I486809

(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 I486809 B

(45)公告日： 中華民國 104 (2015) 年 06 月 01 日

(21)申請案號：099120147 (22)申請日： 中華民國 99 (2010) 年 06 月 21 日

(51)Int. Cl.： *G06F21/64 (2013.01)* *H04N7/18 (2006.01)*

(30)優先權：2009/06/30 歐洲專利局 09164110.0

2009/07/06 美國 61/223,248

(71)申請人：亞克瑟斯公司 (瑞典) AXIS AB (SE)

瑞典

(72)發明人：倫得堡 史蒂芬 LUNDBERG, STEFAN (SE)；吉荷蔓 克麗斯汀 GEHRMANN, CHRISTIAN (SE)；圖爾寶 喬阿西曼 TULLBERG, JOACIM (SE)；藤奈洛特 福瑞德瑞克 TERNEROT, FREDRIK (SE)

(74)代理人：陳長文

(56)參考文獻：

TW I287767 TW I288932

TW I289829 US 6938015B2

審查人員：游象甫

申請專利範圍項數：15 項 圖式數：3 共 43 頁

(54)名稱

用於限制存取由攝影機產生的媒體資料的方法

METHOD FOR RESTRICTING ACCESS TO MEDIA DATA GENERATED BY A CAMERA

(57)摘要

本揭示內容係關於一種用於限制存取由一攝影機(10)產生的媒體資料的方法。該方法包括：在該攝影機(10)中設定一非公開的初始使用者密鑰(K_{ICU})，將該初始使用者密鑰(K_{ICU})提供給一使用者用戶端(16)，藉由自該使用者用戶端(16)發送包含基於該初始使用者密鑰(K_{ICU})之資訊的一鑑認訊息至該攝影機(10)而建立該使用者用戶端(16)與該攝影機(10)之間的一鑑認關係，檢查該攝影機(10)中是否已設定一操作性使用者密鑰(K_{OCU})，及回應於檢查該攝影機(10)中是否已設定該操作性使用者密鑰(K_{OCU})之該動作而僅在若未設定該操作性使用者密鑰(K_{OCU})時執行以下動作 a)至 d)：a)獲取一操作性使用者密鑰(K_{OCU})；b)在該攝影機(10)中設定該操作性使用者密鑰(K_{OCU})；c)將該操作性使用者密鑰(K_{OCU})發送至該使用者用戶端(16)；及 d)在該攝影機(10)中指示該操作性使用者密鑰(K_{OCU})已被設定。該方法進一步包括在該攝影機(10)中設定與該操作性使用者密鑰(K_{OCU})相關之一媒體資料加密/解密密鑰，使用該媒體資料加密密鑰來加密由該攝影機(10)註冊之媒體資料，及將經加密之媒體資料發送至一服務提供商管理伺服器(17)。

The disclosure relates to a method for restricting access to media data generated by a camera (10). The method, comprises: setting a non-public initial user key (K_{ICU}) in the camera (10), providing a user client (16) with the initial user key (K_{ICU}), establishing an authenticated relation between the user client (16) and the camera (10) by sending an authentication message including information based on the initial user key (K_{ICU}) from the user client (16) to the camera (10), checking if an operational user key (K_{OCU}) is set in

the camera (10), and performing, in response to the act of checking if the operational user key (K_{OCU}) is set in the camera (10), the acts a) -d) only if the operational user key (K_{OCU}) is not set: a) acquiring an operational user key (K_{OCU}), b) setting the operational user key (K_{OCU}) in the camera (10), c) sending the operational user key (K_{OCU}) to the user client (16), and d) indicating in the camera (10) that the operational user key (K_{OCU}) is set. The method further comprises setting, in the camera (10), a media data encryption/ decryption key associated with the operational user key (K_{OCU}), encrypting media data registered by the camera (10) using the media data encryption key, and sending the encrypted media data to a service provider management server (17).

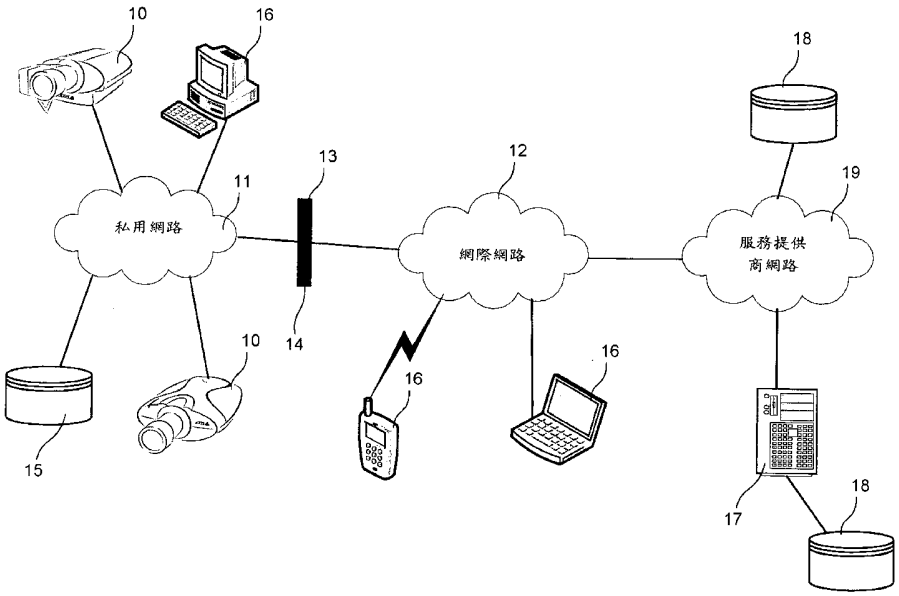

圖 1

10・・・網路視訊攝影機

11・・・私用網路

12・・・網際網路

13・・・網路位址轉換器(NAT)

14・・・防火牆

15・・・本地儲存單元

16・・・使用者用戶端

17・・・服務提供商管理伺服器

18・・・服務提供商儲存單元

19・・・服務提供商網路

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種用於限制存取由一攝影機產生的媒體資料的方法及一種經配置以編碼該產生的媒體資料的攝影機。

【先前技術】

一視訊監視系統之一重要的作用係可能記錄視訊及其他媒體內容，諸如音訊或警報事件。此等記錄允許使用者稍後(例如)搜尋特定的媒體資料及追蹤事故等。

一視訊監視系統之另一重要的作用係可能即時監視該監視系統所涵蓋之區域。

在一基於用戶的監視系統中，該使用者想要一服務提供商處置該監視系統之設定以及媒體儲存及儲存服務，使得該使用者自身無需組態該監視系統或監視資料的任意記錄。例如，該使用者應能夠直接連接至該服務提供商，並且使用該服務提供商所提供之搜尋及檢索服務而搜尋且檢視該監視資料之記錄。

然而，一家庭環境中之即時或記錄的媒體資料可含有該使用者在任何情況下不想要該服務提供商存取之非常敏感的資訊。

因此，重要的是提供一種系統使得在該服務提供商站點處之即時或儲存的媒體資料受到保護且該媒體資料僅可由物產之擁有者存取。此外，仍必須可能使該服務提供商存取元資料之記錄，諸如時戳、視訊觸發資訊、警報資料或

相似物，使得該服務提供商可對終端使用者提供對於警報及記錄之一高效的搜尋服務。

C. H. Bennet之US 7477740中描述一種用於提供由一資料獲取裝置獲取之資料的受保護儲存的系統。US 7477740中描述一種連接至一安全加密處理器之資料獲取裝置，例如具有一麥克風的一視訊攝影機。在將由該資料獲取裝置獲取之資料傳遞至儲存單元之前，該安全加密處理器加密該資料。此暗指該資料一直以加密形式儲存。因此，僅具有正確存取密鑰之一經授權的人士能夠解密該資料。

然而，若根據US 7477740加密該資料且該資料僅由該使用者可存取，則將不可能使該服務提供商存取元資料之記錄，諸如時戳、視訊觸發資訊、警報資料或相似物以使得該服務提供商可對該終端使用者提供對於警報及記錄之一高效的搜尋服務。

本發明描述對上文提及之問題的一解決方案。

【發明內容】

本發明之一目的係防止在該服務提供商站點處之即時或儲存的媒體資料受到未被所監視站點之擁有者/佔有者信任之一人士的未經授權的存取。

以上目的係藉由根據獨立技術方案之方法及攝影機而達成。附屬技術方案中提出本發明之進一步實施例。

特定言之，一種用於限制存取由一攝影機產生的媒體資料的方法包括：在該攝影機中設定一非公開的初始使用者密鑰，將該初始使用者密鑰提供給一使用者用戶端，藉由

自該使用者用戶端發送包含基於該初始使用者密鑰之資訊的一鑑認訊息至該攝影機而建立該使用者用戶端與該攝影機之間的一鑑認關係，檢查該攝影機中是否設定一操作性使用者密鑰，及回應於檢查該攝影機中是否設定該操作性使用者密鑰之該動作而僅在若未設定該操作性使用者密鑰時執行動作a)至d)：a)獲取一操作性使用者密鑰，b)在該攝影機中設定該操作性使用者密鑰，c)在該使用者用戶端中設定該操作性使用者密鑰，及d)在該攝影機中指示該操作性使用者密鑰已被設定。該方法進一步包括在該攝影機(10)中設定與該操作性使用者密鑰相關之一媒體資料加密/解密密鑰，使用該媒體資料加密/解密密鑰來加密由該攝影機註冊之媒體資料，及將經加密之媒體資料發送至一服務提供商管理伺服器。

藉由用於限制存取由一攝影機產生的媒體資料的此方法，可能保護該服務提供商站點處之即時或儲存的媒體資料，使得該媒體資料僅可由該使用者存取，而不可由該服務提供商存取。藉由使用與該操作性使用者密鑰相關之該媒體資料加密/解密密鑰之加密而防止該服務提供商存取由該攝影機註冊且隨後發送至該服務提供商管理伺服器之該媒體資料。該媒體資料加密/解密密鑰可以不同的方式與該操作性使用者密鑰相關。根據本發明之一實施例，該媒體資料加密/解密密鑰之推導係基於該操作性使用者密鑰。根據本發明之另一實施例，可使用共用的操作性使用者密鑰將該媒體資料加密/解密密鑰安全地分配給該攝影

