



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201135663 A1

(43)公開日：中華民國 100 (2011) 年 10 月 16 日

(21)申請案號：099111410

(22)申請日：中華民國 99 (2010) 年 04 月 13 日

(51)Int. Cl. : **G06T1/00 (2006.01)**

(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：李哲瑋 LEE, CHE WEI (TW)；蔡文祥 TSAI, WEN HSIANG (TW)

(74)代理人：林火泉

申請實體審查：有 申請專利範圍項數：6 項 圖式數：5 共 18 頁

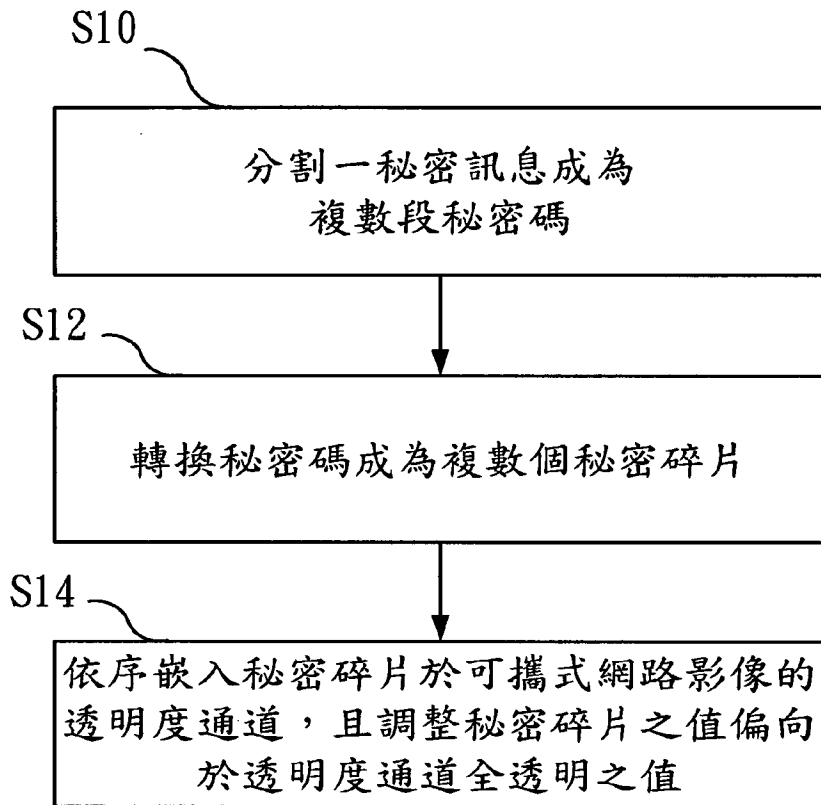
(54)名稱

可攜式網路影像嵌入秘密訊息之方法

A COVERT COMMUNICATION METHOD VIA PNG IMAGES BASED ON THE INFORMATION SHARING TECHNIQUE

(57)摘要

本發明係揭露一種可攜式網路影像嵌入秘密訊息之方法，其係將秘密訊息轉換成秘密碎片後，嵌入於可攜式網路影像(PNG)之透明度通道，並在透明度通道上藉由數值映像(mapping)調整透明度，使得藏密後的可攜式網路影像具高透明度，不致被察覺有異。並且秘密訊息的嵌入不影響可攜式網路影像之紅綠藍通道數值，使得藏有秘密的可攜式網路影像外觀上與原圖並無差異，因而具掩護秘密訊息的效果，而達到秘密傳輸的目的。



發明專利說明書

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※ 申請案號： 99111410

※ 申請日： 99. 4. 13

※IPC 分類：

G06T 1/00

(2006.01)

一、發明名稱：(中文/英文)

可攜式網路影像嵌入秘密訊息之方法 / A covert communication method via PNG images based on the information sharing technique

二、中文發明摘要：

本發明係揭露一種可攜式網路影像嵌入秘密訊息之方法，其係將秘密訊息轉換成秘密碎片後，嵌入於可攜式網路影像(PNG)之透明度通道，並在透明度通道上藉由數值映像(mapping)調整透明度，使得藏密後的可攜式網路影像具高透明度，不致被察覺有異。並且秘密訊息的嵌入不影響可攜式網路影像之紅綠藍通道數值，使得藏有秘密的可攜式網路影像外觀上與原圖並無差異，因而具掩護秘密訊息的效果，而達到秘密傳輸的目的。

三、英文發明摘要：

A covert communication method via PNG images based on the information sharing technique is proposed. In the method, a secret message is transformed into secret shares which are then embedded into the alpha channel of a cover image of the PNG format. By mapping the computed share values of the alpha channel into suitable ranges to yield a nearly uniformly and transparent stego-image. The R, G, and B channels of the stego-image are untouched in the process of message embedding so that the original appearance revealed by the color information of these three channels is kept, achieving the desired effect of steganography for covert communication.

