



(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I499928 B

(45)公告日：中華民國 104 (2015) 年 09 月 11 日

(21)申請案號：103116542

(22)申請日：中華民國 103 (2014) 年 05 月 09 日

(51)Int. Cl. : G06F21/10 (2013.01) G06F21/60 (2013.01)

(71)申請人：國立交通大學(中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號

(72)發明人：李雅琳 LEE, YA LIN (TW)；蔡文祥 TSAI, WEN HSIANG (TW)

(74)代理人：林火泉

(56)參考文獻：

TW 200833059A

TW 201329768A1

CN 102761521A

CN 102843422A

審查人員：楊博翔

申請專利範圍項數：9 項 圖式數：6 共 19 頁

(54)名稱

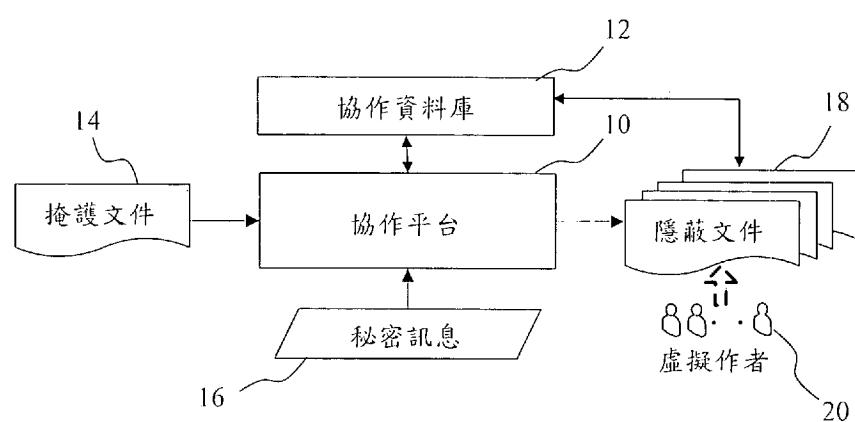
以協作平台上之版本修訂記錄進行資訊隱藏之方法

DATA HIDING METHOD VIA REVISION RECORDS ON A COLLABORATION PLATFORM

(57)摘要

本發明提供一種以協作平台上之版本修訂記錄進行資訊隱藏之方法，其先建立一包括複數文章及複數修訂記錄的協作資料庫，使用者於一協作平台上輸入一掩護文件、一秘密訊息及一金鑰，協作平台依據多人協作過程中可用以隱藏資訊的四個特性，自動將掩護文件轉變成模擬多人協作過程之一隱蔽文件，並將秘密訊息嵌入隱蔽文件中；只有擁有金鑰的授權使用者才能從隱蔽文件中抽出秘密訊息。

The invention provides a data hiding method via revision records on a collaboration platform, which first creates a collaborative database including a plurality of articles and revision records. A user puts as input a cover document, a secret message, and a key on a collaborative platform. Based on four characteristics of multi-user collaborative-writing processing, the collaborative-writing platform is used, together with a key, to hide a secret message into the cover document automatically while simulating a collaborative-writing process. Only authorized users with the key can extract the secret message from the message-hidden document.



- 10 · · · 協作平台
- 12 · · · 協作資料庫
- 14 · · · 掩護文件
- 16 · · · 祕密訊息
- 18 · · · 隱蔽文件
- 20 · · · 虛擬操作者

第1圖

發明摘要

公告本

※ 申請案號：103116542

※ 申請日：103.5.09

※ IPC 分類：G06F 21/00 (2013.01)
G06F 21/60 (2013.01)

【發明名稱】(中文/英文)

以協作平台上之版本修訂記錄進行資訊隱藏之方法 / data hiding method via revision records on a collaboration platform

【中文】

本發明提供一種以協作平台上之版本修訂記錄進行資訊隱藏之方法，其先建立一包括複數文章及複數修訂記錄的協作資料庫，使用者於一協作平台上輸入一掩護文件、一秘密訊息及一金鑰，協作平台依據多人協作過程中可用以隱藏資訊的四個特性，自動將掩護文件轉變成模擬多人協作過程之一隱蔽文件，並將秘密訊息嵌入隱蔽文件中；只有擁有金鑰的授權使用者才能從隱蔽文件中抽取出秘密訊息。

【英文】

The invention provides a data hiding method via revision records on a collaboration platform, which first creates a collaborative database including a plurality of articles and revision records. A user puts as input a cover document, a secret message, and a key on a collaborative platform. Based on four characteristics of multi-user collaborative-writing processing, the collaborative-writing platform is used, together with a key, to hide a secret message into the cover document automatically while simulating a collaborative-writing process. Only authorized users with the key can extract the

I499928

secret message from the message-hidden document.

