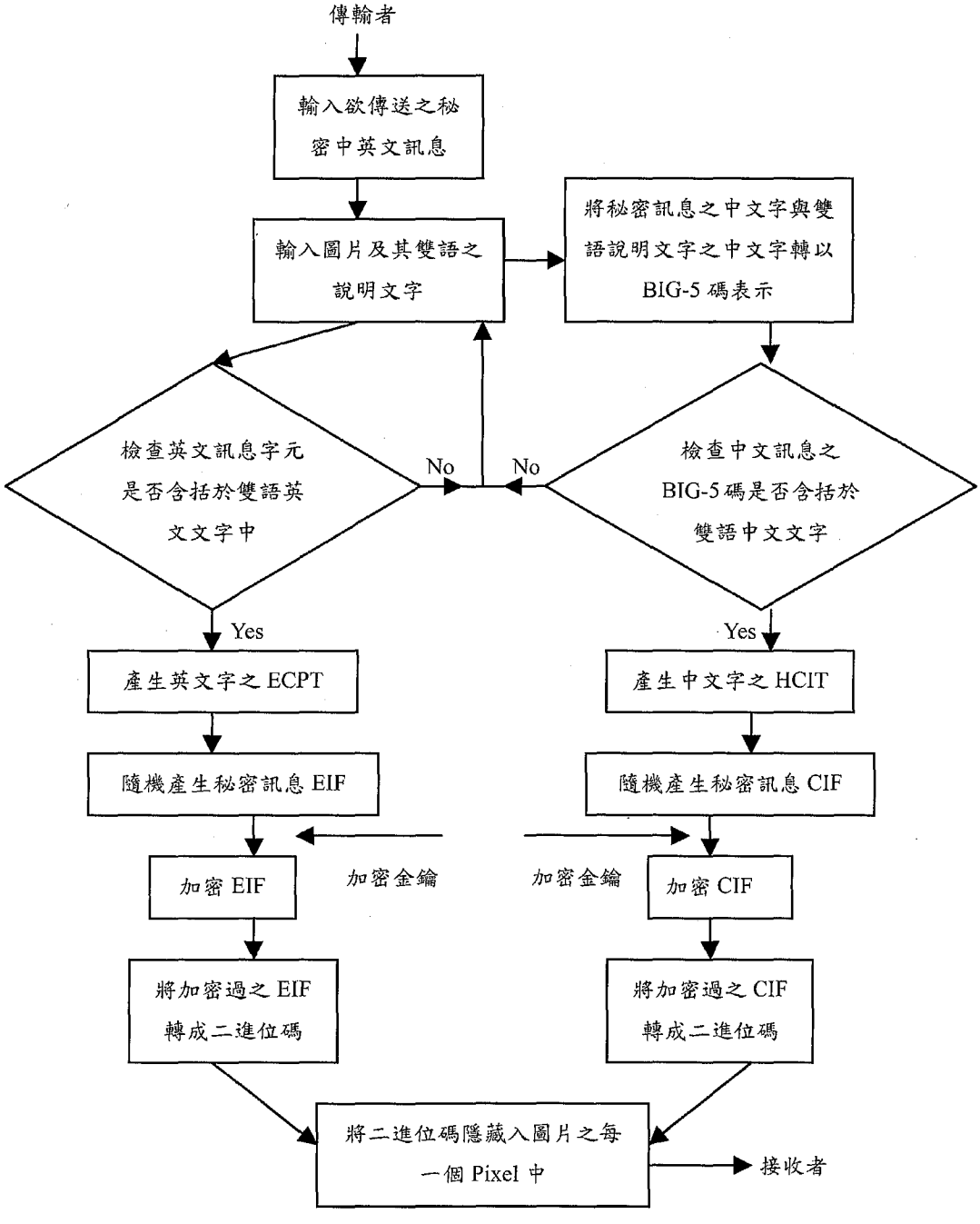

圖2：秘密訊息隱藏之處理流程圖