四、指定代表圖：

(一)本案指定代表圖為：第(二)圖。

(二)本代表圖之元件符號簡單說明：

無。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種影像處理技術，特別是關於一種應用於可攜式網路影像(PNG)藏密技術之可攜式網路影像嵌入秘密訊息之方法。

【先前技術】

現今網際網路發達，各種通訊傳輸與網際網路密不可分。使用者可將文字、聲音、影像及圖片等各種型式的檔案或訊息經由網路傳送至另一端使用者。

然而，透過網路傳輸訊息的安全性不佳，因此，為了將具有機密性的秘密訊息傳送，往往於傳送前將秘密訊息優先進行加密，而接收端進行解密後方可得到原始訊息。雖然加密的方式可提升秘密訊息傳送的安全度，但因加密後的密文呈隨機樣貌，易被識出而予以損毀，遂有另一方式係將秘密訊息隱藏於檔案中，藉由發送檔案將夾帶其中的秘密訊息進行傳送，接收端需將檔案完全解碼方得到隱藏於檔案中之秘密訊息。相較於加密的方式，加密的秘密訊息有較高的機會遭察覺包含有秘密訊息，而透過隱藏於檔案的方式將可透過檔案做為掩護，可大幅避免被察覺的可能。

有鑑於此，本發明係針對上述秘密訊息嵌入並隱藏於檔案的方式做進一步的研究，同時結合影像處理技術與編碼技術，提出一種可攜式網路影像嵌入秘密訊息之方法。

【發明內容】

本發明之主要目的係在提供一種可攜式網路影像嵌入秘密訊息之方法，其係將秘密訊息轉換為秘密碎片後嵌入於可攜式網路影像，使秘密訊息隱藏於可攜式網路影像之中，並隨可攜式網路影像傳送。

本發明之另一目的係在提供一種可攜式網路影像嵌入秘密訊息之方法，其係嵌入秘密訊息於可攜式網路影像而不影響可攜式網路影像的影像內容，可攜式網路影像之紅綠藍色彩通道之數值不會因嵌入秘密訊息而失真。

本發明之又一目的係在提供一種可攜式網路影像嵌入秘密訊息之方法，其係將能簡易還原嵌入可攜式網路影像之秘密訊息，具良好解碼效率。

為達到上述之目的，本發明提出之可攜式網路影像嵌入秘密訊息之方法，其係將一秘密訊息分割成為複數段秘密碼。依序取出秘密碼組成聯立方程式，秘密碼係為聯立方程組之每一方程式的係數，且每一方程式包含與一初始參考值相除取餘數之數學運算。每一方程式將代入不同的變數值以產生對應的數值，該數值即為秘密碎片。如此將轉換秘密碼成為欲嵌入可攜式網路影像之透明通道的複數個秘密碎片。最後，放置秘密碎片於可攜式網路影像之透明度通道，以嵌入秘密訊息於可攜式網路影像。此透明度通道之透明度係介於十進位數 0 至十進位數 255 之間，分別表示白色不透明至全透明。

底下藉由具體實施例配合所附的圖式及數學式詳加說明，當更容易瞭解本發明之目的、技術內容、特點及其所達成之功效。

【實施方式】

本發明提出一種可攜式網路影像嵌入秘密訊息之方法，係嵌入秘密訊息至一可攜式網路影像(PNG)，使秘密訊息得以隱藏於可攜式網路影像隨之傳送，以達到秘密傳輸之目的，並且具備高安全度;嵌有秘密訊息之可攜式網路影像能夠維持高視覺品質，其紅綠藍色彩通道不失真。底下將以較佳

