

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：97141521

※申請日期：97.10.29 ※IPC 分類：G06K 9/62(2006.01)

一、發明名稱：使用條碼做為多層次授權之資料編碼系統
及使用方法

二、申請人：(共 1 人)

姓名或名稱：中華電信股份有限公司

代表人：呂學錦

住居所或營業所地址：桃園縣楊梅鎮新榮里民族路 5 段 551 巷 12 號

國 籍：中 華 民 國

三、發明人：(共 5 人)

姓 名：1.黃景煥

2.鄭維恆

3.游世安

4.柳恆崧

5.吳坤榮

國 籍：中 華 民 國

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係為一種使用條碼做為多層次授權之資料編碼系統及使用方法，特別是一種條碼圖樣中具有多層授權內容的秘密管理方式。

【先前技術】

習用技術如我國專利第 142606 號『一種二維安全自由碼之設計及其編解碼器之製作方法』之所示，係將資料分成一般資料和機密資料，並且提供機密資料兩道防護：第一道防護是將機密資料做資料隱藏以消除破解者之好奇心理；第二道防護則是對機密資料加入安全措施，以增加破解之困難度。由此可知，目前以條碼做為加解密的相關技術皆是採用一張密文影像對應一組解碼金鑰的運作方式，若欲依照不同金鑰層級發佈訊息時，需各自使用相對應的金鑰將密文分成數個層級，然後再編成對應的多張條碼圖樣。唯此方法需要記錄各自圖片與金鑰的對應，因此當數目逐漸增加時，所需要的對應數目也會隨之增加，因此在管理金鑰與條碼密文影像時顯得十分的不方便。

由此可見，上述習用方式仍有諸多缺失，實非一良善之設計，而亟待加以改良。

本案發明人鑑於上述習用方式所衍生的各項缺點，乃亟思加以改良創新，並經研究後，終於成功研發完成本件

使用條碼做為多層次授權之資料編碼系統。

【發明內容】

本發明之主要目的在於提供條碼圖樣中具有多層授權內容的秘密管理方式，係利用金鑰分層授權的方式，對於同一張含有密文的條碼圖樣可以依據使用者所具有的授權金鑰權限，取得符合其權限的內容資訊。

本發明之另一目的在於改進一密文條碼圖樣與對應一組授權金鑰，可減少在數目龐大時對應關係之管理負擔。

可達成上述發明目的之使用條碼做為多層次授權之資料編碼系統及使用方法，主要係利用分層授權的概念，將金鑰分解成多塊具有不同權限的子金鑰，若金鑰其值為 K ，經分解後的子金鑰定義為 $\{K_1, K_2, \dots, K_N\}$ 共計 N 種權限，其中 $K_i, i=1 \sim N$ ，可為 K 中任意區段的排列組合。在加密時，各區段子金鑰各自加密所對應的明文區段產生密文區段，之後將所有的密文區段組合而成一密文全文，並以此密文全文做為條碼內容用以產生一條碼圖樣。

解密時，使用者持一裝置掃描此密文全文之條碼圖樣，此裝置內包含有該使用者所擁有的子金鑰，因此對於同一張條碼密文影像，持有不同子金鑰的使用者可以取得符合其子金鑰授權的訊息，本發明中的條碼解譯模組會依

據所取得的金鑰資訊，將密文解出符合其權限的資訊片段或是資訊全文。

【實施方式】

請參閱圖式係本發明使用條碼做為多層次授權之資料編碼系統，其括有：

一金鑰模組 103，其用途在於產生一組用於加密的金鑰 102，以及將此金鑰 102 依照保密層級分解成多組之子金鑰，該金鑰 102 為金鑰模組 103 中子金鑰的組合，賦予特定權限的使用者操作讀取條碼中的密文使用；

一加密模組 104，其用途在於將資訊明文，依照保密層級各自以對應的子金鑰加密，並輸出加密後的密文片段；

一條碼產生模組 105，用來輸入為經各子金鑰加密後的密文片段，後將片段密文串接組合後做為條碼內容，用以產生包含此內容的條碼圖樣；

一條碼讀取模組 303，用於讀取含有密文的條碼圖樣，並將條碼圖樣內容解譯回密文；以及

一條碼解譯模組 305，利用系統持有的金鑰 102 解譯片段之密文資訊。

如圖一為本發明使用條碼做為多層次授權之資料編碼系統的產生加密條碼實施例圖。其加密條碼產生方式首

先輸入一訊息 101 及一金鑰 102，利用一金鑰模組 103 將金鑰 102 依照使用者定義的機密等級分割成金鑰區塊，並以加密模組 104 對各個訊息區塊加密，再以條碼產生模組 105 製作出加密條碼圖樣 106。其中條碼產生模組 105 所產生之條碼圖樣可為任何形式之一維條碼或是二維條碼。