機及該使用者用戶端。或者，根據本發明之又一實施例，可將已安全地設定於該攝影機及該使用者用戶端中之該操作性使用者密鑰自身用作為該媒體資料加密/解密密鑰。因此，為了存取該攝影機註冊之媒體資料，必須知道與該操作性使用者密鑰相關之該媒體資料加密/解密密鑰。根據本發明，應確保僅該使用者知道該操作性使用者密鑰，且因此知道該媒體資料加密/解密密鑰。這是因為該使用者首先需要在存取該攝影機之前使用該初始使用者密鑰鑑認他/她自身，且僅一經鑑認的使用者才能夠觸發獲取該操作性使用者密鑰，且僅在若該攝影機中尚未設定一操作性使用者密鑰時才獲取該操作性使用者密鑰。此係藉由在獲取該操作性使用者密鑰之前檢查該攝影機中是否已設定該操作性使用者密鑰而達成。例如，若該服務提供商在對該使用者提供該初始使用者密鑰之前使用該初始使用者密鑰將他/她自身註冊為一使用者，則此情況將被該使用者偵測，因為他/她將不能在該攝影機上成功註冊並對該攝影機進行控制。因此，即使係由該服務提供商對該使用者提供該初始使用者密鑰，此方法防止(例如)該服務提供商控制該攝影機。藉此，此程序確保若該服務提供商選擇代表使用者在該攝影機上註冊以存取該操作性使用者密鑰，則該使用者將在其嘗試重複該程序時發現該情況。因為獲取該操作性密鑰會失敗，且該使用者藉此會發現某個人已獲取該操作性使用者密鑰。

根據一實施例，該方法可進一步包括藉由一任意的使用

者用戶端經由該服務提供商管理伺服器擷取媒體資料，及使用該媒體加密/解密密鑰來解密所擷取之媒體資料。

根據另一實施例，該方法可進一步包括獲取待在該攝影機、該使用者用戶端與一服務提供商管理伺服器之間共用的一共同密鑰，在該攝影機中設定該共同密鑰，對該使用者用戶端及對該服務提供商管理伺服器提供該共同密鑰，使用與該共同密鑰相關之一元資料加密/解密密鑰來加密由該攝影機註冊之元資料，及將經加密之元資料發送至該服務提供商管理伺服器。該元資料加密/解密密鑰可以不同的方式與該共同密鑰相關。根據本發明之一實施例，該元資料加密/解密密鑰之推導係基於該共同密鑰。根據本發明之另一實施例，可使用該共用的共同密鑰將該元資料加密/解密密鑰安全地分配給該攝影機、該服務提供商管理伺服器及該使用者用戶端。或者，根據本發明之又一實施例，可將已安全地設定於該攝影機、該服務提供商管理伺服器及該使用者用戶端中之該共同密鑰自身用作為該媒體資料加密/解密密鑰。此將確保防止該元資料被一第三方存取。此外，藉由將該元資料發送至該服務提供商管理伺服器，將可能使該服務提供商存取元資料的記錄，諸如時戳、視訊觸發資訊、警報資料及相似物，使得該服務提供商可對該使用者提供對於警報及記錄之一高效的搜尋服務。

根據又一實施例，該方法可進一步包括獲取一服務提供商密鑰，及對該服務提供商管理伺服器提供該服務提供商

密鑰，其中服務提供商密鑰係用於保證僅該服務提供商管理伺服器可存取服務提供商組態功能。

根據一實施例，在該攝影機中指示該操作性使用者密鑰已被設定之該動作可包括刪除該初始使用者密鑰而不再使用。

根據另一實施例，該方法可進一步包括若該操作性使用者密鑰被設定則指示該操作性使用者密鑰已被設定。

根據又一實施例，該方法可進一步包括在該攝影機中設定一主密鑰。在此情況下，在該攝影機中設定該非公開的初始使用者密鑰之該動作包括：藉由使用一第一單向函數自該主密鑰推導該非公開的初始使用者密鑰而獲取該非公開的初始使用者密鑰。

根據一實施例，獲取該服務提供商密鑰之該步驟可包括：使用一第二單向函數自該主密鑰推導該服務提供商密鑰。

根據另一實施例，獲取該共同密鑰之該步驟可包括：使用一第三單向函數自該非公開的初始使用者密鑰推導該共同密鑰，或使用一第四單向函數自該服務提供商密鑰推導該共同密鑰，其中該第三單向函數及該第四單向函數係經配置以產生無關於該共同密鑰係自該非公開的初始使用者密鑰或自該服務提供商密鑰推導出的一相同的共同密鑰。

根據又一實施例，建立該使用者用戶端與該攝影機之間的該鑑認關係之該動作可進一步包括：在執行藉由自該使用者用戶端發送包含基於該初始使用者密鑰之資訊的一鑑

認訊息至該攝影機而鑑認該使用者用戶端之後，藉由自該攝影機發送一視訊序列至該使用者用戶端以驗證該視訊序列被所期望之攝影機即時擷取，且自該使用者用戶端發送作為該攝影機鑑認之確認的一確認訊息至該攝影機而鑑認該攝影機。

此外，根據本發明之另一態樣，經配置以編碼由該攝影機註冊之媒體資料的一網路攝影機包括：經配置以使用一安全的密鑰產生程序來產生一初始使用者密鑰或一操作性使用者密鑰之一密鑰產生構件；經配置以指示是否已產生該操作性使用者密鑰之一指示構件；經配置以檢查該指示構件是否已指示已產生該操作性使用者密鑰之一檢查構件；經配置以使用與該操作性使用者密鑰相關之一媒體資料加密密鑰來加密由該攝影機註冊之媒體資料的一加密構件；及經配置以傳輸經加密之媒體資料的一數位網路模組。該媒體資料加密/解密密鑰可以不同的方式與該操作性使用者密鑰相關。根據本發明之一實施例，該媒體資料加密/解密密鑰之推導係基於該操作性使用者密鑰。根據本發明之另一實施例，可使用該共用的操作性使用者密鑰將該媒體資料加密/解密密鑰安全地分配給該攝影機及該使用者用戶端。或者，根據本發明之又一實施例，可將已安全地設定於該攝影機及該使用者用戶端中之該操作性使用者密鑰自身用作為該媒體資料加密/解密密鑰。

根據一實施例，該網路攝影機可進一步包括經配置以重設所產生之操作性使用者密鑰之一重設構件。

根據另一實施例，該重設構件可包括一重設按鈕。

根據又一實施例，該指示構件可經配置以刪除該初始使用者密鑰而不再使用(若已產生該操作性使用者密鑰)。

根據一實施例，該密鑰產生構件可進一步經配置以產生一共同密鑰，其中該加密構件可進一步經配置以使用與該共同密鑰相關之一元資料加密/解密密鑰來加密由該攝影機註冊之元資料，且其中該數位網路模組可進一步經配置以傳輸經加密之元資料。該元資料加密/解密密鑰可以不同的方式與該共同密鑰相關。根據本發明之一實施例，該元資料加密/解密密鑰之推導係基於該共同密鑰。根據本發明之另一實施例，可使用該共用的共同密鑰將該元資料加密/解密密鑰安全地分配給該攝影機、該服務提供商管理伺服器及該使用者用戶端。或者，根據本發明之又一實施例，可將已安全地設定於該攝影機、該服務提供商管理伺服器及該使用者用戶端中之該共同密鑰自身用作為該媒體資料加密/解密密鑰。

自下文給出之詳細描述，將易於得知本發明之適用範圍的一進一步範疇。然而，應瞭解的是，因為自此詳細描述，熟習此項技術者將易於得知本發明之精神及範疇內之各種變化及修改，所以雖然該詳細描述及特定實例指示本發明之較佳實施例，但是僅以繪示方式給出。

【實施方式】

將參考展示本發明之實施例的隨附示意圖式以實例方式更詳細地描述本發明。

如圖1中所繪示，視訊監視可實施為一基於用戶的系統，其中一使用者在待監視之一位置處(例如該使用者的家裏)安裝網路視訊攝影機，但是其中該等攝影機係由一服務提供商或至少經由一服務提供商而控制及管理。

根據圖1中所示之實施例的該監視系統包括監視一物產之一網路視訊攝影機10。該網路視訊攝影機10係連接至一私用網路11，該私用網路11係連接至一公用網路(諸如網際網路12)、一網路位址轉換器(NAT)13及/或防止該私用網路11受到外部攻擊之一防火牆14，一使用者用戶端16直接連接至該私用網路11或連接至該網際網路12，一服務提供商透過連接至一服務提供商網路19之一公用服務提供商管理伺服器17提供使用者物產監視服務，且一服務提供商儲存單元18直接連接至該服務提供商管理伺服器17或連接至該服務提供商網路19。該服務提供商網路19亦連接至該公用網路(諸如該網際網路12)。

該網路視訊攝影機10監視該使用者之本地物產且同時在該遠端服務提供商儲存單元18上記錄媒體資料(例如視訊資料及可能其他的媒體資料(諸如音訊資料))。此外，除該媒體資料以外，該網路視訊攝影機10亦記錄元資料，諸如時戳、視訊觸發資訊、警報資料及相似物。該元資料亦記錄在該遠端服務提供商儲存單元18上。視情況，該媒體資料及該元資料亦可記錄在一本地儲存單元15上。

若該使用者想要藉由該使用者用戶端16搜尋並擷取所儲存之媒體資料，則該使用者經由該網際網路12連接至該服

務提供商管理伺服器17。當連接至該服務提供商管理伺服器17時，該使用者可搜尋並下載所記錄之媒體資料。該媒體資料可藉由下載一統一資源定位(URL)或藉由自該服務提供商管理伺服器17擷取一媒體串流而下載。視情況，若該媒體資料及該元資料位於該本地儲存單元15，則該使用者用戶端16可直接在該本地儲存單元15上存取該記錄的媒體資料。

類似地，若該使用者想要存取即時的媒體資料，則該使用者使用該使用者用戶端16連接至該服務提供商管理伺服器17，並請求將即時的媒體資料下載或以串流傳送至該使用者用戶端16。視情況，若該使用者用戶端16係連接至該私用網路11，則該使用者可直接存取該網路視訊攝影機10以存取該即時的媒體資料。