實施例詳述本發明之技術特徵。

第一圖為本發明可攜式網路影像之格式分解示意圖，如圖所示，一可攜式網路影像 10 係包含紅(R)通道 12、綠(G)通道 14、藍(B)通道 16 及透明度(α)通道 18 四個通道平面。紅(R)通道 12、綠(G)通道 14、藍(B)通道 16 係分別包含紅(r)綠(g)藍(b)之色彩通道數值。色彩通道數值係為介於十進位 0 到 255 之間。透明度(α)通道 18 之透明度亦以介於 0 到 255 之間的十進位數表示，0 表示為白色不透明，255 則表示為全透明。底下將對嵌入秘密訊息的步驟做進一步詳細說明。

如第二圖所示為本發明嵌入秘密訊息之流程圖，請同時參閱第三圖之嵌入秘密碎片至透明度通道之示意圖。如圖所示，首先，如步驟 S10，分割一秘密訊息成為複數段秘密碼。秘密訊息係將優先轉換為一二進位串流，且依序每次於二進位串流中取出固定數目的位元成為位元組，並將取出的位元組轉換為十進位數字，即成為秘密碼。例如，一秘密訊息被轉換為 100011010111 之二進位串流，且由左而右依序每次取三個位元成為一個位元組，分別為 100,011,010 與 111，接著將它們轉換為十進位數字，即 4(100), 3(011), 2(010), 與 7(111)。如是，二進位串流將被分割成 {4, 3, 2, 7} 這四個秘密碼。

之後，如步驟 S12，轉換秘密碼成為複數個秘密碎片。其轉換如下列公式(1)所示：

$$\begin{cases} q_1 = F(x_1) = (m_0 + m_1x_1 + m_2x_1^2 + m_3x_1^3)_{\text{mod } p} \\ q_2 = F(x_2) = (m_0 + m_1x_2 + m_2x_2^2 + m_3x_2^3)_{\text{mod } p} \\ q_3 = F(x_3) = (m_0 + m_1x_3 + m_2x_3^2 + m_3x_3^3)_{\text{mod } p} \\ q_4 = F(x_4) = (m_0 + m_1x_4 + m_2x_4^2 + m_3x_4^3)_{\text{mod } p} \end{cases} \quad (1)$$

其中，秘密碼為係數 m_0 、 m_1 、 m_2 與 m_3 。 q_1 、 q_2 、 q_3 與 q_4 即為欲藏入在可攜式網路影像之透明度(α)通道18內的秘密碎片。而 x_1 、 x_2 、 x_3 與 x_4 分別代表四個變數，此變數之值可由使用者自訂，惟其值須小於 p 。公式(1)為一元三次聯立方程式，其中每一方程式係包含除以一初始參考數值 p 以取餘數的運算。初始參考數值 p 係必為一質數，且由於透明度(α)通道18最小值為0，最大值為255，故其值須介於0到255之間，並且為秘密碼之係數 m_0 、 m_1 、 m_2 與 m_3 須小於初始參考數值 p 。

承上例說明，秘密訊息100011010111以每三位元分割並轉換成{4, 3, 2, 7}這四個秘密碼，故 $m_0 = 4$ ， $m_1 = 3$ ， $m_2 = 2$ ，及 $m_3 = 7$ 。而初始參考數值 p 值須為大於 m_0 ， m_1 ， m_2 與 m_3 之值的質數，因此，初始參考數值 p 應為一大於7且最接近7之質數，故初始參考數值 p 將為11。假設 $x_1 = 1$ ， $x_2 = 2$ ， $x_3 = 3$ ， $x_4 = 4$ ，代入公式(1)中計算後，可得秘密碎片 $q_1 = 5$ ， $q_2 = 8$ ， $q_3 = 0$ ， $q_4 = 1$ 。

在產生秘密碎片後，如步驟S14，將秘密碎片依序嵌入至可攜式網路影像的透明度通道(α)18，並且依據調整秘密碎片之值偏向於透明度通道(α)18全透明之值(數值255)，此步驟稱之為數值映像(mapping)。

續承上例說明，初始參考數值 p 之值為11，則秘密碎片 $\{q_1, q_2, q_3, q_4\} = \{5, 8, 0, 1\}$ 係為介於0~10偏向為白色不透明之值(數值0)，為了使秘密碎片之值偏向為全透明之值，將嵌於透明度通道(α)18的秘密碎片 $\{q_1, q_2, q_3, q_4\}$ 統一加上數值245，則秘密碎片 $\{q_1, q_2, q_3, q_4\} = \{250, 253, 245, 246\}$ 。由此可知，即使秘密碎片之值為10，再加上245後，亦不超過透明度通道(α)18之最大值(數值255)。此代表秘密碎片經過數值映像後，全體係偏向全透明之數值(數值255)，且嵌於透明度通道(α)18的所有秘密碎片之值會介於245到255之間。