SECRET

SECRET

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

10 協作平台

12 協作資料庫

14 掩護文件

16 祕密訊息

18 隱蔽文件

20 虛擬作者

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

以協作平台上之版本修訂記錄進行資訊隱藏之方法 / data hiding method via revision records on a collaboration platform

【技術領域】

【0001】 本發明係有關資訊隱藏一種方法，特別是指一種以協作平台上之版本修訂記錄進行資訊隱藏之方法。

● 【先前技術】

【0002】 隨著雲端時代的來臨，有越來越多的協作平台服務已推出，可允許多人共同編輯一份文件，且編修的歷史會被儲存下來，而所有檔案皆傳到雲端上，也產生安全性的隱憂，故尋找出一可應用於協作平台作資訊隱藏的方法是必要的。

【0003】 資訊隱藏為將秘密訊息嵌入在一掩護媒體，其產生的偽裝媒體看起來像原本的掩護媒體，所以攻擊者不會注意到嵌入的訊息之存在。

● 資訊隱藏有許多應用，如機密通訊、安全保存、秘密傳輸等。大部分習知的資訊隱藏方法是利用影像或視訊等媒體來當作掩護媒體，因這些掩護媒體有些部分有人眼難察覺的特性，可用來隱藏資訊；而利用文字組成的文件檔案作掩護媒體的資訊隱藏技術相對的少許多。

【0004】 習知的文字資訊隱藏技術可分為三種種類：(1)基於格式的方法；(2)隨機及統計產生方法；與(3)語言學方法。其中第一種基於格式的方法是改變文件中的格式來隱藏資訊，不會變更到文字的部分，例如利用文字間的空白數量 (inter-word spaces) 來隱藏資訊。第二種隨機及統計產

生的方法直接根據秘密訊息來產生偽裝文件，以避免攻擊者得知原本的隱蔽文件而對隱藏的訊息進行攻擊；或利用重複的模式來隱藏資訊，如空白、縮寫、程式中的區域變數的順序等。

【0005】 第三種語言學方法則是利用自然語言處理中的一些特性來隱藏訊息，如利用同義字替換的方法來隱藏資訊。更詳言之，其主要是根據秘密訊息來挑選要替換的同義字；或利用特定的同義字字典及搭配語辭典來建立一含有秘密訊息的偽裝文件；或利用美國和英國的同義字來替換作資訊的隱藏；或利用追蹤修訂之資訊隱藏方法，將一份文件依一資訊隱藏函式及建立的修訂資料庫改為模擬前版本，再利用追蹤修訂功能將內容還原成原文件。

【0006】 第三種基於文字學作資訊隱藏的方法較第一及第二種方法更容易抵抗攻擊，而最近隨著電腦及網路的發展，有越來越多的協作平台服務推出，如Google Drive、Office Web Apps、維基百科等。這些平台允許多人共同合作編輯一個文件，並會儲存每次編修的記錄，而協作平台也是一個隱藏資訊的極佳平台，可於協作平台提供資訊隱藏的相關應用，如秘密傳輸、訊息之安全保存等。但目前習知之技術未有能適用於協作平台作資訊隱藏的，如同義字替換方法最多只能應用到二篇文章及二個作者，不適用於協作平台上的文件擁有多篇修訂文章及多個作者。

【0007】 有鑑於此，本發明遂針對上述習知技術之缺失，提出一種以協作平台上之版本修訂記錄進行資訊隱藏之方法，提高於雲端協作平台上編輯資料的安全性，以有效克服上述之該等問題。

【發明內容】

【0008】 本發明之主要目的在提供一種以協作平台上之版本修訂記錄進行資訊隱藏之方法，其係在協作平台上模擬多人修訂文件之方式，產生多個版本的文件，藉由二相鄰版本之間文字差異找出所有的修訂配對，並以此建置協作資料庫。

【0009】 更詳言之，本發明利用協作平台版本修訂記錄、進行資訊隱藏之方法，主要係利用協作過程中(1)每一個版本的作者、(2)每個版本中被改的文字序列數量、(3)每個版本中被改的至少一文字序列，以及(4)從協作資料庫中選出新文字序列取代被改的文字序列等特性來隱藏秘密訊息。

