

發明專利說明書

580656

(填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫)

※ 申請案號： 91136899 ※IPC分類： G09C 5/00

※ 申請日期： 91.12.20

壹、發明名稱

(中文) 數位影像版權之保護與驗證方法

(英文) _____

貳、發明人 (共 3 人)

發明人 1 (如發明人超過一人，請填說明書發明人續頁)

姓名：(中文) 孫宏民

(英文) _____

住居所地址：(中文) 台北市南京東路二段一一六號五樓

(英文) _____

國籍：(中文) 中華民國 (英文) _____

參、申請人 (共 1 人)

申請人 1 (如發明人超過一人，請填說明書申請人續頁)

姓名或名稱：(中文) 財團法人資訊工業策進會

(英文) _____

住居所或營業所地址：(中文) 台北市和平東路二段一〇六號十一樓

(英文) _____

國籍：(中文) 中華民國 (英文) _____

代表人：(中文) 黃河明

(英文) _____

☐ 續發明人或申請人續頁 (發明人或申請人欄位不敷使用時，請註記並使用續頁)

003258

發明人 2姓名：(中文) 陳孟彰
(英文)住居所地址：(中文) 台北市南京東路二段一一六號五樓
(英文)

國籍：(中文) 中華民國 (英文)

發明人 3姓名：(中文) 林宸堂
(英文)住居所地址：(中文) 台北市南京東路二段一一六號五樓
(英文)

國籍：(中文) (英文)

發明人 4姓名：(中文)
(英文)住居所地址：(中文)
(英文)

國籍：(中文) (英文)

發明人 5姓名：(中文)
(英文)住居所地址：(中文)
(英文)

國籍：(中文) (英文)

發明人 6姓名：(中文)
(英文)住居所地址：(中文)
(英文)

國籍：(中文) (英文)

捌、聲明事項

☐ 本案係符合專利法第二十條第一項第一款但書或第二款但書規定之期間，其日期為：_____

☐ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號 順序註記】

1. 無_____

2. _____

3. _____

☐ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號 順序註記】

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號 順序註記】

1. _____

2. _____

3. _____

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

1. _____

2. _____

3. _____

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

1. _____

2. _____

3. _____

☐ 熟習該項技術者易於獲得，不須寄存。

008262

玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

一、發明所屬之技術領域

本發明係關於一種數位影像版權之保護與驗證方法，尤指一種植基於數位浮水印與公證者之數位影像版權驗證之方法。

二、先前技術

按，隨著資訊科技發展的日新月異、及網際網路的普及化，目前有越來越多具有商業價值的多媒體資訊在網路環境上傳播，例如圖片(graph)、影像(image)、音樂(audio)、及影片(video)等，使用者可藉由下達簡單的指令而在網路中輕易進行下載。然而，習知卻有部分使用者在下載上述多媒體資訊後，將其加以竄改後宣稱是自己的資料，以進行圖利自己的商業行為，此舉嚴重侵犯了原始資料所有權人的智慧財產權，因此，在網路上傳播的資料必須具備保護智慧財產權的措施，才能讓資料所有權人得到完善的保護。

為了解決有價多媒體資訊遭竊用及竄改的問題，習知係針對密碼學(cryptography)、資料隱藏(data hiding)、數位影像版權保護(image copyright protection)、及數位浮水印(digital watermarking)技術加以研究，以期能找出有效的保護措施。

於密碼技術中，係包括有加密、數位簽章(digital signature)、及時戳簽章(timestamp)等技術，可用以提供智慧財產權安全上的保護，但卻不適合用來處理多媒體

資料，因為多媒體資料通常檔案大小都比文字大很多，且用一般的密碼技術需要大量的時間來加密或簽名；此外，一般的加密和簽名方法不允許失真的情況發生，但多媒體資料只要失真程度在可接受程度下，皆可允許失真情形發生。故習知最廣泛採用的方法係為使用數位浮水印技術及數位影像版權保護技術。

數位浮水印技術則指將代表合法擁有者的圖騰(例如註冊商標、營利事業統一編號、個人肖像等)加入被保護的有價媒體中，用以表示及證明此媒體的合法擁有權之歸屬。且在嵌入浮水印後的媒體在經過一些常見的數位訊號處理和破壞之後，其品質在可接受的範圍之內，則浮水印仍然可被顯示出來，因此能夠證明此媒體的版權歸屬，以發現非法使用者的盜用或仿冒行為。

習知數位浮水印技術須兼具下列特性：透明性(transparency)：以使加入浮水印的媒體與原始媒體間不具有明顯的改變，亦即不讓人察覺媒體中有浮水印的存在；強健性(robustness)：當加入浮水印的媒體在經過數位訊號處理(例如模糊處理、清晰處理、失真壓縮、加入雜點、影像切割、放大縮小、或旋轉處理等)後，品質在可接受範圍內的浮水印仍可被顯示出來；清晰性(unambiguity)：數位浮水印技術在各種可能的攻擊狀況下所取出的浮水印必須能夠明確辨識影像的所有權，而不破壞到影像本身的商業價值；安全性(security)：藏入數位浮水印的演算法係為一公開的演算法；在取出浮水印的過程中不要原始資料(blindness)：通常數位媒體需要