圖二為本發明使用條碼做為多層次授權之資料編碼系統的金鑰模組 103、加密模組 104 及條碼產生模組 105 的細部運作例圖，首先依照使用者選擇將訊息 201 以及金鑰 203 區分成數個對應的訊息區段 202 及金鑰區段 204，利用各個區塊所屬的金鑰對相對應的訊息區塊加密以取得各密文區段 206，之後將各區塊的密文組合成一密文 205。管理者將各金鑰依照欲授權的使用者權限，分別授與包含有屬於該權限的金鑰區塊。

圖三為本發明使用條碼做為多層次授權之資料編碼系統的解譯密文條碼實施例圖，使用者操作解碼時，對於一條碼圖樣 301 使用者利用一條碼讀取裝置 302 讀取條碼，並透過條碼讀取模組 303 以取得條碼內容 304，並利用裝置中的條碼解譯模組 305 及金鑰 306，驗證金鑰暨解析密文 307，用以在密文中解出符合其相對應權限的訊息 308。因為每個使用者的權限不同，因此對於同一張含有密文的條碼圖樣，會將金鑰被賦予授權的密文區塊解析回

明文，對於未授權的區塊則無法解析出任何有意義的資訊。

本發明所提供之使用條碼做為多層次授權之資料編碼系統，與其他習用技術相互比較時，更具備下列優點：

1. 本發明之同一張條碼圖樣可依照使用者所持有的金鑰權限解析出符合其權限內的資訊，可以減少密文條碼圖樣與加密金鑰之間為數眾多的對應關係。

2. 本發明之使用者只能夠依照自己的權限取得所需要的資訊，可利用金鑰有效的管控取得機密資訊權限的使用者。

3. 本發明將密文編碼成條碼圖樣，可以利用條碼具有的容錯功能，即使條碼本身受到部份污損仍可解析資訊，增加資料的可讀性。

上列詳細說明乃針對本發明之一可行實施例進行具體說明，惟該實施例並非用以限制本發明之專利範圍，凡未脫離本發明技藝精神所為之等效實施或變更，均應包含於本案之專利範圍中。

綜上所述，本案不僅於技術思想上確屬創新，並具備習用之傳統方法所不及之上述多項功效，已充分符合新穎性及進步性之法定發明專利要件，爰依法提出申請，懇請貴局核准本件發明專利申請案，以勵發明，至感德便。

【圖式簡單說明】

請參閱有關本發明之詳細說明及其附圖，將可進一步瞭解本發明之技術內容及其目的功效；有關附圖為：

圖一為本發明使用條碼做為多層次授權之資料編碼系統的產生加密條碼實施例圖；

圖二為本發明該使用條碼做為多層次授權之資料編碼系統的金鑰模組、加密模組及條碼產生模組的細部運作例圖；以及

圖三為本發明該使用條碼做為多層次授權之資料編碼系統的解譯密文條碼實施例圖。

【主要元件符號說明】

101、201、308 訊息

102、203、306 金鑰

103 金鑰模組

104 加密模組

105 條碼產生模組

106 加密條碼圖樣

202 訊息區段

204 金鑰區段

205 密文

206 密文區段

201017558

301 條碼圖樣

302 條碼讀取裝置

303 條碼讀取模組

五、中文發明摘要：

一種使用條碼做為多層次授權之資料編碼系統及使用方法，係利用授權等級分段的方式將資訊編碼加密，同時亦將解密金鑰分成與授權等級相互對應的區段；之後將授權等級所屬的解密金鑰以及資訊，分別成對的進行加密，編成區段密文，再組合各區段密文成為密文全文，並以此密文全文做為條碼圖樣的編碼內容。當讀取條碼時，使用者可利用條碼讀取裝置，並配合所屬的金鑰層級解析出該層級對應的資料內容，亦即對於同一張條碼圖樣而言，持有第一層級金鑰之使用者只能解出第一層級的資訊，而持有第二層級金鑰之使用者，則可以解出第二層級的資訊。此系統可以改善含有加密資料的一條碼圖樣只能對應到一組金鑰，而當對應條碼圖樣與金鑰數目眾多時管理上的不便。而分層授權碼的實施，讓使用者讀取一張含有密文資訊的條碼圖樣只能夠取得自身所屬層級的內容，如此可達到資訊保密的目的。