【0010】 本發明在進行資訊隱藏時，係在將秘密訊息嵌入時加入金鑰，讓只有授權使用者擁有金鑰，並藉以從隱蔽文件中抽出秘密訊息。

【0011】 為達上述之目的，本發明所進行資訊隱藏方法包括下列步驟：(1)建立一協作資料庫，協作資料庫中包括複數文章及複數修訂記錄；(2)於一協作平台上輸入一掩護文件、一秘密訊息及一金鑰；(3)協作平台自動將掩護文件轉變成模擬多人協作過程之一隱蔽文件，隱蔽文件中包含秘密訊息；以及(4)擁有金鑰的至少一授權使用者從隱蔽文件中抽出秘密訊息。

【圖式簡單說明】

【0012】

第1圖為本發明以協作平台上之版本修訂記錄進行資訊隱藏之方法之框架示意圖。

第2圖為本發明以協作平台上之版本修訂記錄進行資訊隱藏之方法之流程圖。

第3圖爲第2圖中步驟S12之詳細流程圖。

第4圖爲協作資料庫之建置及文章版本產生之順序示意圖。

第5圖爲利用從複數虛擬作者中擇一以隱藏秘密訊息位元之示意圖。

第6A圖至第6G圖爲本發明實際應用之示意圖。

【實施方式】

【0013】 本發明是一種以協作平台上之版本修訂記錄進行資訊隱藏之方法，其框架如第1圖所示，使用者從大量文章、文件中挑選一篇掩護文件14用以隱藏秘密訊息16，接著在協作平台10上模擬多人協作的過程，此過程對該掩護文件14會模擬修正多個版本，將秘密訊息16隱藏在模擬協作的過程中，最後會產生看似由多個虛擬作者20共同協作並含有修正記錄的隱蔽文件18，文章及修訂記錄儲存在一協作資料庫12中。

【0014】 第2圖爲本發明以協作平台上之版本修訂記錄進行資訊隱藏之方法之流程圖，在步驟S10中，建立協作資料庫，協作資料庫中包括文章及修訂記錄，該些文章可在網路上搜尋得到，例如在網路上下載維基百科的420百萬篇文章；而修訂記錄則是將相鄰版本間有文字序列修訂的部分找尋出來，並利用這些找到的文字序列修訂來建立協作資料庫，如第4圖爲例，所示爲一篇從維基百科下載的文章，其修正記錄含有版本 $\{D_0, D_1, \dots, D_n\}$ ，且圖中實線箭頭爲文章版本產生順序， D_i 中較小*i*表示版本較新，而虛線箭頭代表協作資料庫建置時納入的版本順序；當下載文章後，再對每兩篇相鄰的版本 D_i 和 D_{i-1} 找出所有於其中的修訂配對（correction pairs），每一組修訂配對以 $\langle s_j, s_j' \rangle$ 表示，其中 s_j 爲在 D_i 中的一個文字序列（word sequence），且在 D_{i-1} 中被修正成 s_{j-1}' 。舉例來說，假設 $D_i = "National Chia Tang$

University”，而 D_{i-1} = “National Chiao Tung University”，則修訂配對 $\langle s_1, s_1' \rangle$ = <“Chia Tang”, “Chiao Tung”>會被找出並被加至協作資料庫中。另外本發明利用一延伸的最長公共子序列演算法 (longest common subsequence algorithm) 來自動找出下載資料中的修訂配對，並將之加至協作資料庫中。

【0015】 接著，步驟S12中開始隱藏資訊，使用者於協作平台上輸入掩護文件、秘密訊息及金鑰，協作平台自動將掩護文件轉變成模擬多人協作過程之隱蔽文件，隱蔽文件中包含秘密訊息。

【0016】 步驟S12的詳細步驟請參考第3圖所示之流程圖，首先步驟S122把掩護文件當作修訂版本中的最終版本 D_n ，再根據秘密訊息往前去生成版本 $D_{n-1}, D_{n-2}, \dots, D_1, D_0$ ，直到全部的秘密訊息位元被藏入為止，這部分共分析了協作過程中的四個特性來隱藏資訊，包括每一個版本的作者、每個版本中被改的文字序列數量、每個版本中被改的至少一文字序列、及從協作資料庫中選出新文字序列取代被改的文字序列，分別為步驟S124～S129。首先S124利用每一個版本的作者來隱藏秘密訊息，協作平台從一群虛擬作者中挑出幾個並給每個虛擬作者一組唯一二元碼 a ，並稱此虛擬作者為作者 a ，當秘密訊息的前幾個位元同樣為 a 時，則挑選虛擬作者 a 為版本 D_i 的修訂作者，以將秘密訊息位元 a 藏入，如第5圖所示，若目前要嵌入的秘密訊息位元為“01”，則選擇唯一二元碼為01的虛擬作者Jessy為版本 D_i 的修訂作者。此外，從版本 D_0 至版本 D_n 皆會依此法指定一個修訂作者給該版本，故同一位作者於模擬過程中可能會修改多次或沒有參與修改，符合實際的多人修訂情形。