以上為嵌入秘密訊息至可攜式網路影像10的步驟說明。此外，嵌入之秘密訊息將可經由計算還原，如下列公式(2)所示：

$$F(x) = \left[F(x_1) \frac{(x-x_2)(x-x_3)\dots(x-x_k)}{(x_1-x_2)(x_1-x_3)\dots(x_1-x_k)} + F(x_2) \frac{(x-x_1)(x-x_3)\dots(x-x_k)}{(x_2-x_1)(x_2-x_3)\dots(x_2-x_k)} \right. \\ \left. + \dots + F(x_k) \frac{(x-x_1)(x-x_2)\dots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\dots(x_k-x_{k-1})} \right]_{\text{mod } p} \quad (2)$$

其中，當 $k=4$ 時，公式(2)中的 $F(x_1)$ 到 $F(x_k)$ 對應於公式(1)中的 $F(x_1)$ 到 $F(x_4)$ ； x_1 、 x_2 、 x_3 ... x_k 對應於公式(1)中的使用者自訂變數 x_1 到 x_4 。解密嵌入於可攜式網路影像 10 之秘密訊息的步驟，首先，將秘密碎片 $\{q_1, q_2, q_3, q_4\}$ 分別減去 245，以得到未經過數值映像之秘密碎片 $\{q_1, q_2, q_3, q_4\} = \{5, 8, 0, 1\}$ 。由於解密者為特定、可預期的通訊對象，所以 x_1 到 x_4 的值是可知的，遂將這四片秘密碎片與 x_1 到 x_4 的值代入公式(2)運算可得 $F(x) = 4 + 3x + 2x^2 + 7x^3$ 。各項係數即為秘密碼 m_0 、 m_1 、 m_2 與 m_3 ，分別是 $m_0 = 4$ ， $m_1 = 3$ ， $m_2 = 2$ ，及 $m_3 = 7$ 。再將秘密碼進行十進制轉二進制的轉換 $m_0 = (4)_{10} = (100)_2$ ， $m_1 = (3)_{10} = (011)_2$ ， $m_2 = (2)_{10} = (010)_2$ ， $m_3 = (7)_{10} = (111)_2$ ，並依序串接它們，便可擷取出嵌入於可攜式網路影像 10 的秘密訊息(100011010111)。

經由上述實施例說明可知本發明係為將秘密訊息轉化為秘密碎片，經由數值映像後嵌入於可攜式網路影像10的透明度通道(α)18。並且可藉由反向運算解密嵌入可攜式網路影像10之秘密訊息。此外，本發明將定義出可嵌入的資料容量之通式 tS ，其中 t 代表分割二進位串流的位元數量； S 代表可攜式網路影像10的大小。例如， 512×512 大小的可攜式網路影像10，現有一秘密訊息轉換而成的二進位串流，以每三位元為一位元組做分割時，表示 $t=3$ ，並且最大秘密資訊藏入量為 $tS = 3S = 3 \times 512 \times 512$ ；同理，若以

每四位元為一位元組做分割時， $t=4$ ，代表最大秘密資訊藏入量為 $tS = 4S$ 。藏入量越大，可攜式網路影像10因透明度不均勻造成影像品質的下降就越大。需依據秘密訊息之數量的多寡選擇合適之 t 值。

第四(a)圖與第四(b)圖分別為可攜式網路影像嵌入秘密訊息前後之示意圖，並請同時參閱表(1)。可攜式網路影像10嵌入秘密訊息前與嵌入秘密訊息後之外觀並未有所不同，如此可攜式網路影像10將可提供秘密訊息傳送時良好的偽裝與遮蔽。且表(1)係列出 t 從1到7，可攜式網路影像10對應的資訊藏入量及透明通道峰值訊雜比。請同時參閱第五(a)圖至第五(g)圖所示，由表(1)可知，隨著分割二進位串流的位元數量 t 增加，最大秘密資訊藏入量隨之增加，然而，透明度通道(α)18不均勻亦增加，將使可攜式網路影像10影像品質下降。從第五(a)圖至第五(g)圖可看出 t 由1到7逐漸增加時，可攜式網路影像10的影像品質將隨之下降。