極大的儲存空間，為了節省空間，因此在取出浮水印時，不必藉由原始媒體之輔助即可完成，也就是不用為了取出浮水印而需同時儲存原始媒體；以及，實用性：即浮水印演算法需具有較佳執行效率，以達到較高的實用性。

然而，於習知之數位浮水印技術中，若遭有心人刻意針對數位浮水印演算法加以攻擊，進行反向操作就將能除去其中所藏入之數位浮水印；此外，若在同一份媒體中被藏入複數個浮水印，則難以辨識真正合法的擁有者；又，習知技術所佔用之資料量較大，亦使處理成本提高。因此習知亦提出另一作法用以將媒體中比較重要的資訊作為特徵值，並使用一專門儲存影像特徵值之資料庫來比對及過濾媒體中之特徵資料，以檢查此媒體是否已註冊，然而，此舉僅能辨識出特徵資料是否有註冊過，卻無法像數位浮水印技術一樣可用肉眼辨識取出的浮水印，故同樣難以證明真正的智慧財產權所有人。由此可知，習知數位影像保護技術仍存在有諸多缺失而予以改進之必要。

三、發明內容

本發明之主要目的係在提供一種數位影像版權之保護與驗證方法，俾能確保被保護媒體的強健性，以承受各式各樣的攻擊狀況。

本發明之另一目的係在提供一種數位影像版權之保護與驗證方法，俾使被保護媒體之品質和原始媒體之品質相同。

本發明之再一目的係在提供一種數位影像版權之保護與驗證方法，係藉由向公正第三者註冊以產生一具有時戳簽章之秘密金鑰，以根據時戳簽章來判斷被保護媒體之合法性。

為達成上述之目的，本發明所提出之數位影像版權之保護與驗證方法主要包括第一程序及第二程序。第一程序係用以產生一秘密金鑰，其首先擷取一原始影像及一浮水印影像，其中，原始影像為一 O_H 圖素乘以 O_W 圖素之影像，浮水印影像為一 W_H 圖素乘以 W_W 圖素之影像，且 O_H 為原始影像之高度， O_W 為原始影像之寬度， W_H 為浮水印影像之高度， W_W 為浮水印影像之寬度；接著將原始影像切割為 $W_H \times W_W$ 個區塊；並使用離散餘弦正轉換技術以將每一區塊之數值轉換為一頻率域區塊係數；再以亂數打亂頻率域區塊係數之順序；之後，擷取出上述打亂後之頻率域區塊係數之離散餘弦值，以由 $W_H \times W_W$ 個離散餘弦值來形成一離散餘弦值數列；且將離散餘弦值數列排序後根據一預設之門檻值來產生一暫時金鑰；最後將暫時金鑰併同浮水印影像進行互斥運算以產生一秘密金鑰，以將原始影像轉換為一嵌入有秘密金鑰之保護影像。

第二程序則用以自保護影像中萃取出浮水印影像，其首先擷取一保護影像；並將保護影像切割為 $W_H \times W_W$ 個區塊；再使用離散餘弦正轉換技術，將每一區塊之數值轉換為一頻率域區塊係數；接著，以亂數打亂頻率域區塊係數之順序；且擷取出上述打亂後之頻率域區塊係數之離散餘弦值，以由 $W_H \times W_W$ 個離散餘弦值來形成一形成

一離散餘弦值數列；之後，排序離散餘弦值數列；並自秘密金鑰中擷取出一門檻值，再把扣除門檻值後之秘密金鑰儲存為一第一暫時金鑰；再根據排序後之離散餘弦值數列及門檻值以產生一第二暫時金鑰；最後將第一暫時金鑰及第二暫時金鑰進行互斥運算以萃取出一待測浮水印影像。

四、實施方式

為能讓 貴審查委員能更瞭解本發明之技術內容，特舉一較佳具體實施例說明如下。

本實施例係使用離散餘弦轉換 (Discrete Cosine Transform, DCT) 技術中之離散餘弦正轉換 (Forward DCT) 方法來取得每一欲保護影像的離散餘弦值 (Discrete Cosine, DC) 當作特徵值，再以此影像的特徵值和浮水印內容相互結合來產生一把秘密金鑰，因此影像的合法擁有者可以持有這把秘密金鑰來萃取浮水印，並能將秘密金鑰向一公正第三者註冊，因而產生一具有時戳簽章的金鑰，以透過這把秘密金鑰和具有時戳簽章的金鑰來證明影像版權的所有權。

請參閱圖 1 用以在原始影像中產生秘密金鑰之流程。於本實施例中，原始影像 O 係為由一張每圖素具有 β 位元之灰階影像所構成，而浮水印影像 W 則如圖 2 所示，其係為一二元影像，且原始影像 O 及浮水印影像 W 之定義分別為：

$$O = \{o_{i,j} \mid 0 \leq o_{i,j} \leq 2^{\beta} - 1\},$$

其中，每一 $o_{i,j}$ 為一圖素， $0 \leq i \leq O_H - 1$ ， $0 \leq j \leq O_W - 1$ ，且 O_H 為原始影像 O 的高， O_W 為原始影像 O 的寬；

$$W = \{w_{i,j} \mid w_{i,j} \in \{0,1\}\},$$

其中，每一 $w_{i,j}$ 為一圖素， $0 \leq i \leq W_H - 1$ ， $0 \leq j \leq W_W - 1$ ，且 W_H 為浮水印影像 W 的高， W_W 為浮水印影像 W 的寬。