【0017】 步驟S126將利用目前版本中被改的文字序列數量隱藏秘密

訊息，並產生前一版本。從版本 D_i 中挑選複數文字序列，並將之改成版本 D_{i-1} 中的其他文字序列，而這邊總共改的文字序列數量 N_g 也很適合拿來隱藏資訊，對此，先對每個版本能改的文字序列設一修改上限 N_c ，設定修改上限可使得結果更真實，因一般修正時通常同一個版本不會被改非常多字；接著掃描版本 D_i 中所有文字序列，並搜尋協作資料庫中所有的修訂配對 $\langle s_j, s'_j \rangle$ ，其中 s_j 存在於前一版本 D_{i-1} 中；之後，搜集這些修訂配對的所有 s'_j 為一集合 Q_r ，稱 Q_r 為版本 D_{i-1} 中被改的候選文字序列，並從中挑選 N_g 個候選文字序列出來，以將相等於 N_g 值的二進位表示的秘密訊息位元嵌入，例如挑選出三個候選文字序列，3的二進位表示為11，則將秘密訊息位元“11”嵌入文字序列數量中。

【0018】 步驟S128中係將秘密訊息的位元藏入前一版本 D_{i-1} 中被改的文字序列中，將集合 Q_r 中的候選文字序列分成 N_g 組，每一組根據秘密訊息位元挑選一要被修改的候選文字序列 s'_j ，以此將秘密訊息藏入。

【0019】 S129則是從協作資料庫中挑選出來要取代步驟S128候選文字序列 s'_j 的文字序列，是從前一版本 D_{i-1} 中挑選出 N_g 個文字序列 s_j' ，此文字序列就是步驟S126中的新文字序列，由於在步驟S128又將新文字序列挑出來成為一個集合，因此候選文字序列又等於新文字序列，選出的 N_g 個文字序列 s_j' 利用協作資料庫，從中對每個 s_j' 可改的 s_j 根據其修改次數，利用一霍夫曼編碼給每個可選擇的新文字序列進行編碼，每一新文字序列分別產生相應的一對應編碼，並根據秘密訊息來挑選要改的 s_j ，再將 s_j' 更改為 s_j ，以完成目前版本 D_i 的產生。

【0020】 最後如第2圖步驟S14所述，擁有金鑰的授權使用者從隱蔽

文件中抽取出秘密訊息，因為擁有金鑰的使用者才會知道有哪些修訂配對、新文字序列的對應編碼等訊息。

【0021】 第6A圖至第6G圖為本發明實際應用之示意圖，第6A圖為選擇一篇文章做為掩護文件，要將秘密訊息“Art is long, life is short”藏入掩護文件中，經過協作平台模擬多人協作過程後，共產生五個版本的修訂記錄，如第6B圖所示，修訂記錄中包括修訂的日期、時間和作者，其中最新版本的修訂作者為Natalie，最後隱蔽文件如第6C圖，可看到其內容與第6A圖的掩護文件完全相同。第6E圖為最新版本，其內容等於掩護文件，而第6D圖為第6E圖的前一版本，其中方框框出的單字為被修改過的文字序列，此修改中含有秘密訊息。使用者使用正確的金鑰可從第6E圖的最新版本中抽出正確的秘密訊息，如第6F圖所示，而第6G圖為輸入錯誤金鑰所抽出的錯誤訊息，由此可保護秘密訊息隱藏在文件中的安全性。