表(1)

t 值	可攜式網路影像	
	資訊藏入量 (bits)	透明度通道(α)峰值訊雜(PSNR) (dB)
$t = 1$	262144	45.44
$t = 2$	524,288	39.77
$t = 3$	786,432	32.69
$t = 4$	1,048,576	28.68
$t = 5$	1,310,720	21.72
$t = 6$	1,572,864	16.74

$t=7$	1,835,008	10.61
-------	-----------	-------

以上所述之實施例僅係為說明本發明之技術思想及特點，其目的在使熟習此項技藝之人士能夠瞭解本發明之內容並據以實施，當不能以之限定本發明之專利範圍，即大凡依本發明所揭示之精神所作之均等變化或修飾，仍應涵蓋在本發明之專利範圍內。

【圖式簡單說明】

第一圖為本發明可攜式網路影像之格式分解示意圖。

第二圖為本發明嵌入秘密訊息之流程圖。

第三圖為本發明嵌入秘密碎片至透明度通道之示意圖。

第四(a)圖為本發明可攜式網路影像嵌入秘密訊息前之示意圖。

第四(b)圖為本發明可攜式網路影像嵌入秘密訊息後之示意圖。

第五(a)圖至第五(g)圖為本發明分割二進位串流位元數量 t 嵌入秘密訊息於可攜式網路影像之示意圖。

【主要元件符號說明】

- 10 可攜式網路影像
- 12 紅(R)通道
- 14 綠(G)通道
- 16 藍(B)通道
- 18 透明度通道(α)