因此在擷取原始影像 O 及浮水印影像 W 後 (步驟 S101)，將原始影像 O 根據浮水印影像 W 的長寬比例切割成 $W_H \times W_W$ 個等比例區塊 $B_{m,n}$ (步驟 S102)，且每一區塊大小為 $\frac{O_H}{W_H} \times \frac{O_W}{W_W}$ ，而上述之等比例區塊 $B_{m,n}$ 則記錄為如下所示之行列式：

$$B_{m,n} = \begin{bmatrix} o_{i,j} & o_{i,j+1} & \cdots & o_{i,j+w-1} \\ o_{i+1,j} & o_{i+1,j+1} & \cdots & o_{i+1,j+w-1} \\ \cdots & \cdots & \cdots & \cdots \\ o_{i+h-1,j} & \cdots & \cdots & o_{i+h-1,j+w-1} \end{bmatrix},$$

當中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ 。

需注意的是，本實施例較佳係將原始影像 O 切割為等比例區塊，當然亦可切割為不等比例之區塊，只要所切割出區塊之數量等於 $W_H \times W_W$ 個即可。

再來，將 $W_H \times W_W$ 個切割後的區塊 $B_{m,n}$ ，從空間域的數位資料透過離散餘弦正轉換 (FDCT) 技術以轉換為頻率域的係數 $C_{m,n}$ (步驟 S103)，藉以取得每一等比例區塊 $B_{m,n}$ 之特徵值，其中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ ；接著使用亂數種子數來擾亂頻率域區塊的排列順序 (步驟 S104)；並取出經過打亂後的每個頻率域區塊係數 $C'_{m,n}$ 的離散餘弦 (DC) 值 (步驟 S105)，總計將可取得 $W_H \times W_W$ 個離散餘弦

值，因此形成一離散餘弦值數列 $D_{m,n}$ ；之後將 $W_H \times W_W$ 個離散餘弦值數列 $D_{m,n}$ 由大到小排序成為排序後之離散餘弦值數列 $DS_{m,n}$ (步驟S106)。

接下來，將根據排序後之離散餘弦值數列 $DS_{m,n}$ 及一預設之門檻值(以下簡稱TH)來產生如圖3所示之暫時金鑰T(步驟S107)：

$$T = \{t_{m,n} \mid t_{m,n} \in \{0,1\}\},$$

其中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ ，且當 $DS_{m,n}$ 之前($TH \times$ 區塊總數)之數在 $D_{m,n}$ 之相對區塊上設定為1時， $t_{m,n}$ 為1；當 $DS_{m,n}$ 之後(區塊總數－($TH \times$ 區塊總數))之數在該 $D_{m,n}$ 之相對區塊上設定為0時， $t_{m,n}$ 為0。此外，門檻值TH可由合法使用者自行控制，且可依每一張影像的特性來設定不同門檻值TH，以由門檻值TH來決定暫時金鑰T的0與1的個數，不過為了安全性考量，因此門檻值TH建議不宜設定得太高或太低，較佳係介於0.2至0.8之間。

而在從原始影像O中取得暫時金鑰T後，將可併同暫時金鑰T與浮水印影像W來進行互斥(exclusive-OR)運算，藉以產生如圖4所示之秘密金鑰K(步驟S108)，其中：

$$K = (T \oplus W) \parallel TH。$$

此外，為了宣告原始影像O所產生之時間點，因此必須將秘密金鑰K向一公正第三者註冊，以產生具有時戳簽章的金鑰 K_s (步驟S109)，將可解決誰先加入浮水印影像W的問題，且上述具有時戳簽章的金鑰 K_s 係由公正第三者加以保管。由此可知，本實施例的方法在藏入浮水印影像W時，並不是直接將浮水印影像W嵌入於原始影像O

中，而是另外產生一把秘密金鑰 K ，所以能確保被保護的影像品質將和原始影像 O 一樣好，且更能藉由具有時戳簽章的金鑰 K_s 來證明先後順序以消弭爭議，實為一大進步。

因此，當欲萃取出保護影像中之浮水印影像時，請參閱圖5之流程。在擷取保護影像 S (watermarked image)後(步驟S501)，亦將保護影像 S 根據浮水印影像 W 的長寬比例切割為 $W_H \times W_W$ 個等比例區塊 $B_{m,n}$ (步驟S502)，其中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ ，每一區塊大小為 $\frac{S_H}{W_H} \times \frac{S_W}{W_W}$ ，且

S_H 為保護影像 S 的高， S_W 為保護影像 S 的寬。

接著，圖5之步驟S502至步驟S506的流程皆與圖1之步驟S102至步驟S106的流程相同，故不再贅述，唯在圖5中，標的為保護影像 S ，而在圖1中之標的則為原始影像 O 。