如與該使用者完全自行組態且管理該監視系統之一系統相比，在系統中包含該服務提供商之優點在於前者將需要來自該使用者之先進的組態技術。另外，此種組態將需要額外的軟體及設備。此外，因為該網路視訊攝影機10或該本地儲存單元15位於一防火牆14及/或一網路位址轉換器13之後，故該使用者將不能夠自該網際網路12容易地存取該網路視訊攝影機10或該本地儲存單元15。另一方面，因為一服務提供商將存取來自該使用者之物產的即時的媒體資料或記錄的媒體資料，所以具有該服務提供商之一系統需要該使用者對該服務提供商充分信任。本發明解決此問題。

根據本發明，提出一種基於在若干步驟中之密鑰推導的媒體保護解決方案。根據一實施例，在若干步驟中之該密鑰推導執行如下，參見圖2。

作為一第一步驟，步驟100產生一唯一的秘密主密鑰K_M。步驟102在該攝影機10中設定該秘密主密鑰K_M。該主密鑰K_M之此設定可(例如)藉由在該視訊攝影機10中儲存該主密鑰K_M而執行。該主密鑰K_M之該儲存可(例如)由一攝影機製造商或由該服務提供商執行。該主密鑰K_M係使用一安全的密鑰產生程序而產生，諸如(例如)使用與一安全的偽隨機數產生器組合之基於熱或無線電雜訊之量測的安全的隨機源之密鑰產生。該主密鑰K_M可在該攝影機10自身內產生或該主密鑰K_M可在外部產生然後提供給該攝影機10。

步驟104將該主密鑰K_M用於推導一初始使用者密鑰K_{ICU}。該初始使用者密鑰K_{ICU}可為攝影機唯一。步驟106亦將該主密鑰K_M用於推導一服務提供商密鑰K_{SP}。該服務提供商密鑰K_{SP}可為攝影機唯一。步驟108繼而將該初始使用者密鑰K_{ICU}或該服務提供商密鑰K_{SP}用於推導一共同密鑰K_C。該共同密鑰K_C亦可為攝影機唯一。

自該主密鑰K_M推導該初始使用者密鑰K_{ICU}可藉由一第一單向函數f_1而執行，亦即$K_{ICU}=f_1(K_M)$。

一適當的單向函數係對於每個輸入容易計算但是難以逆轉給出一隨機輸入之影像的一函數。此等函數之實例係雜湊(hash)函數(諸如SHA-1或SHA-256)或自此等雜湊函數推導之函數(諸如對於固定(已知)文字輸入(將密鑰值作為未

知的輸入)之基於SHA-1的雜湊訊息鑑認碼(HMAC))或基於SHA-256的雜湊訊息鑑認碼及相似物。

類似地，自該主密鑰(K_M)推導該服務提供商密鑰K_{SP}可藉由一第二單向函數f_2而執行，亦即$K_{SP}=f_2(K_M)$。

可藉由一第三單向函數f_3自該初始使用者密鑰K_{ICU}推導該共同密鑰K_C，亦即$K_C=f_3(K_{ICU})$。或者，可藉由一第四單向函數f_4自該服務提供商密鑰K_{SP}推導該共同密鑰K_C，亦即$K_C=f_4(K_{SP})$。

該第三單向函數(f_3)及該第四單向函數(f_4)係經配置以產生無關於該共同密鑰K_C係自該非公開的初始使用者密鑰K_{ICU}或自該服務提供商密鑰K_{SP}推導的一相同的共同密鑰K_C，亦即$K_C=f_3(K_{ICU})=f_4(K_{SP})$。此種建構之一實例係在推導$K_{ICU}$及$K_{SP}$時，使得$K_{ICU}$及$K_{SP}$具有一共同的相同部分，且使得該單向函數$f_3$將$K_{ICU}$截斷至此共同部分並對該截斷部分應用一適當的雜湊函數。類似地，然後f_4首先將K_{SP}截斷至該共同部分，且然後對此部分應用相同的雜湊函數。在此情況下，f_1及f_2需經選擇以匹配此需要。f_1及f_2其實可以藉由(例如)將$f_1(K)$定義為$a_{(K)}+f'_{1(K)}$且將$f_2(K)$定義為$a_{(K)}+f'_{2(K)}$之此一方式而選擇，其中+標示串連(concatenation)，且f'_1及f'_2皆標示唯一的單向雜湊函數。

將所有此等密鑰(該主密鑰K_M、該初始使用者密鑰K_{ICU}、該服務提供商密鑰K_{SP}及該共同密鑰K_C)用作為信任實體與半信任實體之間的初始安全關聯的基礎，但是其等不必為用於該媒體資料之實際保護的密鑰。

步驟110在該攝影機10中設定該初始使用者密鑰K_{ICU}，步驟112將該初始使用者密鑰K_{ICU}連同該攝影機10提供給該使用者用戶端16。因此，該初始使用者密鑰K_{ICU}實體上位於該使用者用戶端16處且由該使用者控制。該服務提供商可(例如)將該攝影機10及該初始使用者密鑰K_{ICU}提供給該使用者。

步驟113在該攝影機10中設定該服務提供商密鑰K_{SP}，且步驟114將該服務提供商密鑰K_{SP}提供給該服務提供商。

步驟115在該攝影機10中設定該共同密鑰K_C，且步驟116及118將該共同密鑰K_C提供給該使用者及該服務提供商兩者。此操作可(例如)使用上文所述之該共同密鑰K_C、該初始使用者密鑰K_{ICU}與該服務提供商密鑰K_{SP}之間的關係而執行，亦即$K_C=f_3(K_{ICU})=f_4(K_{SP})$。

藉由在該攝影機中設定該主密鑰且隨後自該主密鑰推導該初始使用者密鑰、該服務提供商密鑰及該共同密鑰而提供一種用於高效地分配用於存取媒體資料、元資料及攝影機之密鑰的解決方案。

在存取該攝影機10之前，該使用者需要在該攝影機10上鑑認其自身為該使用者。在該鑑認期間，步驟120建立該使用者用戶端16與該攝影機10之間的一鑑認關係。該使用者係藉由自該使用者用戶端16發送包含基於該初始使用者密鑰K_{ICU}之資訊的一鑑認訊息及一使用者身份至該攝影機10而鑑認。該攝影機係藉由自該攝影機10發送一視訊序列至該使用者用戶端16以驗證該視訊序列被所期望之攝影機

10即時擷取，且自該使用者用戶端16發送作為該攝影機鑑認之確認的一確認訊息至該攝影機10而鑑認。

當已經建立該攝影機10與該使用者用戶端16之間的該鑑認關係時，步驟124獲取一操作性使用者密鑰K_{OCU}，步驟126在該攝影機中設定該操作性使用者密鑰K_{OCU}，且步驟128對該使用者分配該操作性使用者密鑰K_{OCU}。步驟127亦在該攝影機10指示該操作性使用者密鑰K_{OCU}之該設定。僅該操作性使用者密鑰K_{OCU}之擁有者將具有對該攝影機10及由該攝影機10產生之媒體資料的完全的存取權力。該操作性使用者密鑰K_{OCU}可(例如)在該攝影機10中產生。該操作性使用者密鑰K_{OCU}之分配可受該初始使用者密鑰K_{ICU}保護。該操作性使用者密鑰K_{OCU}可為攝影機唯一。

在執行獲取該操作性使用者密鑰K_{OCU}之步驟124之前，步驟122進行檢查該攝影機中是否設定該操作性使用者密鑰K_{OCU}之一檢查。僅在若自步驟122中之該檢查的結果指出該攝影機10中未設定該操作性使用者密鑰K_{OCU}時，才執行步驟124獲取該操作性使用者密鑰K_{OCU}、步驟126在該攝影機10中設定該操作性使用者密鑰K_{OCU}、步驟127在該攝影機10中指示該操作性使用者密鑰K_{OCU}被設定、及步驟128將該操作性使用者密鑰K_{OCU}發送至該使用者用戶端16。因此，該該初始使用者密鑰K_{ICU}將僅被使用一次以產生該操作性使用者密鑰K_{OCU}。因此，若該服務提供商在對該使用者提供該初始使用者密鑰K_{ICU}之前使用該初始使用者密鑰K_{ICU}鑑認他/她自身為一使用者，則此情況將被該使

用者偵測，因為他/她將無法在該攝影機10上成功鑑認且控制該攝影機。

因此，此方法防止(例如)該服務提供商控制該攝影機，即使該服務提供商對該使用者提供該初始使用者密鑰K_{ICU}。藉此，該程序確保若該服務提供商選擇代表使用者在該攝影機10上註冊以存取該操作性使用者密鑰K_{OCU}，則該使用者將在其嘗試重複該程序時發現該情況。因為獲取該操作性密鑰K_{OCU}會失敗，且該使用者藉此會發現某個人已獲取該操作性密鑰K_{OCU}。

若在該使用者向該攝影機10註冊期間出現任何問題，則該使用者可產生一新的初始使用者密鑰K_{ICU}或一新的操作性使用者密鑰K_{OCU}。例如，具有對該攝影機10之實體存取或根據其他存取限制規則的一使用者能夠重設該攝影機中之安全設定並觸發該攝影機中之一新的初始使用者密鑰K_{ICU}的一產生(步驟130)。或者，具有對該攝影機之實體存取或根據其他存取限制規則的一使用者能夠刪除當前所使用之操作性使用者密鑰K_{OCU}，並需要使用該初始使用者密鑰K_{ICU}之一新的註冊，且因此獲取一新的操作性使用者密鑰K_{OCU}(步驟132)。該重設程序(步驟130)或該刪除程序(步驟132)可藉由按壓位於該攝影機10外殼上的一重設按鈕而啟動。其他的存取限制規則之實例可為(例如)基於由該使用者提供之無線或光傳輸觸發信號之遠端本地控制或基於一受保護觸發之經由網路的遠端控制。在後一種情況下，該觸發可受(例如)該共同密鑰K_C或該服務提供商密鑰K_{SP}