【0022】 綜上所述，本發明提供之以協作平台上之版本修訂記錄進行資訊隱藏之方法係分析由真人協作的網路資料庫後，從中取得可用的協作資料以建置一協作資料庫，再選擇其中一篇文章做為掩護文件，將秘密訊息隱藏在隱蔽文件中，使隱蔽文件與掩護文件表面看來完全相同，此隱蔽文件中包括模擬多人協作的修訂記錄，並將此修訂記錄加到協作資料庫中。而秘密訊息的嵌入更藉由多人協作過程中可隱藏資訊的四個特性協助秘密訊息的位元一一隱藏到隱蔽文件中；更根據文章中文字序列的修改次數以霍夫曼編碼對此數值編碼，以提升模擬結果的真實性。藉由本發明之方法，可應用到多個作者及多篇修訂文章的協作，更有效地隱藏秘密訊息，可用於秘密傳輸、資訊安全保存等。

【0023】 唯以上所述者，僅為本發明之較佳實施例而已，並非用來限定本發明實施之範圍。故即凡依本發明申請範圍所述之特徵及精神所為之均等變化或修飾，均應包括於本發明之申請專利範圍內。

【符號說明】

【0024】

10 協作平台

12 協作資料庫

14 掩護文件

16 祕密訊息

18 隱蔽文件

20 虛擬作者

申請專利範圍

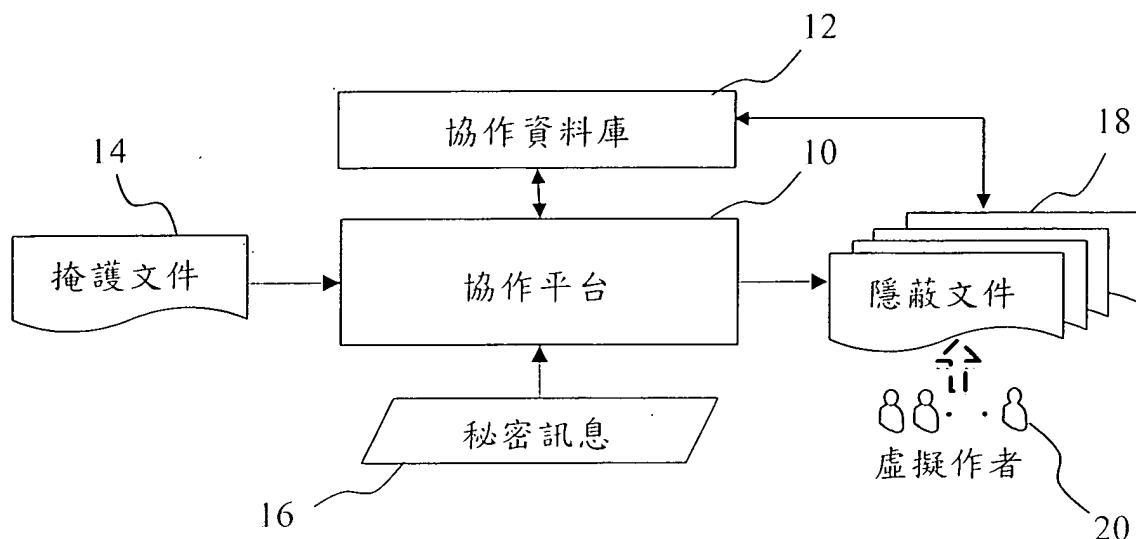
1. 一種以協作平台上之版本修訂記錄進行資訊隱藏之方法，包括下列步驟：
建立一協作資料庫，該協作資料庫中包括複數文章及複數修訂記錄；
於一協作平台上輸入一掩護文件、一秘密訊息及一金鑰，該協作平台自動將該掩護文件轉變成模擬多人協作過程之一隱蔽文件，該隱蔽文件中包含該秘密訊息；以及
擁有該金鑰的至少一授權使用者從該隱蔽文件中抽取出該秘密訊息。
2. 如請求項1所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中該秘密訊息之嵌入係模擬多人協作過程中之複數特性，包括每一個版本的作者、每個版本中被改的文字序列數量、每個版本中被改的至少一文字序列、及從該協作資料庫中選出至少一新文字序列取代被改的至少一文字序列。
3. 如請求項1所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，更包括比較該等文章中相鄰版本者，利用一最長公共子序列演算法（Longest common subsequence algorithm）找出該等文章中所有被改的該文字序列，得到該等修訂記錄，並將其加入該協作資料庫中。
4. 如請求項2所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中該隱蔽文件之產生包括下列步驟：
將該掩護文件做為該文章的最終版本；以及
依據協作過程中的該等特性，將秘密訊息的位元一一隱藏到該掩護文件中，並往前生成前一版本至前n版本的該文章，直到該秘密訊息的全部位元被藏入，形成該隱蔽文件。

