行動媒體之機密資訊傳輸與共享機制

林珮瑜[1*]、藍文劭[2]
元智大學資訊傳播學系
[1]pylin@saturn.yzu.edu.tw、[2]s1046424@mail.yzu.edu.tw

摘要

隨著雲端網路的盛行及資訊科技的進步，行動裝置如智慧型手機與平版電腦廣泛使用於生活中，其拍照功能逐漸取代傳統相機，帶動新形態的社群分享及雲端儲存應用。針對行動裝置所拍攝之數位媒體，其共享與安全保護相當重要，然而目前相關研究技術相當缺乏且較少被探討。當行動裝置媒體於雲端進行儲存時，其個人的智慧財產權易受到威脅，故須有保護技術來保護拍攝的數位媒體。此外，考慮拍攝照片的社群分享特性，在照片進行共享時，若能額外傳輸雙方分享的機密資訊，將可有效提升使用者對媒體共享的新穎性與應用性。為了設計適用於行動裝置之資訊共享與保護技術，且考量行動裝置的低運算與即時性需求，本研究利用行動裝置內鍵之影像處理模組，來藏匿共享的機密資訊。方法有效利用影像直方圖運算，以即時還原出機密資訊，行動裝置不需額外安裝硬體設備，故技術適用於一般行動裝置及數位相機應用。在藏匿共享的機密資訊過程中，也不會破壞裝置媒體外觀的可視品質，滿足使用者對於行動裝置媒體的觀看與共享使用。

關鍵詞：機密分享、行動裝置、直方圖、不可察覺

Secret Communication and Sharing Mechanism for Mobile Media

Pei-Yu Lin[1*], Wen-Shao Lan[2]
[1, 2]Department of Information Communication, Yuan Ze University,
[1]pylin@saturn.yzu.edu.tw, [2]s1046424@mail.yzu.edu.tw

Abstract

Mobile devices, such as smart phone and tablet PC, are commonly used to capture a real-world scene instead of the traditional camera in recent decades. The interflow and share of the captured media over the cloud storages and social websites become the popular behavers via digital devices. These communicated and shared media have the piracy and illegal problems without proper protection. Nevertheless, the related protection techniques concerning the real-time mobile media are considerably rare. The conventional protection

* 通訊作者 (Corresponding author.)

schemes normally applied to protect the media based on the high efficiency platform (such as personal computer) with high computational complexity. Such protection algorithms are unsuitable for light-weight mobile devices. In this article, we proposed an efficient mechanism adopts the observation of inner operation of mobile devices to achieve the media secret sharing and ownership protection of the mobile media directly. The procedure is low computational complexity that can be applied to convey the secret information of the captured media via mobile devices.