六、英文發明摘要：

十、申請專利範圍：

1. 一種使用條碼做為多層次授權之資料編碼系統，主要包括：

一金鑰模組，其用途在於產生一組用於加密的金鑰，以及將此金鑰依照保密層級分解成多組之子金鑰，該金鑰為金鑰模組中子金鑰的組合，賦予特定權限的使用者操作讀取條碼中的密文使用；

一加密模組，其用途在於將資訊明文，依照保密層級各自以對應的子金鑰加密，並輸出加密後的密文片段；

一條碼產生模組，其輸入為經各子金鑰加密後的密文片段，本模組會將片段密文串接組合後做為條碼內容，用以產生包含此內容的條碼圖樣；

一條碼讀取模組，用於讀取含有密文的條碼圖樣，並將條碼圖樣內容解譯回密文；以及

一條碼解譯模組，利用系統持有的金鑰解譯片段之密文資訊。

2. 如申請專利範圍第 1 項所述之使用條碼做為多層次授權之資料編碼系統，其中條碼產生模組所產生之條碼圖樣可為任何形式之一維條碼或是二維條碼。

3. 一種如申請專利範圍第 1 項所述之使用條碼做為多層次授權之資料編碼系統的使用方法，其加密條碼產生方式首先輸入一訊息及一金鑰，利用該金鑰模組將金鑰依

照使用者定義的機密等級分割成金鑰區塊，並以該加密模組對各個訊息區塊加密，再以該條碼產生模組製作出加密條碼圖樣；解碼時，使用者利用該條碼讀取裝置讀取相對條碼圖樣，並透過該條碼讀取模組以取得條碼內容，並利用裝置中的條碼解譯模組及金鑰，驗證金鑰暨解析密文，用以在密文中解出符合其相對應權限的訊息。

4. 如申請專利範圍第 3 項所述之使用條碼做為多層次授權之資料編碼系統的使用方法，其中條碼產生模組將各等級金鑰的密文片段組合成一密文全文，並以此密文全文做為條碼的內容，經條碼產生模組產生對應的條碼圖樣。
5. 如申請專利範圍第 4 項所述之使用條碼做為多層次授權之資料編碼系統的使用方法，其中條碼解譯模組利用一條碼讀取模組讀取條碼圖樣，並利用條碼解譯模組和金鑰，解譯相對應權限之資訊區塊。
6. 如申請專利範圍第 1 項所述之使用條碼做為多層次授權之資料編碼系統的使用方法，其中該條碼解譯模組對於金鑰未被授權的密文區塊將無法解譯出任何有意義資訊；或條碼解譯模組可檢查該金鑰是否符合密文區塊的授權，若否，則自動略過解譯該區塊資訊。