保護。

本發明基於該操作性使用者密鑰K_{OCU}使自該攝影機10傳輸之全部媒體資料受到保護，且使由該攝影機監視之站點的擁有者/佔有者具有對由該攝影機10產生之媒體資料的獨佔控制。

根據本發明之一實施例，該媒體資料係由使用一媒體資料加密/解密密鑰之對稱加密而加密。根據一實施例，此媒體資料加密/解密密鑰係時間片段密鑰。為增加安全性，本發明提供待劃分為不同時間片段的一通信，各時間片段可使用不同的時間片段密鑰加密。該所使用之時間片段密鑰可(例如)基於時間、所發送之資料數量或所發送之訊息數目而改變。例如，該時間片段密鑰可在x分鐘之後改變，在y百萬位元組資料之後改變，或在發送z個訊息之後改變。根據本發明，用於各自的時間片段的時間片段密鑰未被丟棄，而是與各時間片段之經加密的資訊關聯予以加密且儲存以用於解密及/或鑑認，亦即當前的時間片段密鑰可用於解密包含一較早的時間片段密鑰的資料，從而致能對藉由此較早的時間片段密鑰加密之媒體資料的解密。如在此項技術中已知，對稱加密技術使用相同的密鑰用於加密與解密兩者。對稱加密及解密係快速但是需要發送器(在此情況下為該攝影機10)及接收器(在此情況下為該使用者用戶端16)預先共用一密鑰。根據本發明，預先共用之該密鑰可為該操作性使用者密鑰K_{OCU}。該媒體資料自身係使用呈一時間片段密鑰形式之媒體資料加密/解密密

鑰而加密及解密。

根據本發明之一實施例，呈時間片段密鑰形式之媒體資料加密/解密密鑰的推導可基於該操作性使用者密鑰K_{OCU}。

此外，根據另一實施例，可使用預先共用之該操作性使用者密鑰K_{OCU}將呈時間片段密鑰形式之媒體資料加密/解密密鑰安全地分配給該發送器(該攝影機10)及該接收器(該使用者用戶端16)。

或者，根據本發明之一實施例，可將已安全地分配給該攝影機10及該使用者用戶端16之該操作性使用者密鑰K_{OCU}自身用作為媒體資料加密/解密密鑰。

因此，由該攝影機10產生之媒體資料係使用與該操作性使用者密鑰K_{OCU}相關之媒體資料加密/解密密鑰而加密及解密(步驟134)。因為該媒體資料加密/解密密鑰係自該操作性使用者密鑰K_{OCU}推導(其被安全地分配且受該操作性使用者密鑰K_{OCU}保護)，或者該媒體資料加密/解密密鑰其實就是該操作性使用者密鑰K_{OCU}，所以由該攝影機監視之站點的擁有者/佔有者具有對由該攝影機10產生之媒體資料的獨佔控制。

當該資料媒體被加密時，該資料媒體正被發送至該服務提供商管理伺服器17(步驟136)以用於儲存。

因為僅該使用者擁有該媒體資料加密/解密密鑰，所以僅該使用者可解密及實際上檢視由該攝影機10產生之媒體資料。另外，可基於該共同密鑰K_C替代地保護全部元資

料。

根據本發明之一實施例，該元資料亦由使用一元資料加密/解密密鑰之對稱加密而加密。該元資料加密/解密密鑰可為時間片段密鑰，關於該等時間片段密鑰參見上文。根據本發明，預先共用之該密鑰可為該共同密鑰K_C。該元資料自身係使用呈時間片段密鑰形式之元資料加密/解密密鑰而加密及解密。

根據本發明之一實施例，呈時間片段密鑰形式之元資料加密/解密密鑰的推導可基於該共同密鑰K_C。

此外，根據另一實施例，可使用預先共用之該共同密鑰K_C安全地將呈時間片段密鑰形式之元資料加密/解密密鑰分配給該發送器(該攝影機10)及該接收器(該服務提供商管理伺服器17及/或該使用者用戶端16)。

或者，根據本發明之一實施例，可將已安全地分配給該攝影機10、該服務提供商管理伺服器17及/或該使用者用戶端16之該共同密鑰K_C自身用作為元資料加密/解密密鑰。

因此，由該攝影機10產生之元資料係使用該元資料加密/解密密鑰而加密及解密(步驟138)。因此，由該攝影機10註冊之元資料可使用與該共同密鑰K_C相關之該元資料加密密鑰來加密及解密(步驟138)，且將該元資料發送至該服務提供商管理伺服器17(步驟140)。因此，該使用者與該服務提供商兩者可存取由該攝影機10產生之該元資料，這是因為該使用者與該服務提供商兩者皆具有對該共同密鑰K_C之存

取。

或者，該攝影機10可以使用該共同密鑰K_C來保護全部資料(媒體資料與元資料兩者)之此種方式組態，使得該元資料與該媒體資料兩者可由該使用者與該服務提供商兩者存取。當該使用者想要該服務提供商監視該攝影機站點時，此情況係有用。當該使用者長時間在外時，此實例可為有用。

因此，取決於組態，正當使用者可在該操作性使用者密鑰K_{OCU}或該共同密鑰K_C的幫助下隨時存取且解密媒體資料。

此外，該攝影機10可組態為遠端組態。遠端組態之介面被劃分為至少兩個子集合(可能部分重疊)：可由該服務提供商存取之一集合及可由該使用者存取之另一集合。該服務提供商密鑰K_{SP}係用於保證僅該服務提供商可存取該等服務提供商組態功能，例如服務提供商位址網路組態、無線設定、韌體升級等。類似地，該操作性使用者密鑰K_{OCU}係用於保證僅該使用者可存取使用者組態功能，例如實施攝影機存取保護機構使得僅該操作性使用者密鑰K_{OCU}之持有者將能夠設定加密策略，亦即應基於該操作性使用者密鑰K_{OCU}或該共同密鑰K_C來保護該媒體資料。僅對於該使用者可用之其他功能之實例係媒體串流組態(訊框速率、解析度等)或搖攝-傾斜-放大縮小(Pan-Tilt-Zoom)控制。

為了使該系統容易使用，該使用者可配備一工具(安全性符記/安全性裝置)以產生加密及解密密鑰對且有助於密

鑰儲存。例如，在當該媒體資料加密/解密密鑰係基於該操作性使用者密鑰K_{OCU}之情況下，該操作性使用者密鑰K_{OCU}可儲存在一硬體安全性符記內部，且在該符記與該攝影機之間使用一密鑰管理方案，使得媒體資料加密/解密密鑰總是在該符記及該攝影機內部產生而不在該安全符記外部暴露該操作性使用者密鑰K_{OCU}。

實際的媒體保護(鑑認、加密等)可使用適當之申請專利當時之技術水準的媒體保護機制執行，諸如(例如)Bennett之美國專利第7,477,740號中所述之方法。

接著給出對不同密鑰之推導及在一家庭環境中安裝視訊監視時所涉及之安裝步驟(其係由一基於用戶的系統完成，其中一使用者在他家中安裝一網路視訊攝影機10，但是其中該攝影機10係由一服務提供商控制且管理)的一更詳細的描述。

該攝影機10係由攝影機製造商製造。該主密鑰K_M可在製造該攝影機10時使用一安全的密鑰產生程序產生且而後在該攝影機10中予以設定。在該攝影機10中設定該主密鑰K_M可(例如)藉由使用一安全的程序在該攝影機10中儲存該主密鑰K_M而進行。此一安全程序之一實例係一所謂的受保護攝影機硬體內部的機上密鑰產生。另一實例係使用一安全的密鑰產生程序在該攝影機外部產生密鑰且然後將其傳遞至該攝影機內部之一受保護儲存位置的情況。在後一種情況下，該密鑰將在成功地安裝至該攝影機10中之後，在外部環境中被安全地銷毀。

該主密鑰K_M稍後用於產生三個不同的子密鑰：該服務提供商密鑰K_{SP}、該初始使用者密鑰K_{ICU}及該共同密鑰K_C。此等子密鑰亦在該攝影機10中設定。該等密鑰可(例如)藉由將其等安全地儲存在該攝影機10中而在該攝影機10中予以設定。

可使用一適當的第一單向函數f_1自該主密鑰K_M推導該初始使用者密鑰K_{ICU}，亦即$K_{ICU}=f_1(K_M)$，使得在已知該初始使用者密鑰K_{ICU}之情況下，將不可計算推導該主密鑰K_M。類似地，使用一適當的第二單向函數f_2自該主密鑰K_M推導該服務提供商密鑰K_{SP}，亦即$K_{SP}=f_2(K_M)$，使得在已知該服務提供商密鑰K_{SP}之情況下，將不可計算推導該主密鑰K_M。此外，建構適當的第一單向函數f_1及第二單向函數f_2，使得藉由使用額外的第三單向函數f_3及第四單向函數f_4，該共同密鑰K_C可根據下式而推導：$K_C=f_3(K_{ICU})=f_4(K_{SP})$。因此，可藉由一第三單向函數$f_3$自該初始使用者密鑰$K_{ICU}$推導該共同密鑰$K_C$，亦即$K_C=f_3(K_{ICU})$，或替代地，可藉由一第四單向函數$f_4$自該服務提供商密鑰$K_{SP}$推導該共同密鑰$K_C$，亦即$K_C=f_4(K_{SP})$。該第三單向函數($f_3$)及該第四單向函數($f_4$)係經配置以產生無關於該共同密鑰$K_C$係自該非公開的初始使用者密鑰$K_{ICU}$或自該服務提供商密鑰$K_{SP}$推導的一相同的共同密鑰$K_C$，亦即$K_C=f_3(K_{ICU})=f_4(K_{SP})$。

將該服務提供商密鑰K_{SP}提供給該服務提供商。該攝影機10可能在被遞送至該使用者之前被遞送至該服務提供商。在此情況下，可能的是，該服務提供商密鑰K_{SP}及該