Keywords: Secret sharing, mobile device, histogram operation, imperceptible

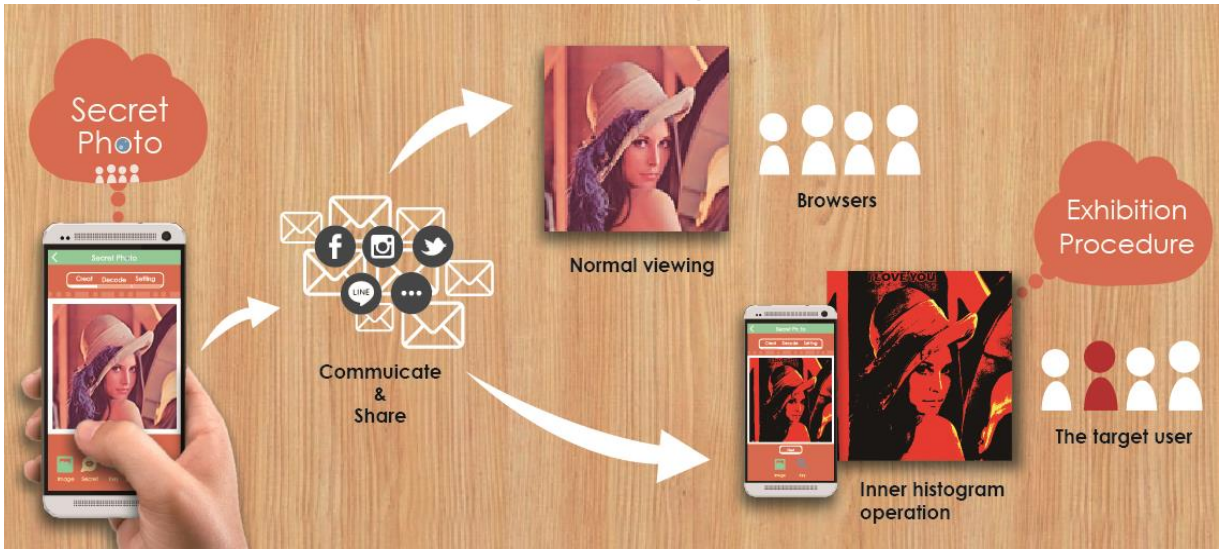
壹、前言

現今的行動裝置 (如智慧型手機、平板電腦)，功能越來越強大，內建的攝像功能不輸給一般相機，其便利性讓許多使用者習慣以行動裝置進行影片拍攝與數位錄影，逐漸取代傳統相機以及數位相機。行動裝置媒體的雲端傳輸以及社群分享，成為現代使用者的熱門應用趨勢，然而，其網路上的非法擷取途徑也跟著猖獗。在裝置媒體傳輸與共享受到威脅時，若沒有適當的保護機制，這些社群共享與雲端儲存媒體，容易被不法人士利用、竄改或複製，故必須有一套安全的防衛機制，以遏止非法行為的發生 [2][4][8][10]。

如何保護行動裝置所拍攝之數位媒體，提供機密共享與安全保護技術，對目前廣泛利用智慧行動裝置的使用者相當重要，然而針對行動裝置媒體所設計的保護技術較少被探討，其相關研究技術相當缺乏 [7]。基於上述安全應用考量，本論文針對行動裝置媒體，考量其於雲端進行儲存時，須有安全機制以保護拍攝的數位媒體。而數位媒體於社群分享時，須能額外傳輸雙方分享的機密資訊，以提升使用者對媒體共享的新穎性與價值性。故為了保護裝置媒體的所有權問題以及機密資訊分享，本研究技術將機密資訊嵌入至行動裝置所拍攝的數位媒體中，使用行動裝置通用的影像直方圖模組功能，調整影像色度，利用這種特性來將機密資訊隱藏於行動裝置媒體之色彩空間中 [1][3][6][7]。其嵌入機密資訊後的行動裝置媒體，在外觀上與原圖相同，一般使用者並不會察覺到任何異狀。在使用行動裝置進行影像傳輸時，可滿足使用者在媒體觀看與共享時的視覺品質。授權接收者可運用行動裝置來進行直方圖模組顯示運算，得到完整的機密分享資訊或宣示的所有權圖騰。

我們所設計之共享演算法可應用於行動裝置拍攝之靜態圖像以及動態影片，達到機密資訊的雲端傳輸保護與社群機密分享。技術利用普遍行動裝置內鍵之影像處理模組，故行動裝置不需要額外安裝硬體處理設備，可有效應用於智慧型手機、平板電腦以及數位相機。故使用者透過自己的行動裝置就能達到機密共享及所有權宣示的目的。本技術

架構可應用於一般行動裝置，達到保護的安全機制，圖一為機密資訊分享之示意圖。當使用者用行動裝置進行拍攝時，本技術可即時將機密資訊以不可察覺的方式嵌入拍攝的媒體內。其嵌入機密後的數位媒體，在人眼視覺上與原圖一致，故可於雲端進行傳輸儲存以及社群分享。當授權者欲顯示共享機密或所有權時，利用行動裝置之影像處理模組，可即時將隱藏的機密資訊進行顯示，透過人眼視覺可辨識機密資訊內容。



圖一：機密資訊分享流程示意圖

貳、研究方法

為了設計適用於常見行動裝置之媒體保護與共享機制，本方法考慮行動裝置與數位相機通用之內鍵影像處理模式，建置即時與低運算量之機密資訊共享技術。本技術能普及應用於一般的行動裝置，不論是智慧型手機、平板電腦或是數位相機，都能完成機密偽裝及機密分享的功能，對於生活在 E 世代的使用者而言，是相當實用的保護與分享應用。