5. 如請求項4所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中利用該每一個版本的作者來隱藏該秘密訊息之特性中，該協作平台選擇複數虛擬作者並分別給予一組唯一二元碼，當該秘密訊息的前複數位元與其中一虛擬作者的該唯一二元碼相同時，則定義該作者為一目前版本的修訂作者，將該秘密訊息的該等位元藏入該修訂作者的位元中。
6. 如請求項4所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中利用該每個版本中被改的文字序列數量來隱藏該秘密訊息之特性中，先對每個版本中被改的文字序列數量設一修改上限，再掃描一目前版本中之該等文字序列及該協作資料庫中之複數修訂配對，比對取代該等文字序列之該等新文字序列是否出現於一前一版本中，並蒐集該等新文字序列成為一集合，從該集合中挑選複數候選文字序列，該等候選文字序列的數量轉為二進位表示法，將該秘密訊息的複數位元嵌入該等候選文字序列數量的二進位中。
7. 如請求項6所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中利用該每個版本中被改的文字序列來隱藏該秘密訊息之特性中，係先將該集合中的該等候選文字序列分成複數組，每一組根據該秘密訊息的位元挑選出一該候選文字序列，用以將該秘密訊息的位元嵌入該候選文字序列中。
8. 如請求項7所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中該利用該協作資料庫中選出該新文字序列來取代被改的該文字序列之特性中，從該前一版本中挑選出複數新文字序列並分別給予一對應編碼，再根據該秘密訊息挑選要改的至少一該文字序列，再將要改的該文

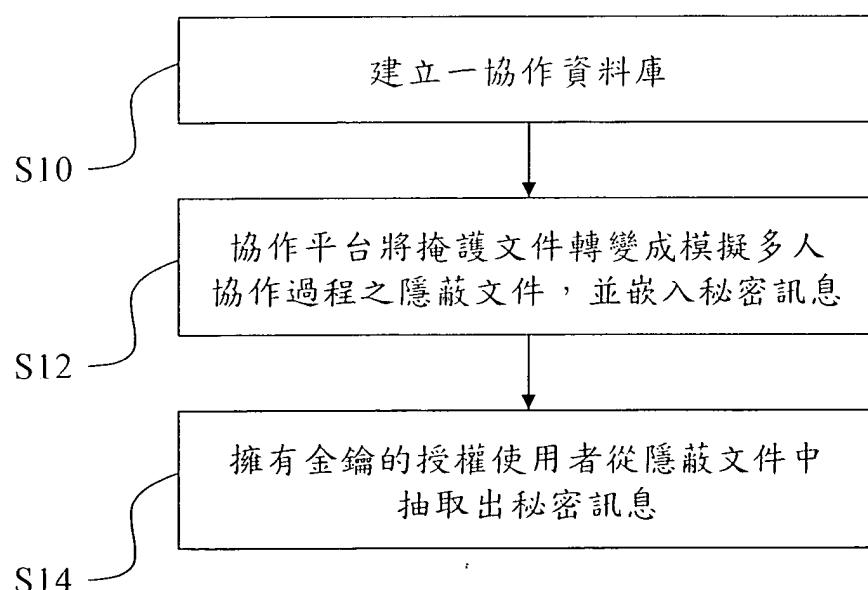
字序列取代該新文字序列，回覆到該目前版本。

9. 如請求項8所述之以協作平台上之版本修訂記錄進行資訊隱藏之方法，其中該對應編碼係分析該等新文字序列的修改次數，利用一霍夫曼編碼根據該修改次數給每個可選擇的該等新文字序列進行編碼。