而在步驟S507中，將自原本根據原始影像 O 所計算出之秘密金鑰 K 中擷取出其對應之門檻值 TH ，並將秘密金鑰 K 扣除門檻值 TH 以取得如圖6所示之第一暫時金鑰 $T1$ (步驟S508)；再來，根據排序後之離散餘弦值數列 $DS_{m,n}$ 及一預設之門檻值(以下簡稱 TH)來產生如圖7所示之第二暫時金鑰 $T2$ (步驟S509)：

$$T2 = \{t_{m,n} \mid t_{m,n} \in \{0,1\}\},$$

其中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ ，且當 $DS_{m,n}$ 之前($TH \times$ 區塊總數)之數在 $D_{m,n}$ 之相對區塊上設定為1時， $t_{m,n}$ 為1；當 $DS_{m,n}$ 之後($DS_{m,n} - (TH \times \text{區塊總數})$)之數在 $D_{m,n}$ 之相對區塊上設定為0時， $t_{m,n}$ 為0。

最後，將第一暫時金鑰T1及第二暫時金鑰T2進行互斥運算以萃取出如圖8所示之待測浮水印影像W' (步驟S510)，其計算方式為： $W' = (T1 \oplus T2)$ 。若保護影像S未被破壞過，則W'會等於W；否則兩者之間可能會有些許差異，其係使用位元正確率(bit correct ratio, BCR)法來計算兩者的相似度：

$$BCR = \frac{\sum_{i=1}^{W_H} \sum_{j=1}^{W_W} w(i,j) \oplus w'(i,j)}{W_H \times W_W} \times 100\% ,$$

其中， $w(i,j)$ 為原始浮水印影像W在座標(i,j)之位元值， $w'(i,j)$ 為待測浮水印影像W'在座標(i,j)之位元值。

根據上述之說明，顯示本發明所提出之數位影像版權之保護與驗證方法能在不影響原始影像之品質的前提下，根據原始影像來產生秘密金鑰；並能透過向公正第三者註冊以產生具有時戳簽章的金鑰，藉以比對出較早註冊者為合法使用者，以防杜仿冒等侵權行為；且若攻擊者宣稱他具有合法擁有者影像的版權時，將無法萃取出清晰的攻擊者浮水印，顯示本發明之方法能確保被保護媒體的強健性，以承受各式各樣的攻擊狀況；而且，在萃取出浮水印影像的過程中不需使用到原始資料，且除了合法擁有者之外，他人無法偵測出此影像藏有浮水印，實為一大進步。

上述實施例僅係為了方便說明而舉例而已，本發明所主張之權利範圍自應以申請專利範圍所述為準，而非僅限於上述實施例。

五、圖式簡單說明

- 圖 1 係本發明實施例用以產生秘密金鑰之流程圖。
- 圖 2 係本發明實施例浮水印影像之示意圖。
- 圖 3 係本發明實施例暫時金鑰之示意圖。
- 圖 4 係本發明實施例秘密金鑰之示意圖。
- 圖 5 係本發明實施例用以萃取浮水印影像之流程圖。
- 圖 6 係本發明實施例第一暫時金鑰之示意圖。
- 圖 7 係本發明實施例第二暫時金鑰之示意圖。
- 圖 8 係本發明實施例待測浮水印影像之示意圖。

圖號說明

原始影像 O	浮水印影像 W
暫時金鑰 T	秘密金鑰 K
保護影像 S	第一暫時金鑰 T1
第二暫時金鑰 T2	待測浮水印影像 W'

肆、中文發明摘要

本發明係有關於一種數位影像版權之保護與驗證方法，其係使用離散餘弦轉換技術以取得每一張欲保護影像的離散餘弦值作為特徵值，並以此影像的特徵值和浮水印影像的內容使用互斥運算相互結合，進而產生一把秘密金鑰，合法使用者可持有此秘密金鑰來萃取出保護影像中的浮水印影像，且在將秘密金鑰向公正第三者註冊後，可產生具有時戳簽章的秘密金鑰，以證明此影像之擁有時間順序。本發明係結合產生秘密金鑰之演算法以計算出原始影像之秘密金鑰、及浮水印萃取之演算法以根據秘密金鑰自保護影像中萃取出浮水印影像。

伍、英文發明摘要

006260

陸、(一)、本案指定代表圖爲：第1圖

(二)、本代表圖之元件代表符號簡單說明：

流程圖無元件符號說明。

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

拾、申請專利範圍

1. 一種數位影像版權之保護與驗證方法，主要包括：

第一程序，用以產生一秘密金鑰，其包括下列步驟：

(A1) 擷取一原始影像及一浮水印影像，其中，該原始影像係為一 O_H 圖素乘以 O_W 圖素之影像，該浮水印影像係為一 W_H 圖素乘以 W_W 圖素之影像，當中， O_H 為該原始影像之高度， O_W 為該原始影像之寬度， W_H 為該浮水印影像之高度， W_W 為該浮水印影像之寬度；