攝影機10一起被遞送。或者，可在該攝影機10連接至該服務提供商伺服器17時將該服務提供商密鑰K_{SP}提供給該服務提供商。在將該服務提供商密鑰K_{SP}遞送或提供給該服務提供商之後，該服務提供商使用該函數f_4並計算該共同密鑰K_C，$K_C=f_4(K_{SP})$，且在一適當的資料庫中安全地儲存該服務提供商密鑰K_{SP}及該共同密鑰K_C。使用者資料(例如姓名、地址等)係儲存在與該服務提供商密鑰K_{SP}及該共同密鑰K_C相關之該資料庫中。該服務提供商密鑰K_{SP}亦可用於保證僅該服務提供商管理伺服器17可存取服務提供商組態功能，例如服務提供商位址及相似物。

將該攝影機10遞送至該使用者且安裝至使用者居住網路11中。該使用者接收與該攝影機10一起之該攝影機唯一的初始使用者密鑰K_{ICU}(可能經由該服務提供商或藉由其他方式)。將該攝影機10安裝至該居住網路11中，使得該服務提供商可以網際網路12存取自任意位置存取該攝影機10，且該使用者用戶端16可以網際網路12存取自任意位置存取該攝影機10。

將該初始使用者密鑰K_{ICU}提供給該使用者用戶端16。例如，該使用者可將該初始使用者密鑰K_{ICU}安全地安裝至該使用者用戶端16中。該初始使用者密鑰K_{ICU}之安裝可經由一通用串列匯流排(USB)棒或相似物而執行。接著，該第三單向函數f_3用於計算該共同密鑰K_C，亦即$K_C=f_3(K_{ICU})$，該共同密鑰K_C亦被安全地儲存在該使用者用戶端16中。

該使用者可能經由服務提供商系統連接至該攝影機10，

並請求該攝影機10註冊該使用者用戶端16。

該使用者用戶端16可(例如)連接至將允許在該使用者用戶端16與該攝影機10之間建立一安全的資料傳輸通道的該服務提供商網路中之一代理伺服器。

使用資料傳輸通道之傳輸可受保護以達成機密性及完整性。此可透過諸如TLS、SSH或IKE/IPsec之協定而達成。在建立該通道時，該攝影機10係使用一公開密鑰憑證而鑑認。該公開密鑰憑證應由一受信任的第三方憑證機構簽署，且此機構之簽署應由該用戶端在接受該安全通道建立之前予以驗證，全部皆根據所使用之所選的協定(TLS、SSH或IKE/IPsec)。

接著，在該使用者用戶端16與該攝影機10之間執行一相互鑑認。該使用者用戶端16係藉由自該使用者用戶端16發送包含基於該初始使用者密鑰K_{ICU}之資訊的一鑑認訊息至該攝影機10而鑑認。而該攝影機10係藉由自該攝影機10發送一視訊序列至該使用者用戶端16以驗證該視訊序列被所期望之攝影機10即時擷取，且自該使用者用戶端16發送作為該攝影機10鑑認之確認的一確認訊息至該攝影機10而鑑認。若該相互鑑認失敗，則該攝影機10及/或該使用者用戶端16中止該鑑認程序。

接著給出對該攝影機10之鑑認的一更詳細描述。在該安全通道建立以後，該攝影機10將一個或若干視訊序列(例如由該攝影機10記錄之JPEG影像的一序列)發送至該使用者用戶端16。此等視訊序列係以在該通道建立時之該攝影

機鑑認所使用之相同的公開密鑰簽署。

該使用者用戶端16自該攝影機10接收該經簽署的一個或若干視訊序列，且驗證其等係由用於該安全通道建立之該相同的公開密鑰簽署。然後，一註冊軟體使用者介面要求該使用者驗證該一個或若干視訊序列確實由該攝影機10即時攝影。若該使用者確認此情況，則在該安全通道之保護下，該使用者用戶端16發送作為該攝影機10鑑認之確認的一確認訊息。

當已建立該攝影機10與該使用者用戶端16之間的一鑑認關係時，獲取一操作性使用者密鑰K_{OCU}並在該攝影機中設定該操作性使用者密鑰K_{OCU}，且將其分配給該使用者。亦在該攝影機10中指示該操作性使用者密鑰K_{OCU}之該設定。僅該操作性使用者密鑰K_{OCU}之擁有者將具有對由該攝影機10產生之媒體資料的完全的存取權力。該操作性使用者密鑰K_{OCU}可藉由在該攝影機10中產生該操作性使用者密鑰K_{OCU}而獲取。該操作性使用者密鑰K_{OCU}之該分配可受該初始使用者密鑰K_{ICU}保護。該操作性使用者密鑰K_{OCU}可為攝影機唯一。

當執行該相互鑑認時，該操作性使用者密鑰K_{OCU}係(例如)藉由該攝影機10中之安全產生而獲取。在獲取該操作性使用者密鑰K_{OCU}之前，執行檢查該攝影機10中是否已設定該操作性使用者密鑰K_{OCU}之一檢查。該操作性使用者密鑰K_{OCU}僅在若該攝影機10中未設定該操作性使用者密鑰K_{OCU}時才獲取。在獲取該操作性使用者密鑰K_{OCU}之後，在

該攝影機10中設定該操作性使用者密鑰K_{OCU}，並在該安全通道保護下將其發送至該使用者用戶端16。因此，該初始使用者密鑰K_{ICU}將僅被使用一次以產生該操作性使用者密鑰K_{OCU}。此防止(例如)該服務提供商控制該媒體資料，即使該服務提供商將該初始使用者密鑰K_{ICU}提供給該使用者。例如，若該服務提供商在對該使用者提供該初始使用者密鑰K_{ICU}之前使用該初始使用者密鑰K_{ICU}將他/她自身註冊為一使用者，則此情況將被該使用者偵測，因為他/她將不能在該攝影機10上成功註冊且控制該攝影機10。該操作性使用者密鑰K_{OCU}被安全地儲存在該攝影機10中及該使用者用戶端16中。

接著，該攝影機10停用該初始使用者密鑰K_{ICU}而不再使用。因此，該攝影機10將不會接受此初始使用者密鑰K_{ICU}作為任何新的操作性使用者密鑰K_{OCU}之建立的基礎。此可(例如)藉由在該攝影機中指示該初始使用者密鑰K_{ICU}被使用、藉由在該攝影機中指示該操作性使用者密鑰K_{OCU}被設定或藉由刪除該初始使用者密鑰K_{ICU}而執行。

上述程序確保若該服務提供商選擇代表使用者在該攝影機10上註冊以存取該操作性使用者密鑰K_{OCU}，則將告知該使用者。當真正的使用者嘗試重複該程序時，該程序會失敗且該使用者會偵測該服務提供商所做的冒用。

根據本發明之一第二實施例，可在該使用者用戶端16與多重攝影機10之間共用該操作性使用者密鑰K_{OCU}。可以若干不同的方式達成此目的。

根據一替代實施例，取代在該攝影機10中產生該操作性使用者密鑰K_{OCU}，而係在該使用者用戶端16中產生該操作性使用者密鑰K_{OCU}且而後將其安全地傳遞至該攝影機10。因此，該使用者用戶端16可將該相同的操作性使用者密鑰K_{OCU}傳遞至若干不同的攝影機10。

根據一第二替代實施例，仍然在該攝影機10中產生該操作性使用者密鑰K_{OCU}。然而，該操作性使用者密鑰K_{OCU}之該產生係基於全部攝影機之間共用的一共同的秘密密鑰以及識別該使用者想要在他/她的系統中控制之各攝影機的一攝影機唯一的識別符(例如一攝影機序號)。在各攝影機10中產生該操作性使用者密鑰K_{OCU}之步驟期間，該使用者將識別該使用者想要在他/她的系統中控制之各攝影機的該攝影機唯一的識別符提供給該攝影機10，且因此確保將在全部攝影機中產生相同的唯一秘密密鑰。若該使用者用戶端未在該產生程序期間將該攝影機唯一的識別符提供給該攝影機，則該攝影機將拒絕註冊。

根據一第三替代實施例，其使用替代實施例一與替代實施例二之一組合。

圖3繪示根據本發明之一實施例的一具網路功能的數位視訊攝影機10。該具網路功能的數位視訊攝影機經配置以連接至一數位網路。該數位網路可為(例如)由一服務提供商管理之一監視系統的部分。該網路攝影機10包括一密鑰產生構件50、一指示構件52、一檢查構件54、一加密構件56、一數位網路模組58、一重設構件60、一密鑰儲存構件

62、一輸入/輸出(I/O)埠64、一影像感測器66及一影像處理器68。

在該具網路功能的數位視訊攝影機10中產生媒體資料(例如數位視訊影像)再將該媒體資料提供給該輸入/輸出埠64可描述如下。該影像感測器66(例如一CCD或一CMOS)擷取數位影像。將所擷取之數位影像轉送至該影像處理器68，其中處理該等數位視訊影像。可將經處理之數位視訊影像轉送至壓縮單元(未展示)，其中根據一預定義標準(諸如H.264、JPEG、M-JPEG或MPEG)壓縮該等數位視訊影像。而後，(可能經壓縮的)數位視訊或影像信號在被轉送至經配置以傳輸且接收數位信號之該數位網路模組58之前由該加密構件56進行加密，其中處理經加密的數位視訊或影像信號(亦即經加密的媒體資料)且準備經由該輸入/輸出埠64透過一數位網路傳輸。

應注意，該具網路功能的數位視訊攝影機亦可經調適以記錄音訊資料。該音訊資料亦可在經由該數位網路模組58傳輸之前由該加密構件56進行加密。

該加密構件56藉由與該操作性使用者密鑰K_{OCU}相關之該媒體加密/解密密鑰來加密該媒體資料(亦即音訊資料及視訊或影像資料)。根據上述內容，藉由憑藉與該操作性使用者密鑰K_{OCU}相關之該媒體加密/解密密鑰來加密該媒體資料，僅該使用者可存取該媒體資料，這是因為該服務提供商不知道該操作性使用者密鑰K_{OCU}。另外根據以上內容，替代地可使用該共同密鑰K_C來保護該媒體資料(亦即

音訊資料及視訊或影像資料)。藉由使用該共同密鑰K_C來保護該媒體資料，該使用者與該服務提供商兩者皆可存取該媒體資料，這是因為該使用者與該服務提供商兩者皆知道該共同密鑰K_C。