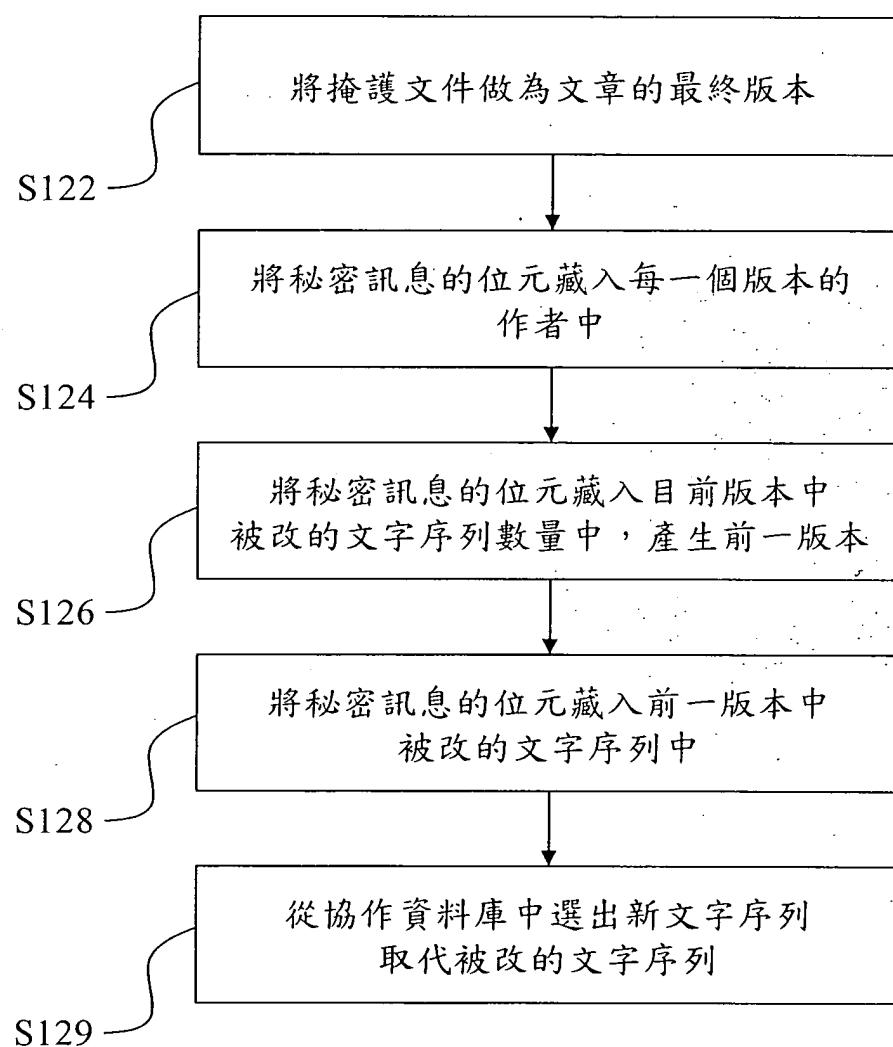
圖式



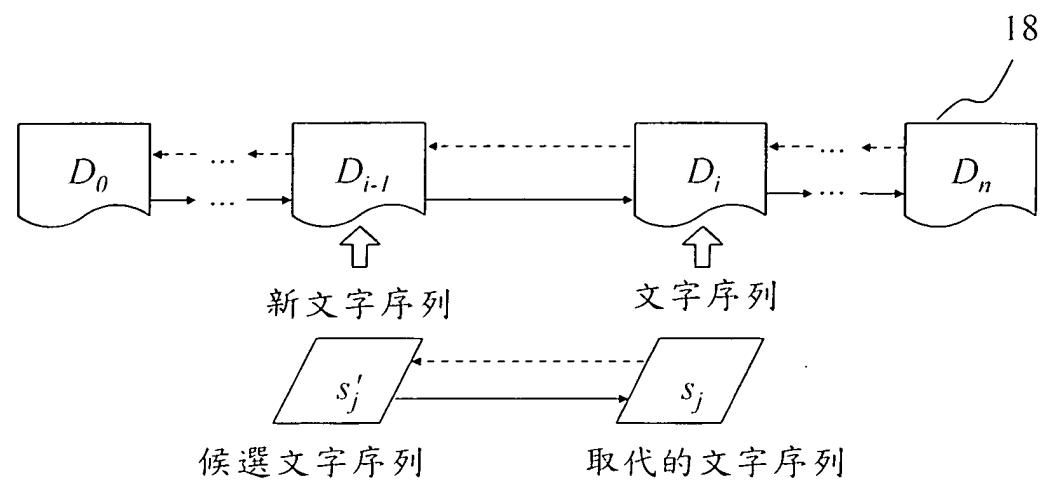
第1圖



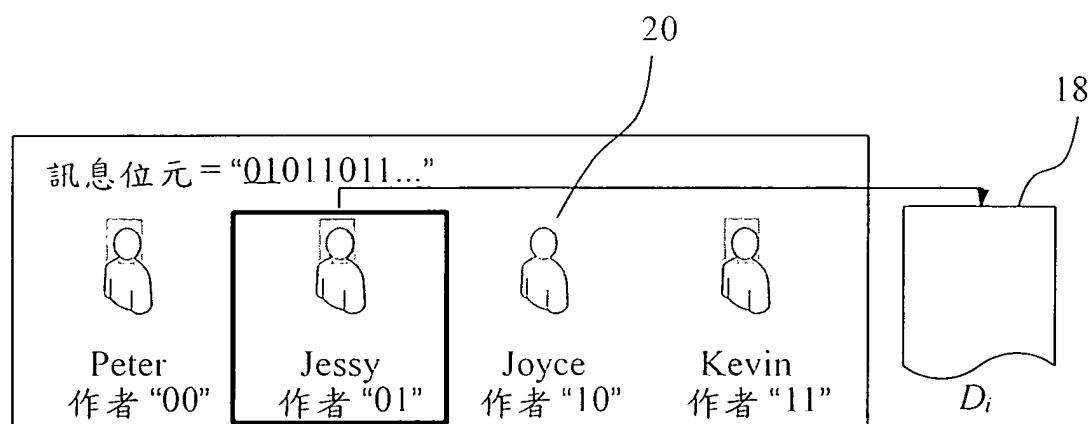
第2圖



第3圖



第4圖



第5圖

12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35

A new tool, called signal-rich-art image, for automatic identification and data-capture applications is proposed, which is created from an artistic target image for use as a carrier of a given message. The created image is visually similar to the target image, achieving the effect of so-called signal-rich-art. With its function similar to those of barcodes or QR codes, such a type of image is produced by fragmenting the composing characters of the message and injecting them into the target image by a novel image-block luminance modulation scheme. Skillful techniques are also proposed for message extraction from a mobile phone-captured version of the signal-rich-art image printed on paper or displayed on a screen. Good experimental results show the feasibility of the proposed method.

第6A圖

- [\(cur | prev\)](#)  15:40, 13 May 2013 Natalie (Talk) [Edit](#)
 - [\(cur | prev\)](#)  12:49, 13 May 2013 David (Talk) [Edit](#)
 - [\(cur | prev\)](#)  10:08, 13 May 2013 Abigail (Talk) [Edit](#)
 - [\(cur | prev\)](#)  08:24, 13 May 2013 Mason (Talk) [Edit](#)
 - [\(cur | prev\)](#)  05:48, 13 May 2013 Samantha (Talk) [Edit](#)

第6B圖

A new tool, called signal-rich-art image, for automatic identification and data capture applications is proposed, which is created from an artistic target image for use as a carrier of a given message. The created image is visually similar to the target image, achieving the effect of so-called signal rich art. With its function similar to those of barcodes or QR codes, such a type of image is produced by fragmenting the composing characters of the message and injecting them into the target image by a novel image-block luminance modulation scheme. Skillful techniques are also proposed for message extraction from a mobile phone-captured version of the signal-rich-art image printed on paper or displayed on a screen. Good experimental