(A2) 將該原始影像切割為 $W_H \times W_W$ 個區塊；

(A3) 使用離散餘弦正轉換技術，將每一區塊之數值轉換為一頻率域區塊係數；

(A4) 以亂數打亂該等頻率域區塊係數之順序；

(A5) 擷取出該等打亂後之頻率域區塊係數之離散餘弦值，以由 $W_H \times W_W$ 個離散餘弦值來形成一離散餘弦值數列；

(A6) 排序該離散餘弦值數列；

(A7) 根據該排序後之離散餘弦值數列及一預設之門檻值以產生一暫時金鑰；及

(A8) 將該暫時金鑰併同該浮水印影像進行互斥運算以產生一秘密金鑰，以將該原始影像轉換為一嵌入有該秘密金鑰之保護影像；

以及

第二程序，用以自一保護影像中萃取出一 W_H 圖素乘以 W_W 圖素之浮水印影像，其中，該保護影像係具有一秘

密金鑰， W_H 為該浮水印影像之高度， W_W 為該浮水印影像之寬度，其包括下列步驟：

- (B1) 擷取一保護影像；
- (B2) 將該保護影像切割為 $W_H \times W_W$ 個區塊；
- (B3) 使用離散餘弦正轉換技術，將每一區塊之數值轉換為一頻率域區塊係數；
- (B4) 以亂數打亂該等頻率域區塊係數之順序；
- (B5) 擷取出該等打亂後之頻率域區塊係數之離散餘弦值，以由 $W_H \times W_W$ 個離散餘弦值來形成一離散餘弦值數列；
- (B6) 排序該離散餘弦值數列；
- (B7) 自一秘密金鑰中擷取出一門檻值，並將扣除該門檻值後之該秘密金鑰儲存為一第一暫時金鑰；
- (B8) 根據該排序後之離散餘弦值數列及該門檻值以產生一第二暫時金鑰；及
- (B9) 將該第一暫時金鑰及該第二暫時金鑰進行互斥運算以萃取出一待測浮水印影像。

2. 如申請專利範圍第1項所述之方法，其中，該原始影像為 $O = \{o_{i,j} \mid 0 \leq o_{i,j} \leq 2^b - 1\}$ ，當中，每一 $o_{i,j}$ 係為一圖素，每一圖素係具有 β 位元，且 $0 \leq i \leq O_H - 1$ ， $0 \leq j \leq O_W - 1$ 。

3. 如申請專利範圍第2項所述之方法，其中，該原始影像係為一灰階影像。

4. 如申請專利範圍第2項所述之方法，其中，該浮水印影像係為一二元影像 $W = \{w_{i,j} \mid w_{i,j} \in \{0,1\}\}$ ，當中，每一 $w_{i,j}$ 係為一圖素，且 $0 \leq i \leq W_H - 1$ ， $0 \leq j \leq W_W - 1$ 。

5. 如申請專利範圍第1項所述之方法，其中，於步驟(A2)中，每一區塊之大小為 $\frac{O_H}{W_H} \times \frac{O_W}{W_W}$ ，且每一區塊

$$\text{係為 } B_{m,n} = \begin{bmatrix} O_{i,j} & O_{i,j+1} & \cdots & O_{i,j+w-1} \\ O_{i+1,j} & O_{i+1,j+1} & \cdots & O_{i+1,j+w-1} \\ \cdots & \cdots & \cdots & \cdots \\ O_{i+h-1,j} & \cdots & \cdots & O_{i+h-1,j+w-1} \end{bmatrix}, \text{ 當中, } 0 \leq m \leq W_H - 1,$$

$$0 \leq n \leq W_W - 1.$$

6. 如申請專利範圍第1項所述之方法，其中，於步驟(A7)中，該暫時金鑰為 $T = \{t_{m,n} | t_{m,n} \in \{0,1\}\}$ ，當中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ ，且當 $DS_{m,n}$ 之前(門檻值 $\times$ 區塊總數)之數在 $D_{m,n}$ 之相對區塊上設定為1時， $t_{m,n}$ 為1，當 $DS_{m,n}$ 之後(區塊總數 - (門檻值 $\times$ 區塊總數))之數在該 $D_{m,n}$ 之相對區塊上設定為0時， $t_{m,n}$ 為0，且 $DS_{m,n}$ 為該排序後之離散餘弦值數列， $D_{m,n}$ 為該離散餘弦值數列。

7. 如申請專利範圍第1項所述之方法，其中，於步驟(A8)中，該秘密金鑰為 $K = (T \oplus W) \parallel TH$ ，當中， T 為該暫時金鑰， W 為該浮水印影像， TH 為該門檻值。

8. 如申請專利範圍第1項所述之方法，其中，於步驟(B8)中，該第二暫時金鑰為 $T2 = \{t_{m,n} | t_{m,n} \in \{0,1\}\}$ ，當中， $0 \leq m \leq W_H - 1$ ， $0 \leq n \leq W_W - 1$ ，且當 $DS_{m,n}$ 之前(門檻值 $\times$ 區塊總數)之數在 $D_{m,n}$ 之相對區塊上設定為1時， $t_{m,n}$ 為1，當 $DS_{m,n}$ 之後($DS_{m,n}$ - (門檻值 $\times$ 區塊總數))之數在 $D_{m,n}$ 之相對區塊上設定為0時， $t_{m,n}$ 為0，且 $DS_{m,n}$ 為該排序後之離散餘弦值數列， $D_{m,n}$ 為該離散餘弦值數列。

9. 如申請專利範圍第8項所述之方法，其中，於步驟(B9)中，該待測浮水印影像為 $W'=(T1 \oplus T2)$ ，當中， $T1$ 為該第一暫時金鑰， $T2$ 為該第二暫時金鑰。