2.1 最佳區域選擇運算

令 O 為行動裝置所拍攝的數位影像，以及 W 為一所有權或欲分享的機密資訊圖像。首先找尋 O 中最大的平滑區域，令此平滑區塊為 b，而 b 區塊之大小為 $M \times N$ 個像素 (Pixel)。由於 b 為彩色區塊，故計算 b 區塊的彩色平面 (Plane) 之像素平均值，令 b_R、b_G、b_B 分別為 b 區塊之 R (Red)、G (Green) 與 B (Blue) 色彩空間的像素平均值，其計算方法為：

$$\begin{cases} b_R = \dfrac{1}{M \times N} \sum_{i=1}^{M \times N} b_R(p_i), \\ b_G = \dfrac{1}{M \times N} \sum_{i=1}^{M \times N} b_G(p_i), \\ b_B = \dfrac{1}{M \times N} \sum_{i=1}^{M \times N} b_B(p_i). \end{cases} \tag{1}$$

其中 $b_R(p_i)$，$b_G(p_i)$與 $b_B(p_i)$ 分別代於 R、G 與 B 彩色平面之像素值 p_i，$i = 1, 2, \ldots, M \times N$。

令 b_c 為 b_R，b_G 與 b_B 中，平均值最小的平面，令其最小平均值為 m，$C \in R, G, B$。

2.2 不可視機密嵌入運算

為了將機密資訊圖像 W 嵌入至選定之 b 區塊，方法首先將 W 重新調整與 b 相同之 $M \times N$ 大小。其 b 與 W 可表示為：

$$b_C = \{ b_C(p_i) | \, b_C(p_i) = 0, 1, \ldots, 255, \quad \text{且 } i = 1, 2, \ldots, M \times N \}. \tag{2}$$

$$W = \{ W_i \mid W_i = 0, 1, \quad \text{且 } i = 1, 2, \ldots, M \times N \}. \tag{3}$$

上述 $W_i = 0$ 代表機密分享影像於位置 i 的顏色為白色像素，$W_i = 1$ 代表機密分享影像於影像位置 i 的顏色為黑色像素。

為了產生一個視覺上不容易察覺之偽裝影像，W 嵌入 b_c 之隱藏方式必須滿足下列方程式：

$$b'_C(p_i) = \begin{cases} m + 2, & \text{if } W_i = 0 \text{ and } b_C(p_i) < m + 2, \\ m, & \text{if } W_i = 1 \text{ and } b_C(p_i) > m. \end{cases} \tag{4}$$

$b'_C(p_i)$為嵌入 W_i 至 $b_C(p_i)$之後的偽裝像素值，$i = 1, 2, \ldots, M \times N$。

為了嵌入多個所有權顯示或機密資訊，以上述 2.1 相同演算法找尋 O 中之次佳平滑區塊，並重複 2.2 運算即可嵌入多機密分享資訊。最後，即可產生嵌入機密 W 之偽裝影像 O'。

2.3 機密資訊顯示運算

由於方法植基於行動裝置及數位相機普遍內鍵之影像處理功能，故授權使用者只需利用其行動裝置，快速透過影像直方圖模組運算，即可清楚的顯示機密分享資訊，不需要額外安裝影像解碼等設備，其低運算成本相當適用於行動裝置所拍攝媒體，達到即時保護與共享應用。

給予一共享的偽裝影像 O'，以及 m 值，其直方圖模組 $[\alpha,\beta]$ 之調整運算公式如下，

$$\alpha = m, \qquad \beta = m + 2. \tag{5}$$

當有多個所有權圖像或機密資訊時，則重複上述直方圖模組運算，可還原出其他部分的機密分享影像，透過人眼即可清楚辨視所有權宣示及共享機密內容。

在此，m 值可為裝置傳送者以機密傳輸方式，將 m 值給予授權接收者。然而，為方便裝置媒體之立即結合應用，其 m 值可有效利用目前常見之資訊隱藏方式，將一或多組 m 值，以可逆或不可逆的資訊隱藏技術 [5] [9] [11][12]，嵌入於 O 中。接受者可利用其金鑰擷取 m 值，以顯示所有權圖像及機密分享資訊。