七、申請專利範圍：

1、一種可攜式網路影像嵌入秘密訊息之方法，其包含有下列步驟：

分割一秘密訊息成為複數段秘密碼；

轉換該秘密碼成為複數個秘密碎片；以及

依序嵌入該秘密碎片至一可攜式網路影像之一透明度通道，並調整每一

該秘密碎片之值偏向於該透明度通道之全透明之值。

2、如申請專利範圍第 1 項所述之可攜式網路影像嵌入秘密訊息之方法，其

中該透明度通道之透明度係為介於十進位數 0 至 255 之間，且該十進位

數 0 為該透明度通道呈現白色不透明之值，該十進位數 255 為該透明度

通道呈現全透明之值。

3、如申請專利範圍第 1 項所述之可攜式網路影像嵌入秘密訊息之方法，其

中該秘密碎片係為由秘密碼組成的聯立方程式表示。

4、如申請專利範圍第 3 項所述之可攜式網路影像嵌入秘密訊息之方法，其

中該聯立方程式之每一方程式係包含與一初始參考數值相除取餘數的

運算。

5、如申請專利範圍第 4 項所述之可攜式網路影像嵌入秘密訊息之方法，其

中該初始參考數值係為介於該透明度通道之十進位數質數。

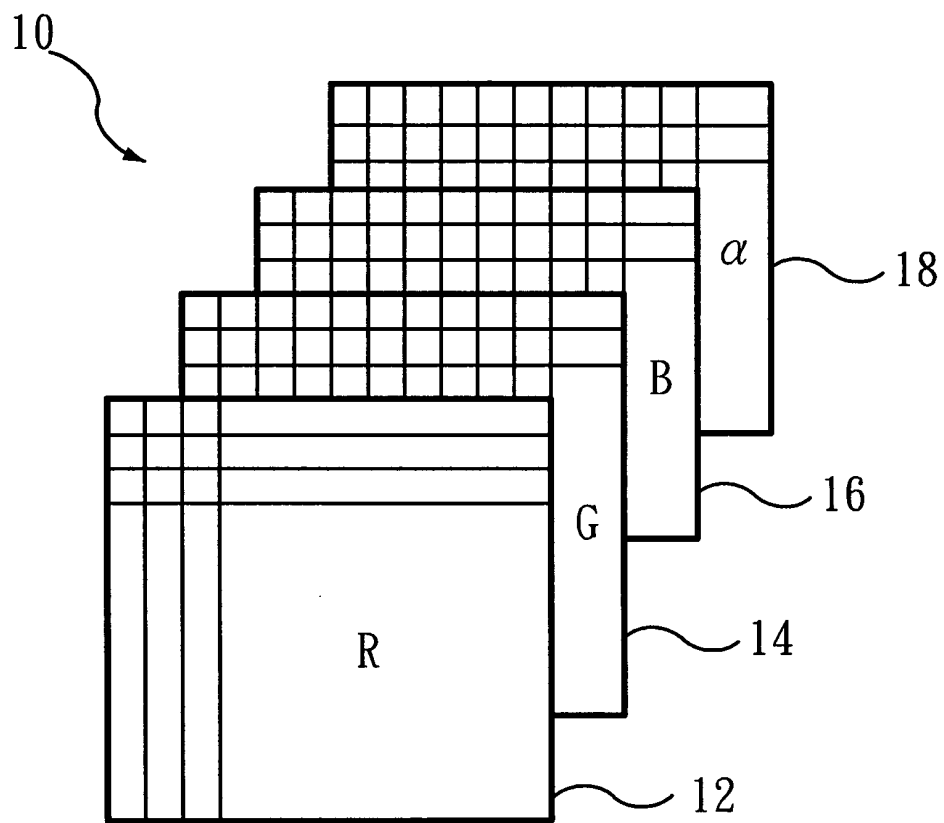
6、如申請專利範圍第 1 項所述之可攜式網路影像嵌入秘密訊息之方法，其

中於依序嵌入該秘密碎片至該可攜式網路影像之該透明度通道的步驟

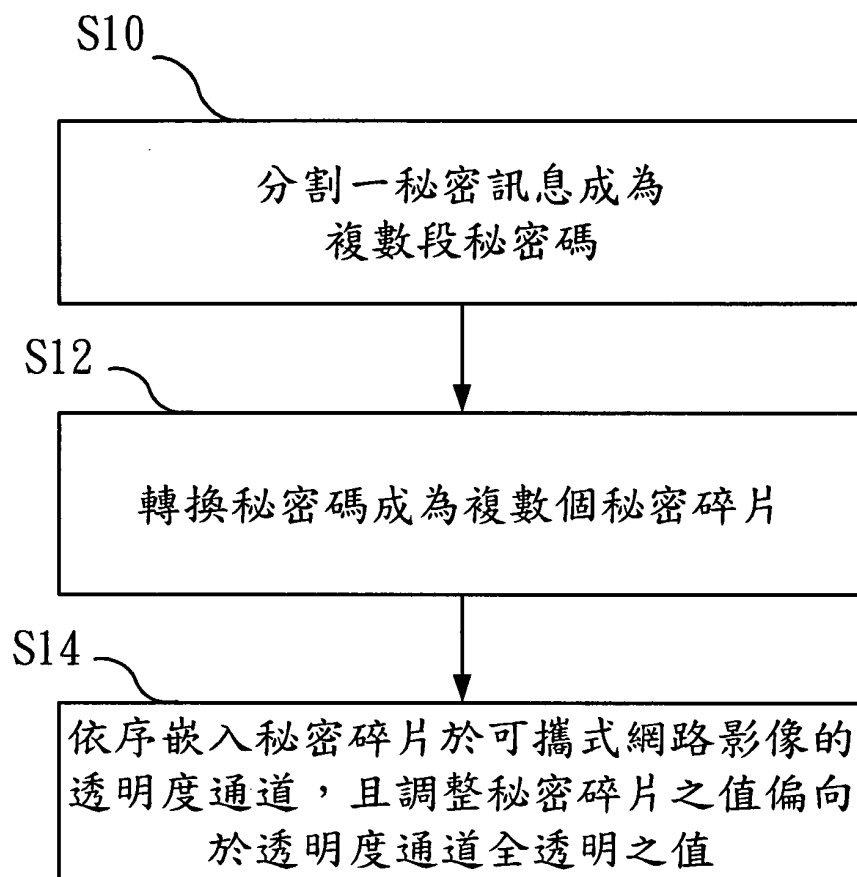
中，將該秘密碎片之值同加一數值，以調整該秘密碎片之值皆偏向於該

透明度通道之全透明之值。

八、圖式：



第一圖



第二圖

Q1	Q2	Q3	Q4
⋮				α

18

第三圖

10



第四(a)圖

10



第四(b)圖

10



第五(a)圖

10



第五(b)圖

10



第五(c)圖

10



第五(d)圖

10



第五(e)圖

10



第五(f)圖

10



第五(g)圖