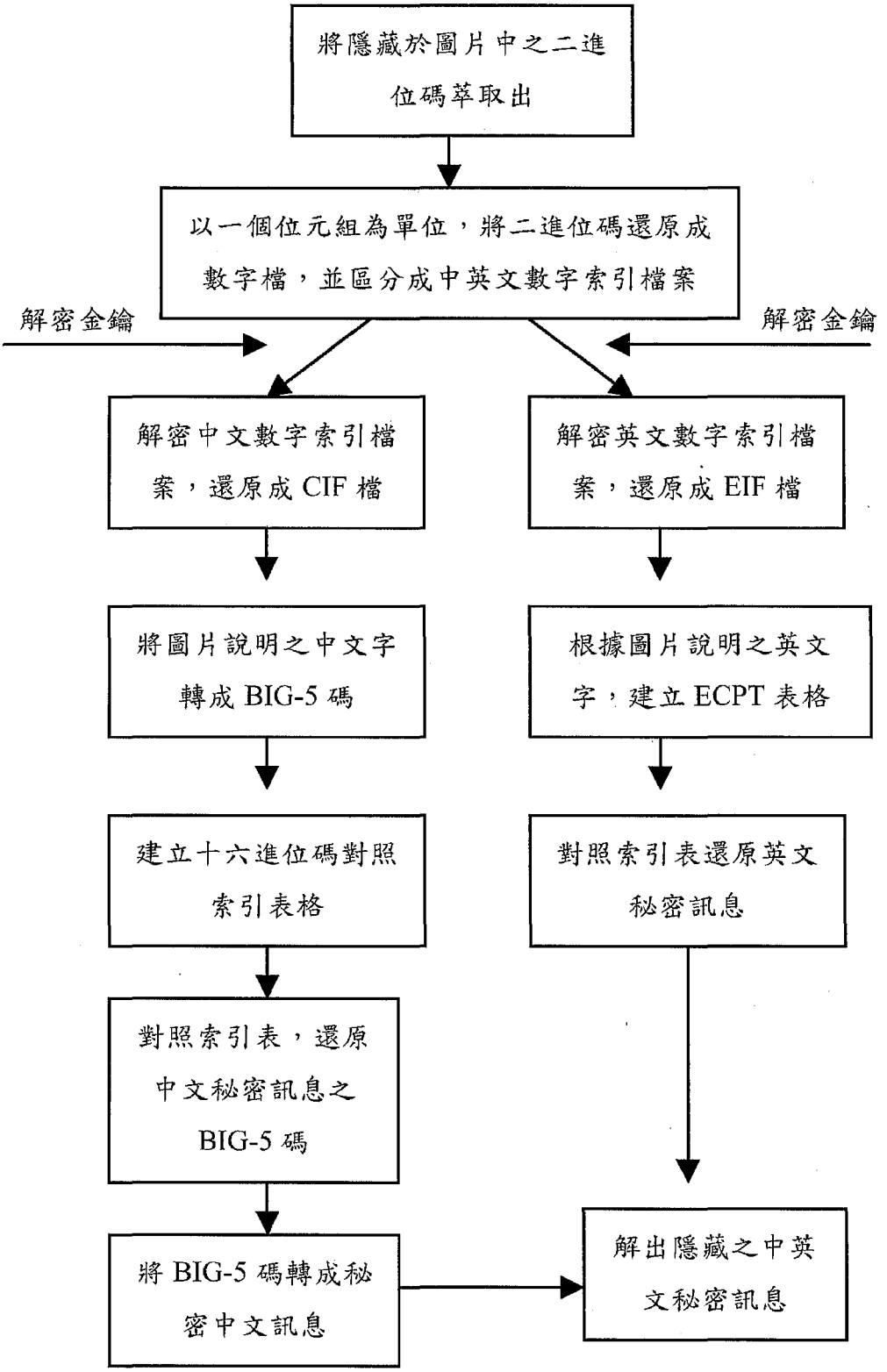

圖3：秘密訊息萃取之解密流程圖