10. 如申請專利範圍第1項所述之方法，其中，於步驟(A8)之後尚包括一步驟(A9)，其將該秘密金鑰向一公正第三者註冊，以產生一具有一時戳簽章之金鑰。

11. 如申請專利範圍第1項所述之方法，其係使用位元正確率法以比對原始浮水印影像及該待測浮水印影像之相似度。

12. 如申請專利範圍第11項所述之方法，其中，該位元正確率法為 $BCR = \frac{\sum_{i=1}^{W_H} \sum_{j=1}^{W_W} \overline{w(i,j) \oplus w'(i,j)}}{W_H \times W_W} \times 100\%$ ，當

中， $w(i,j)$ 為該原始浮水印影像在座標 (i,j) 之位元值， $w'(i,j)$ 為該待測浮水印影像在座標 (i,j) 之位元值。

13. 如申請專利範圍第1項所述之方法，其中，步驟(A2)係將該原始影像切割為 $W_H \times W_W$ 個等比例區塊。

14. 如申請專利範圍第1項所述之方法，其中，步驟(B2)係將該保護影像切割為 $W_H \times W_W$ 個等比例區塊。

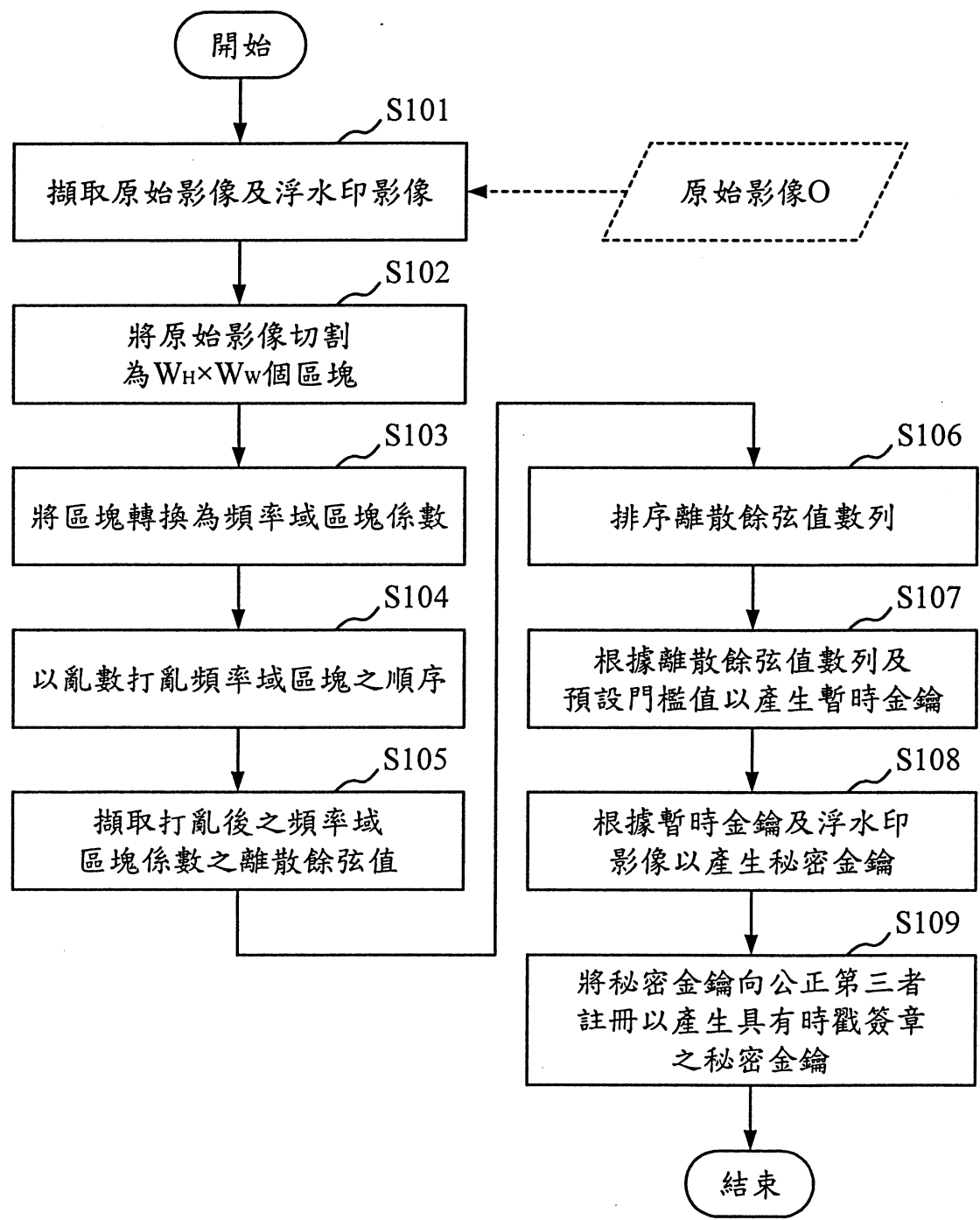


圖1

000277

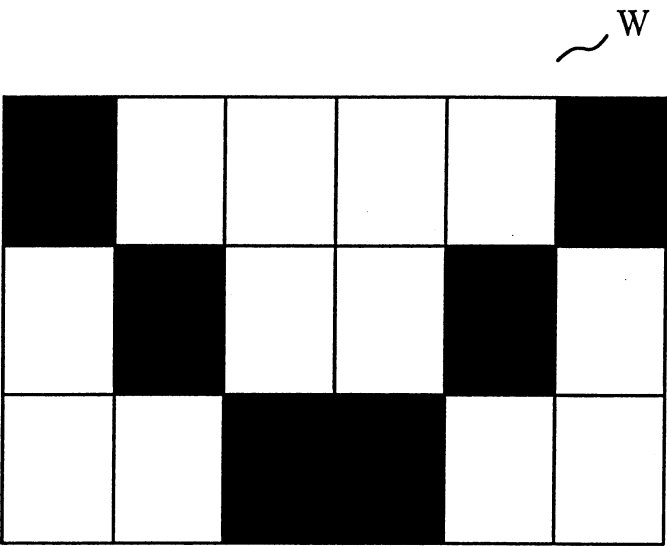


圖2