此外，由該攝影機10註冊或產生之元資料(諸如時戳、視訊觸發資訊、警報資料或相似物)可由該加密構件56進行加密。因此，該數位網路模組58係經配置以傳輸經加密的元資料。根據上述內容，該元資料可(例如)藉由與該共同密鑰K_C相關之該元資料加密/解密密鑰而加密。藉由憑藉該元資料加密/解密密鑰而加密該元資料，該使用者與該服務提供商兩者皆可存取該元資料，這是因為該使用者與該服務提供商兩者皆知道該共同密鑰K_C。因此，該服務提供商可存取該元資料且因此(例如)能夠對該使用者提供對於警報及記錄之一高效率的搜尋服務。

該操作性使用者密鑰K_{OCU}及該共同密鑰K_C係由該密鑰產生構件50產生。該密鑰產生構件50可進一步經配置以產生該初始使用者密鑰K_{ICU}及/或服務提供商密鑰K_{SP}。該初始使用者密鑰K_{ICU}、該操作性使用者密鑰K_{OCU}、該共同密鑰K_C及服務提供商密鑰K_{SP}係使用一安全的密鑰產生程序而產生。一安全的密鑰產生程序係在防止秘密資訊洩露給相同平台上執行之不安全的軟體或防止透過直接實體篡改裝置而洩露之一受保護的執行環境(硬體及/或軟體)中執行。

該等所產生之密鑰係儲存在該密鑰儲存構件62中。由(例如)該攝影機10製造商(參見上文)產生之該主密鑰K_M亦

儲存在該密鑰儲存構件62中。

根據上文，可使用一適當的第一單向函數f_1自該主密鑰K_M推導該初始使用者密鑰K_{ICU}，亦即$K_{ICU}=f_1(K_M)$，使得在已知該初始使用者密鑰K_{ICU}之情況下，將不可計算推導該主密鑰K_M。類似地，使用一適當的第二單向函數f_2自該主密鑰K_M推導該服務提供商密鑰K_{SP}，亦即$K_{SP}=f_2(K_M)$，使得在已知該服務提供商密鑰K_{SP}之情況下，將不可計算推導該主密鑰K_M。此外，建構適當的第一單向函數f_1及第二單向函數f_2，使得對於額外的第三單向函數f_3及第四單向函數f_4而言，該共同密鑰K_C可根據下式推導：$K_C=f_3(K_{ICU})=f_4(K_{SP})$。因此，可藉由一第三單向函數$f_3$自該初始使用者密鑰$K_{ICU}$推導該共同密鑰$K_C$，亦即$K_C=f_3(K_{ICU})$，或替代地，可藉由一第四單向函數$f_4$自該服務提供商密鑰$K_{SP}$推導該共同密鑰$K_C$，亦即$K_C=f_4(K_{SP})$。該第三單向函數($f_3$)及該第四單向函數($f_4$)係經配置以產生無關於該共同密鑰$K_C$係自該非公開的初始使用者密鑰$K_{ICU}$或自該服務提供商密鑰$K_{SP}$推導的一相同的共同密鑰$K_C$，亦即$K_C=f_3(K_{ICU})=f_4(K_{SP})$。

此外，根據上文，該服務提供商(呈該服務提供商管理伺服器17之形式)具有服務提供商密鑰K_{SP}，且該使用者(例如呈該使用者用戶端16之形式)具有該初始使用者密鑰K_{ICU}。

在存取該攝影機10之前，該使用者需要在該攝影機10上鑑認其自身為該使用者。在該鑑認期間，建立該使用者用戶端16與該攝影機10之間的一鑑認關係。該使用者係藉由

自該使用者用戶端16發送包含基於該初始使用者密鑰K_{ICU}之資訊的一鑑認訊息至該攝影機10而鑑認。該攝影機係藉由自該攝影機10發送一視訊序列至該使用者用戶端16以驗證該視訊序列被所期望之攝影機10即時擷取，且自該使用者用戶端16發送作為該攝影機鑑認之確認的一確認訊息至該攝影機10而鑑認。

在已建立該攝影機10與該使用者用戶端16之間的該鑑認關係時，該檢查構件54係經配置以檢查該攝影機10中是否已設定該操作性使用者密鑰K_{OCU}。此可(例如)藉由檢查該指示構件52是否已指示該操作性使用者密鑰K_{OCU}已被設定而執行。

此外，若自該檢查構件54所執行之該檢查的結果係該攝影機10中已設定該操作性使用者密鑰K_{OCU}，則將一訊息發送至該使用者用戶端，從而指示該攝影機10中已設定該操作性使用者密鑰K_{OCU}。在此情況下，該使用者可藉由刪除該攝影機10中所設定之該操作性使用者密鑰K_{OCU}而重設該攝影機10之安全設定，並且重新開始該鑑認程序。或者，在此情況下，該使用者可藉由刪除該攝影機10中所設定之該操作性使用者密鑰K_{OCU}而重設該攝影機10之安全設定，並且獲取待於該攝影機10中產生且設定之一新的操作性使用者密鑰K_{OCU}(參見上文)。該重設可藉由該重設構件60執行。該重設構件60係經配置以重設該設定操作性使用者密鑰K_{OCU}。該重設構件60可包括一重設按鈕62。

或者，若自該檢查構件54所執行之該檢查的結果係該攝

影機10中尚未設定該操作性使用者密鑰K_{OCU}，則該密鑰產生構件50產生該操作性使用者密鑰K_{OCU}。此外，當產生該操作性使用者密鑰K_{OCU}時，藉由該密鑰儲存構件62設定該操作性使用者密鑰K_{OCU}，以及由該指示構件52指示在該攝影機中已設定該操作性使用者密鑰K_{OCU}。因此，該指示構件52係經配置以指示是否已產生該操作性使用者密鑰K_{OCU}。根據一實施例，該指示構件52可經配置以在若已產生該操作性使用者密鑰K_{OCU}時刪除該初始使用者密鑰K_{ICU}而不再使用。或者，該指示構件52可經配置以設定指示已產生該操作性使用者密鑰K_{OCU}之一旗標。

在該攝影機中產生並設定該操作性使用者密鑰K_{OCU}之後，該操作性使用者密鑰K_{OCU}被發送至該使用者用戶端16，且因此被發送至該使用者。僅該操作性使用者密鑰K_{OCU}之擁有者將具有對該攝影機10及由該攝影機10產生之媒體資料的完全的存取權力。

【圖式簡單說明】

圖1係根據本發明之一監視系統之一實施例的一示意圖；

圖2係產生安全相關密鑰及加密密鑰以及加密由一攝影機註冊之媒體資料及元資料的程序之一示意流程圖；及

圖3係根據本發明之一實施例之一攝影機的一示意圖式。

【主要元件符號說明】

10　　網路視訊攝影機

11	私用網路
12	網際網路
13	網路位址轉換器(NAT)
14	防火牆
15	本地儲存單元
16	使用者用戶端
17	服務提供商管理伺服器
18	服務提供商儲存單元
19	服務提供商網路
50	密鑰產生構件
52	指示構件
54	檢查構件
56	加密構件
58	數位網路模組
60	重設構件
62	密鑰儲存構件
64	輸入/輸出(I/O)埠
66	影像感測器
68	影像處理器

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：99120147

※ 申請日：99.6.21 ※IPC 分類：G06F 21/64 (2013.01)
H04N 1/18 (2006.01)

一、發明名稱：（中文/英文）

用於限制存取由攝影機產生的媒體資料的方法

METHOD FOR RESTRICTING ACCESS TO MEDIA DATA GENERATED BY A CAMERA

二、中文發明摘要：

本揭示內容係關於一種用於限制存取由一攝影機(10)產生的媒體資料的方法。該方法包括：在該攝影機(10)中設定一非公開的初始使用者密鑰(K_{ICU})，將該初始使用者密鑰(K_{ICU})提供給一使用者用戶端(16)，藉由自該使用者用戶端(16)發送包含基於該初始使用者密鑰(K_{ICU})之資訊的一鑑認訊息至該攝影機(10)而建立該使用者用戶端(16)與該攝影機(10)之間的一鑑認關係，檢查該攝影機(10)中是否已設定一操作性使用者密鑰(K_{OCU})，及回應於檢查該攝影機(10)中是否已設定該操作性使用者密鑰(K_{OCU})之該動作而僅在若未設定該操作性使用者密鑰(K_{OCU})時執行以下動作a)至d)：a)獲取一操作性使用者密鑰(K_{OCU})；b)在該攝影機(10)中設定該操作性使用者密鑰(K_{OCU})；c)將該操作性使用者密鑰(K_{OCU})發送至該使用者用戶端(16)；及d)在該攝影機(10)中指示該操作性使用者密鑰(K_{OCU})已被設定。該方法進一步包括在該攝影機(10)中設定與該操作性

使用者密鑰(K_{OCU})相關之一媒體資料加密/解密密鑰，使用該媒體資料加密密鑰來加密由該攝影機(10)註冊之媒體資料，及將經加密之媒體資料發送至一服務提供商管理伺服器(17)。

三、英文發明摘要：

The disclosure relates to a method for restricting access to media data generated by a camera (10). The method, comprises: setting a non-public initial user key (K_{ICU}) in the camera (10), providing a user client (16) with the initial user key (K_{ICU}), establishing an authenticated relation between the user client (16) and the camera (10) by sending an authentication message including information based on the initial user key (K_{ICU}) from the user client (16) to the camera (10), checking if an operational user key (K_{OCU}) is set in the camera (10), and performing, in response to the act of checking if the operational user key (K_{OCU}) is set in the camera (10), the acts a) - d) only if the operational user key (K_{OCU}) is not set: a) acquiring an operational user key (K_{OCU}), b) setting the operational user key (K_{OCU}) in the camera (10), c) sending the operational user key (K_{OCU}) to the user client (16), and d) indicating in the camera (10) that the operational user key (K_{OCU}) is set. The method further comprises setting, in the camera (10), a media data encryption/decryption key associated with the operational user key (K_{OCU}), encrypting media data registered by the camera (10) using the media data encryption key, and sending the encrypted media data to a service provider management server (17).