十一、圖式：

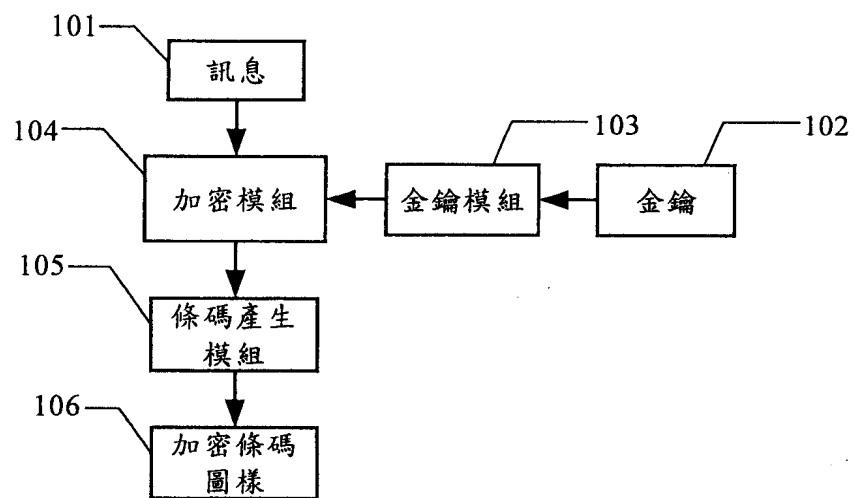


圖 一

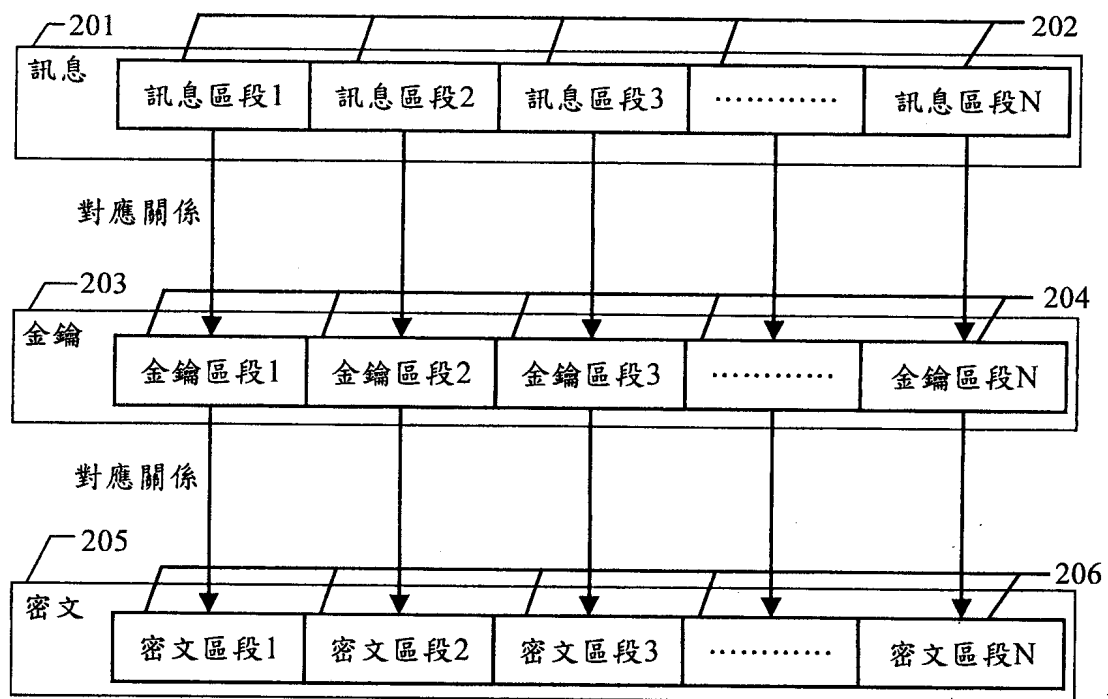


圖 二

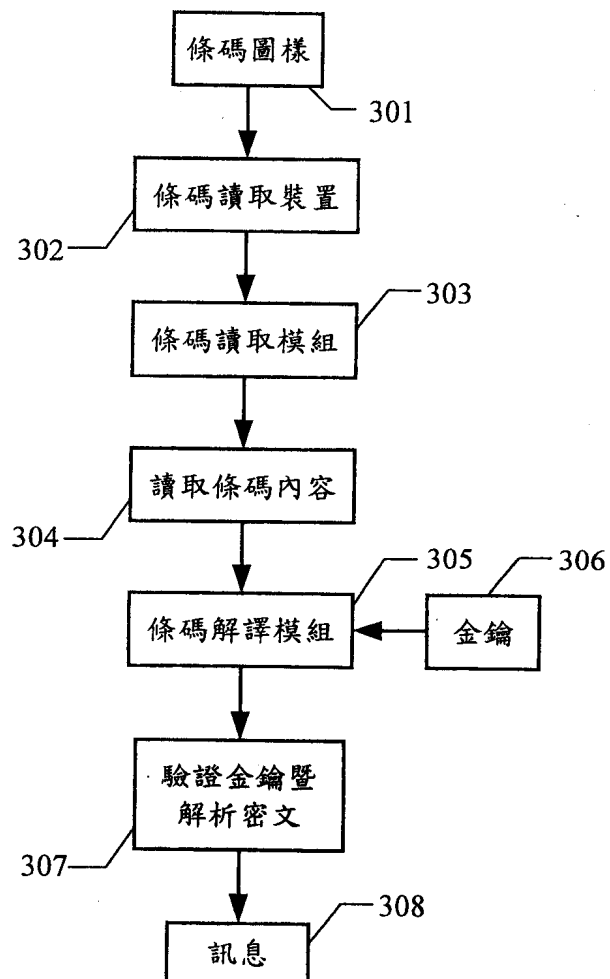


圖 三

七、指定代表圖：

(一)本案指定代表圖為：第 (一) 圖。

(二)本代表圖之元件符號簡單說明：

101 訊 息

102 金 鑰

103 金 鑰 模 組

104 加 密 模 組

105 條 碼 產 生 模 組

106 加 密 條 碼 圖 樣

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：