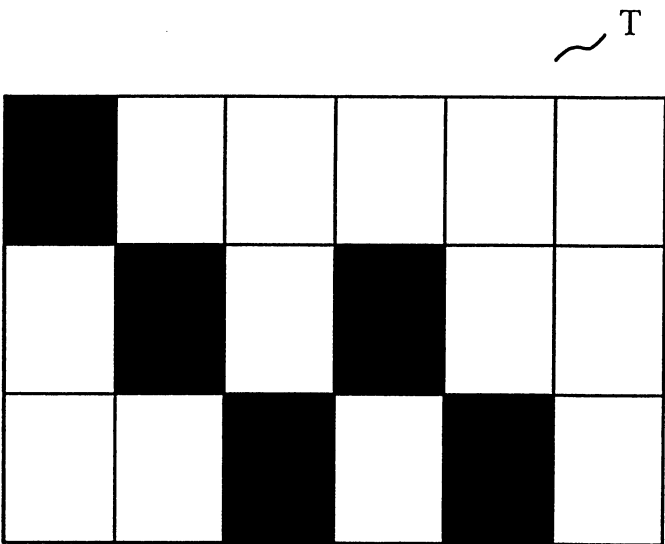


圖3

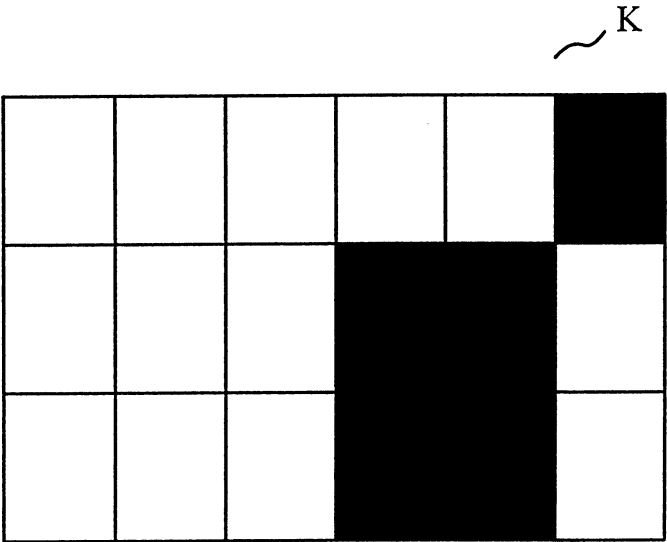


圖4

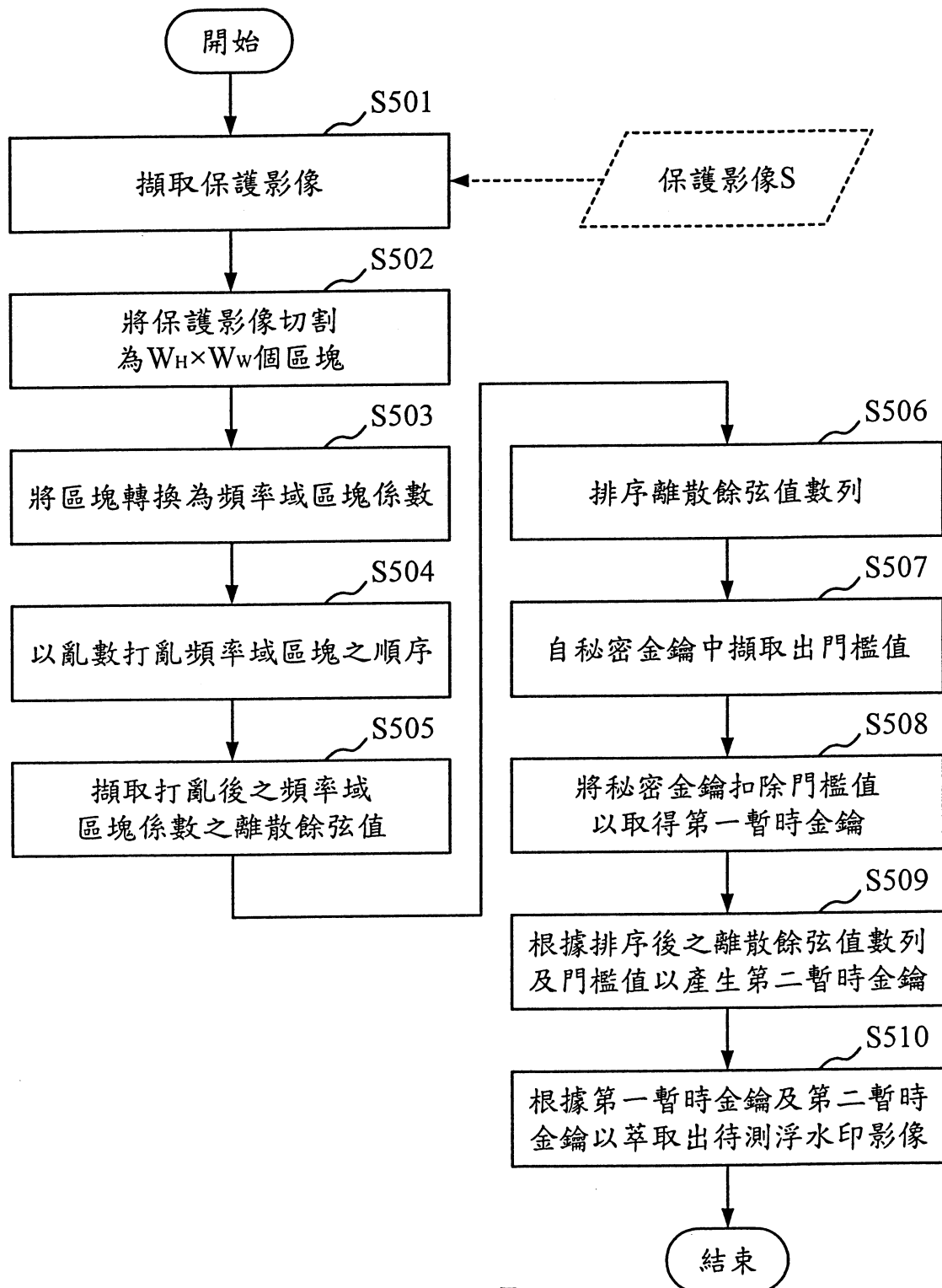


圖5

~T1

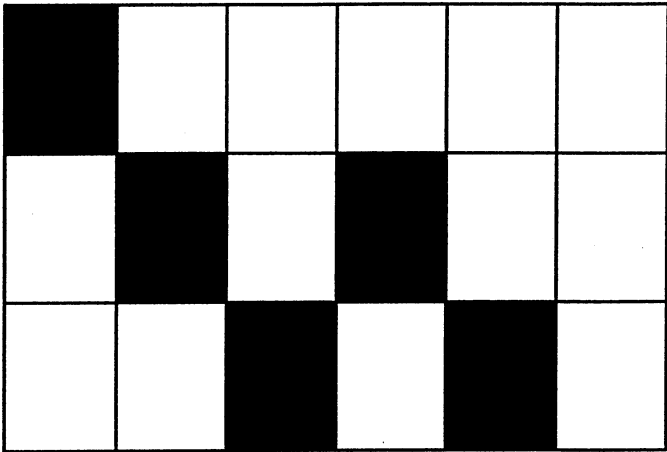


圖6

~T2

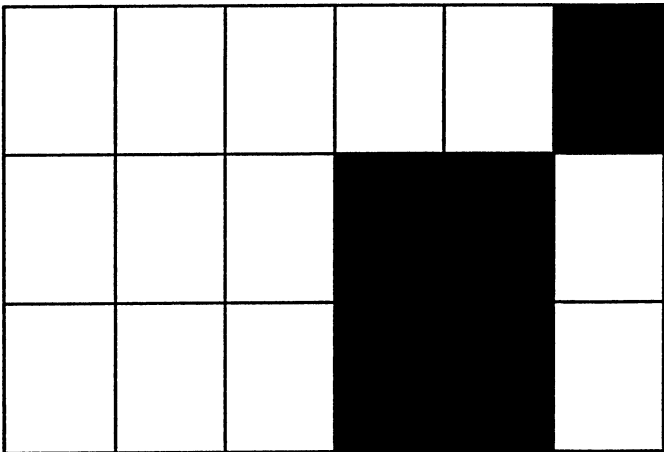


圖7

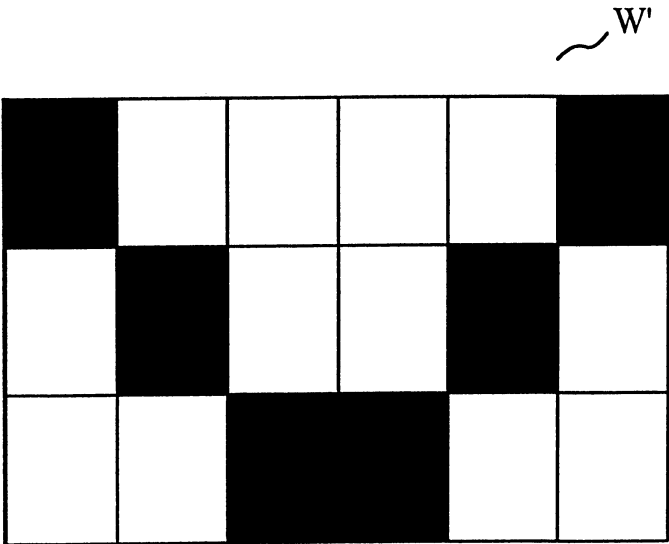


圖8

000202