八、圖式：

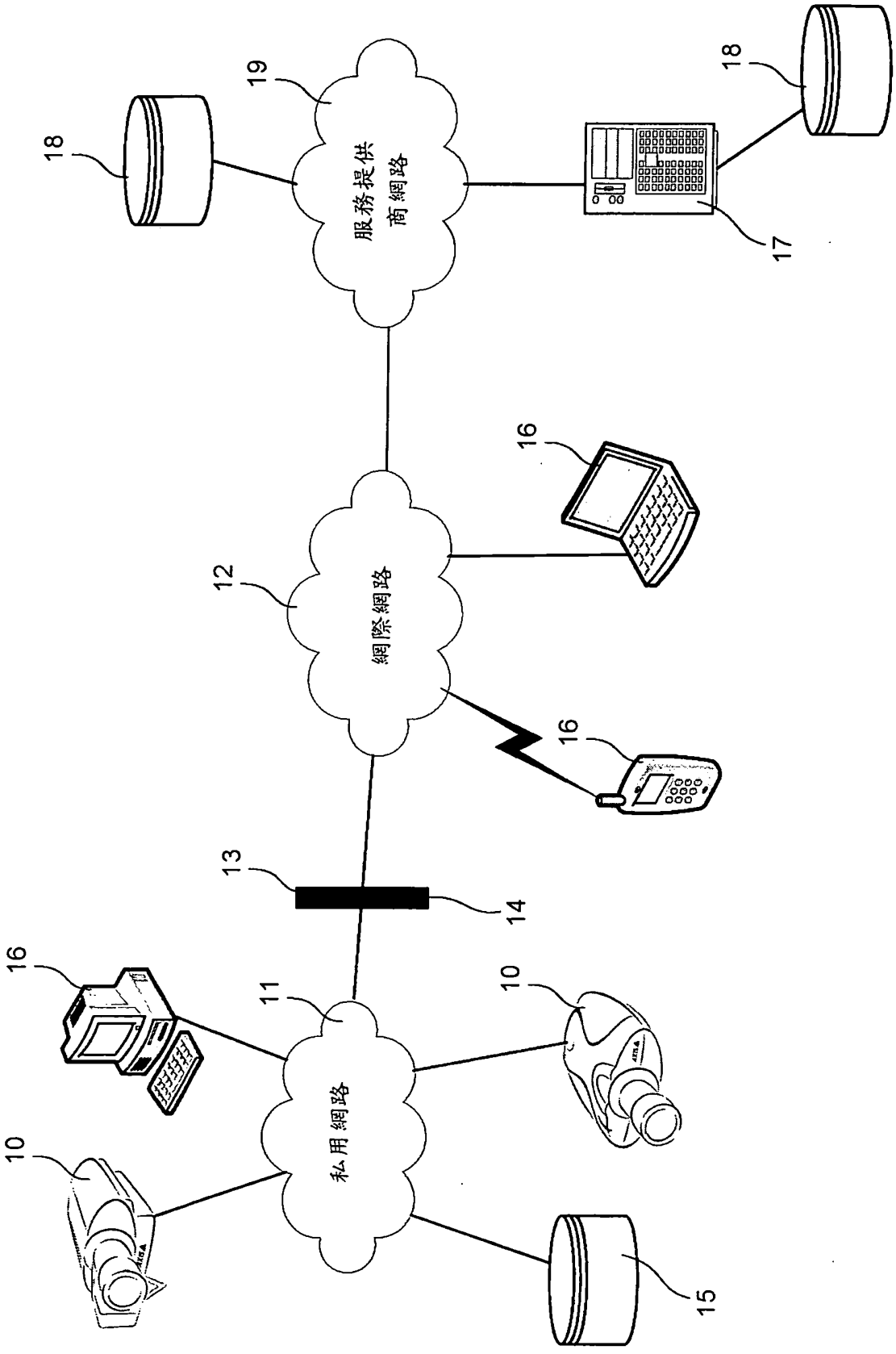

圖 1

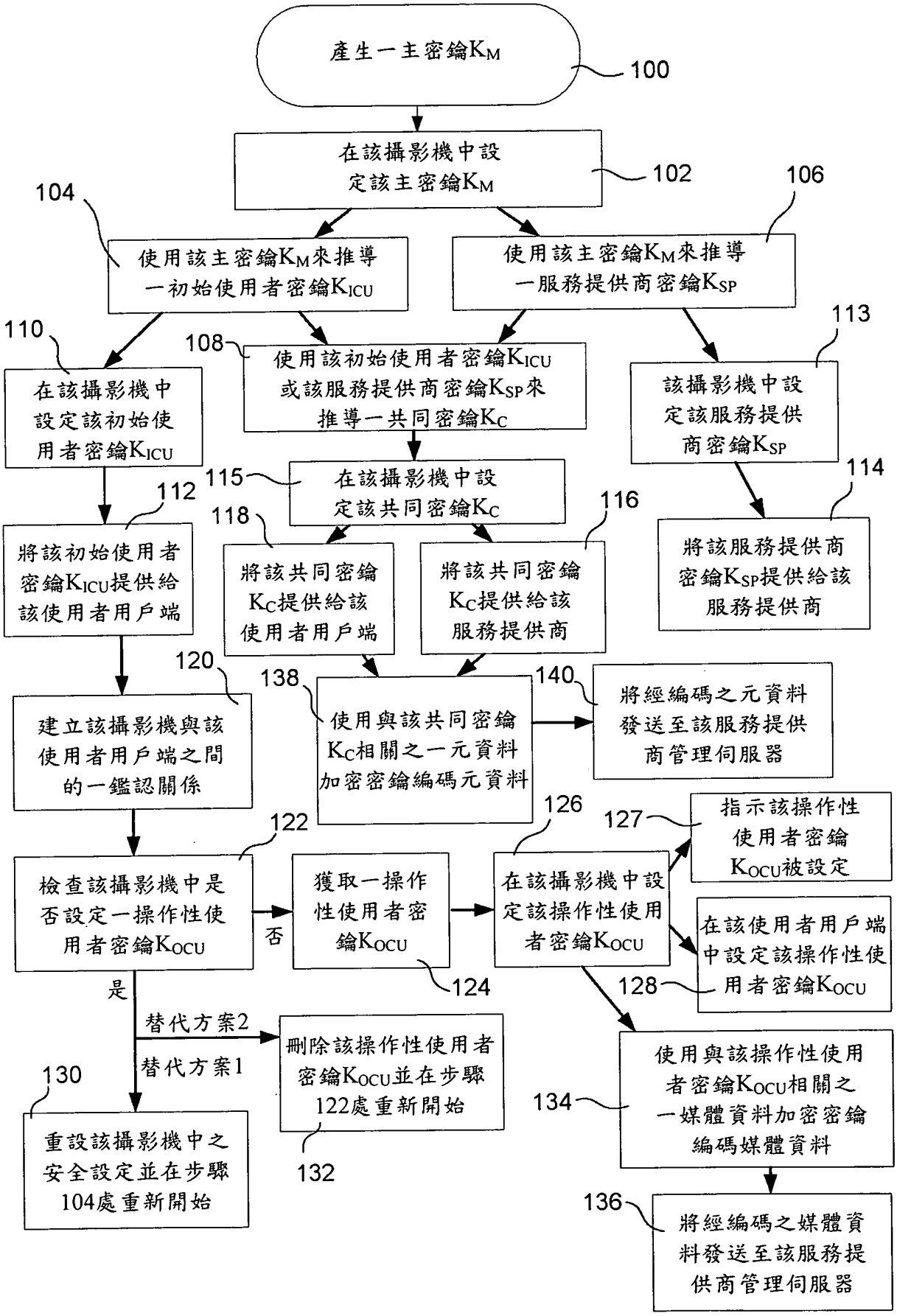
產生一主密鑰K_M
100
在該攝影機中設定該主密鑰K_M
102
104
106
使用該主密鑰K_M來推導一初始使用者密鑰K_{ICU}
使用該主密鑰K_M來推導一服務提供商密鑰K_{SP}
110
108
113
在該攝影機中設定該初始使用者密鑰K_{ICU}
使用該初始使用者密鑰K_{ICU}或該服務提供商密鑰K_{SP}來推導一共同密鑰K_C
該攝影機中設定該服務提供商密鑰K_{SP}
115
114
在該攝影機中設定該共同密鑰K_C
112
118
116
將該初始使用者密鑰K_{ICU}提供給該使用者用戶端
將該共同密鑰K_C提供給該使用者用戶端
將該共同密鑰K_C提供給該服務提供商
將該服務提供商密鑰K_{SP}提供給該服務提供商
120
138
140
建立該攝影機與該使用者用戶端之間的一鑑認關係
使用與該共同密鑰K_C相關之一元資料加密密鑰編碼元資料
將經編碼之元資料發送至該服務提供商管理伺服器
122
126
127
檢查該攝影機中是否設定一操作性使用者密鑰K_{OCU}
否
獲取一操作性使用者密鑰K_{OCU}
在該攝影機中設定該操作性使用者密鑰K_{OCU}
指示該操作性使用者密鑰K_{OCU}被設定
是
124
128
在該使用者用戶端中設定該操作性使用者密鑰K_{OCU}
替代方案2
替代方案1
130
134
刪除該操作性使用者密鑰K_{OCU}並在步驟122處重新開始
使用與該操作性使用者密鑰K_{OCU}相關之一媒體資料加密密鑰編碼媒體資料
132
136
重設該攝影機中之安全設定並在步驟104處重新開始
將經編碼之媒體資料發送至該服務提供商管理伺服器