results show the feasibility of the proposed method. Signal rich art, as defined by Davis [1], is the art that communicates its identity to context-aware devices. A type of image of this nature, called signal-rich-art image, is proposed in this paper. The image may be printed as a hardcopy for use of any purpose, which is then "re-imaged" by a mobile-phone camera and "understood" by some automatic

第6C圖

A new tool, called signal-rich-art image, for automatic identification and information capture applications is proposed, which is created from an artistic target image for use as a carrier of a given message. The created image is visually similar to the target image, achieving the effect of so-called signal poor art. With its function similar to those of barcodes or QR codes, such a type of image is produced by fragmenting the composing characters of the message and injecting them into the target image by a novel image-block luminance modulation scheme. Skillful techniques are also proposed for message extraction from a mobile phone-captured version of the signal-rich-art image printed on paper or displayed on a screen. Good experimental results show the feasibility of the proposed method.

第6D圖

A new tool, called signal-rich-art image, for automatic identification and data capture applications is proposed, which is created from an artistic target image for use as a carrier of a given message. The created image is visually similar to the target image, achieving the effect of so-called signal rich art. With its function similar to those of barcodes or QR codes, such a type of image is produced by fragmenting the composing characters of the message and injecting them into the target image by a novel image-block luminance modulation scheme. Skillful techniques are also proposed for message extraction from a mobile phone-captured version of the signal-rich-art image printed on paper or displayed on a screen. Good experimental results show the feasibility of the proposed method.

第6E圖

Art is long, life is short

第6F圖

瓊沃樂頌抱「豐徹」姬留揮鑑「歸統」娘慈。對。混。鑑。龍。獸。道。翌。佳。始。

第6G圖