圖 2

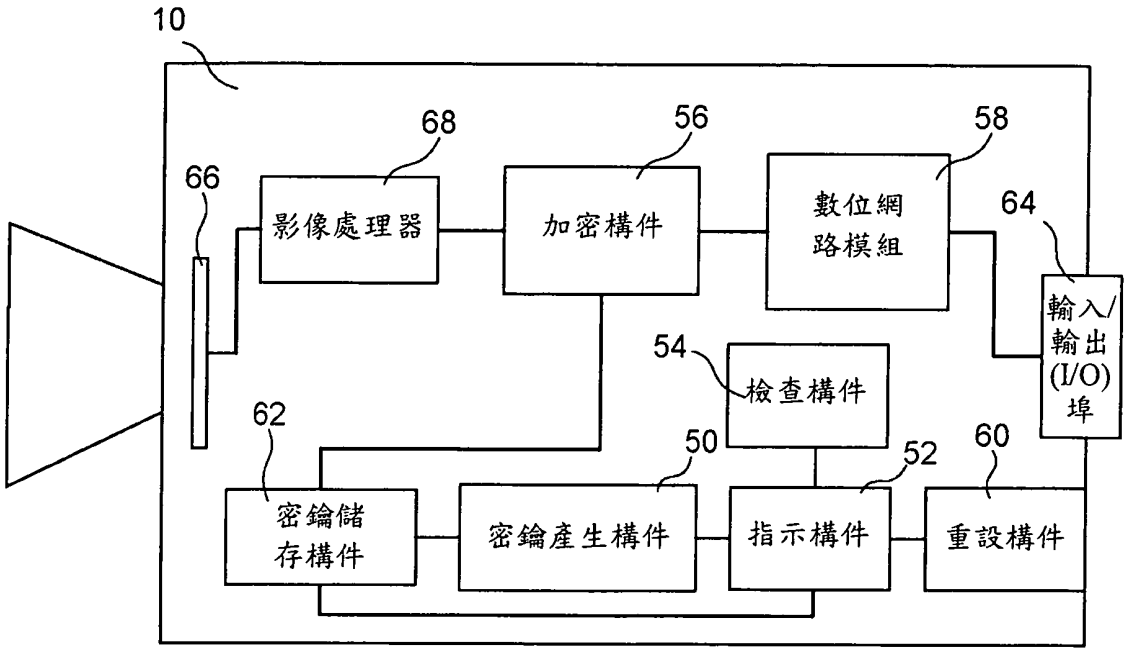
10
68
56
58
66
影像處理器
加密構件
數位網路模組
64
輸入/輸出(I/O)埠
54
檢查構件
62
50
52
60
密鑰儲存構件
密鑰產生構件
指示構件
重設構件

圖 3

四、指定代表圖：

(一)本案指定代表圖為：第(1)圖。

(二)本代表圖之元件符號簡單說明：

10	網路視訊攝影機
11	私用網路
12	網際網路
13	網路位址轉換器(NAT)
14	防火牆
15	本地儲存單元
16	使用者用戶端
17	服務提供商管理伺服器
18	服務提供商儲存單元
19	服務提供商網路

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

七、申請專利範圍：

1. 一種用於限制存取由一攝影機(10)產生的媒體資料的方法，該方法包括：

在該攝影機(10)中設定一非公開(non-public)的初始使用者密鑰(K_{ICU})；

將該初始使用者密鑰(K_{ICU})提供給一使用者用戶端(16)；

藉由自該使用者用戶端(16)發送包含基於該初始使用者密鑰(K_{ICU})之資訊的一鑑認(authenticated)訊息至該攝影機(10)而建立該使用者用戶端(16)與該攝影機(10)之間的一鑑認關係；

檢查該攝影機(10)中是否已設定一操作性使用者密鑰(K_{OCU})；及

回應於檢查該攝影機(10)中是否已設定該操作性使用者密鑰(K_{OCU})之該動作而僅在若未設定該操作性使用者密鑰(K_{OCU})時執行以下動作a)至d)：

a)獲取一操作性使用者密鑰(K_{OCU})，

b)在該攝影機(10)中設定該操作性使用者密鑰(K_{OCU})，

c)在該使用者用戶端(16)中設定該操作性使用者密鑰(K_{OCU})，及

d)在該攝影機(10)中指示該操作性使用者密鑰(K_{OCU})已被設定；

在該攝影機(10)中設定與該操作性使用者密鑰(K_{OCU})

相關之一媒體資料加密/解密密鑰；

使用該媒體資料加密密鑰來加密由該攝影機(10)註冊之媒體資料；及

將經加密之該媒體資料發送至一服務提供商管理伺服器(17)。

2. 如請求項1之方法，其進一步包括藉由一任意的使用者用戶端(16)經由該服務提供商管理伺服器(17)擷取媒體資料及使用該媒體加密/解密密鑰來解密所擷取之該媒體資料的動作。

3. 如請求項1或2之方法，其進一步包括：

獲取將在該攝影機(10)、該使用者用戶端(16)與一服務提供商管理伺服器(17)之間共用的一共同密鑰(K_C)；

在該攝影機(10)中設定該共同密鑰(K_C)；

對該使用者用戶端(16)且對該服務提供商管理伺服器(17)提供該共同密鑰(K_C)；

使用與該共同密鑰(K_C)相關之一元資料加密/解密密鑰來加密由該攝影機(10)註冊之元資料；及

將經加密之該元資料發送至該服務提供商管理伺服器(17)。

4. 如請求項1之方法，其進一步包括：

獲取一服務提供商密鑰(K_{SP})；及

對該服務提供商管理伺服器(17)提供該服務提供商密鑰(K_{SP})，其中該服務提供商密鑰(K_{SP})係用於保證僅該服務提供商管理伺服器(17)可存取諸服務提供商組態功

能。

5. 如請求項1之方法，其進一步包括在若該操作性使用者密鑰(K_{OCU})已被設定時指示該操作性使用者密鑰(K_{OCU})已被設定。

6. 如請求項1或5中任一項之方法，其中在該攝影機(10)中指示該操作性使用者密鑰(K_{OCU})已被設定之該動作包括刪除該初始使用者密鑰(K_{ICU})而不再使用。

7. 如請求項1之方法，其進一步包括：

在該攝影機(10)中設定一主密鑰(K_M)；

且其中在該攝影機中設定該非公開的初始使用者密鑰(K_{ICU})之該動作包括：藉由使用一第一單向函數(f_1)自該主密鑰(K_M)推導該非公開的初始使用者密鑰(K_{ICU})，亦即$K_{ICU}=f_1(K_M)$，而獲取該非公開的初始使用者密鑰(K_{ICU})。

8. 如請求項4之方法，其進一步包括在該攝影機(10)中設定一主密鑰(K_M)，其中在該攝影機中設定該非公開的初始使用者密鑰(K_{ICU})之該動作包括：藉由使用一第一單向函數(f_1)自該主密鑰(K_M)推導該非公開的初始使用者密鑰(K_{ICU})，亦即$K_{ICU}=f_1(K_M)$，而獲取該非公開的初始使用者密鑰(K_{ICU})，且其中獲取該服務提供商密鑰(K_{SP})之該步驟包括：使用一第二單向函數(f_2)自該主密鑰(K_M)推導該服務提供商密鑰(K_{SP})，亦即$K_{SP}=f_2(K_M)$。

9. 如請求項8之方法，其進一步包括：

獲取待在該攝影機(10)、該使用者用戶端(16)與一服

務提供商管理伺服器(17)之間共用的一共同密鑰(K_C)；

在該攝影機(10)中設定該共同密鑰(K_C)；

對該使用者用戶端(16)且對該服務提供商管理伺服器(17)提供該共同密鑰(K_C)；

使用與該共同密鑰(K_C)相關之一元資料加密/解密密鑰來加密由該攝影機(10)註冊之元資料；及

將經加密之該元資料發送至該服務提供商管理伺服器(17)；

其中獲取該共同密鑰(K_C)之該步驟包括：使用一第三單向函數(f_3)自該非公開的初始使用者密鑰(K_{ICU})推導該共同密鑰(K_C)，或使用一第四單向函數(f_4)自該服務提供商密鑰(K_{SP})推導該共同密鑰(K_C)，其中該第三單向函數(f_3)及該第四單向函數(f_4)係經配置以產生無關於該共同密鑰(K_C)係自該非公開的初始使用者密鑰(K_{ICU})或自該服務提供商密鑰(K_{SP})推導的一相同的共同密鑰(K_C)，亦即$K_C=f_3(K_{ICU})=f_4(K_{SP})$。

10. 如請求項1之方法，其中建立該使用者用戶端(16)與該攝影機(10)之間的該鑑認關係之該動作進一步包括：在執行藉由自該使用者用戶端(16)發送包含基於該初始使用者密鑰(K_{ICU})之資訊的一鑑認訊息至該攝影機(10)而鑑認該使用者用戶端(16)之後，藉由自該攝影機(10)發送一視訊序列至該使用者用戶端(16)以驗證該視訊序列被所期望(intended)之攝影機(10)即時擷取、且藉由自該使用者用戶端(16)發送作為該攝影機鑑認之確認的一確認訊

息至該攝影機(10)而鑑認該攝影機(10)。

11. 一種網路攝影機，該網路攝影機經配置以編碼由該攝影機註冊之媒體資料，該網路攝影機包括：

一密鑰產生構件(50)，其經配置以使用一安全的密鑰產生程序來產生一初始使用者密鑰(K_{ICU})或一操作性使用者密鑰(K_{OCU})；

一指示構件(52)，其經配置以指示是否已經產生該操作性使用者密鑰(K_{OCU})；

一檢查構件(54)，其經配置以檢查該指示構件(52)是否已經指示已經產生該操作性使用者密鑰(K_{OCU})，其中若該操作性使用者密鑰(K_{OCU})尚未被產生，則該密鑰產生構件(50)經配置以產生該操作性使用者密鑰(K_{OCU})；

一加密構件(56)，其經配置以使用與該操作性使用者密鑰(K_{OCU})相關之一媒體資料加密密鑰來加密由該攝影機註冊之媒體資料；及

一數位網路模組(58)，其經配置以傳輸經加密之該媒體資料。

12. 如請求項11之網路攝影機，其中該密鑰產生構件(50)係進一步經配置以產生一共同密鑰(K_C)，其中該加密構件(56)係進一步經配置以使用與該共同密鑰(K_C)相關之一元資料加密/解密密鑰來加密由該攝影機註冊之元資料，且其中該數位網路模組(58)係進一步經配置以傳輸經加密的該元資料。

13. 如請求項11之網路攝影機，其進一步包括經配置以重設

該產生的操作性使用者密鑰(K_{OCU})之一重設構件(60)。

14. 如請求項13之網路攝影機，其中該重設構件(60)包括一重設按鈕(62)。

15. 如請求項11之網路攝影機，其中該指示構件(52)係經配置以在若已產生該操作性使用者密鑰(K_{OCU})時刪除該初始使用者密鑰(K_{ICU})而不再使用。