參、實驗結果

本研究技術可有效應用於行動裝置所拍攝之數位靜態照片與動態影片，其測試之靜態照片如圖二所示。圖三為欲嵌入之所有權圖像與分享之機密資訊，所有權圖像如圖三(a)及三(b)，共享之機密資訊可利用 QR 碼產生 [13][14] 或任何機密分享圖像，如圖三(c)及三(d)。

(a) Bandon

(b) Lena

(c) Skyline arch

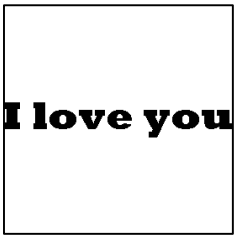
圖二：測試靜態影像, O

圖四為本方法應於行動裝置之實作結果，當智慧型手機拍攝照片時 (圖二(a))，可即時將圖三之所有權圖像與機密分享資訊，以不可察覺方式嵌入至照片內。嵌入後的偽裝影像，可於雲端進行儲存或利用社群軟體進行分享。其影像外觀與原始照片無異，故可有效提供使用者對照片內容的觀看及分享。唯授權接收者可利用金鑰 m 值，透過行動裝置的直方圖進行模組調整，便可立即將隱藏的所有權圖像與機密分享資訊，以人眼可辨識方式，顯示於媒體外觀。此影像模組調整相當快速且計算量低，故研究方法相當適用於低功率的行動裝置與數位相機設備。

(a) 所有權圖像 1

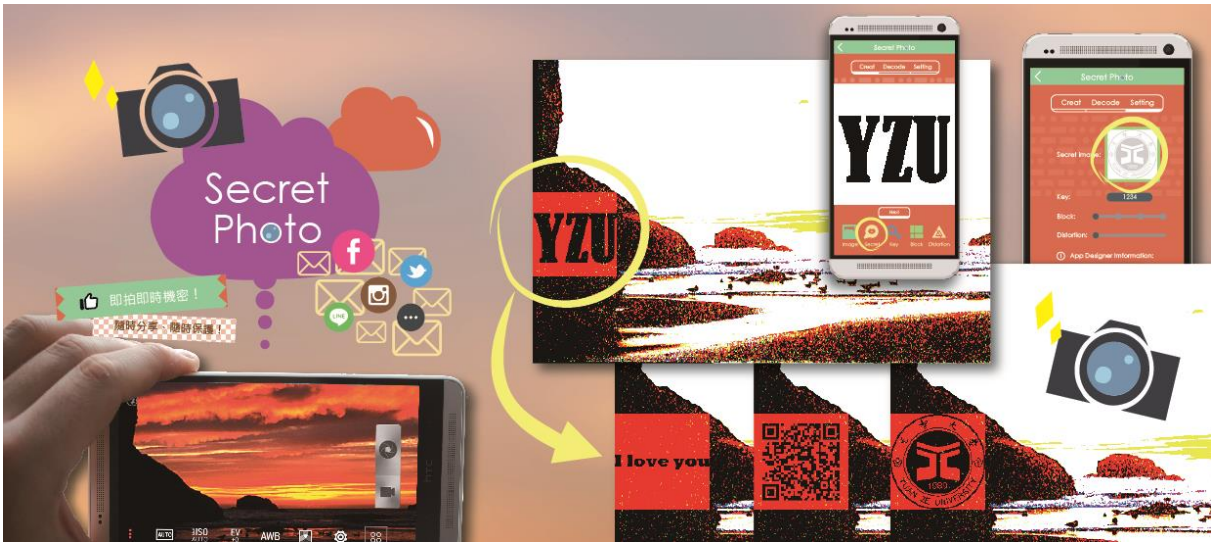
(b) 所有權圖像 2

(c) 機密分享資訊 1



(d) 機密分享資訊 2

圖三：所有權圖像與機密分享資訊, W



圖四：使用不同機密分享影像隱藏之示意圖

除了利用人眼視覺判斷偽裝影像的可視外觀，為了評估方法所產生之偽裝影像品質，我們利用 PSNR (peak signal-to-noise rate) 作為評估，計算原始影像與偽裝影像之間的相似數值，其計算公式如下：

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB} \tag{6}$$

在此，mean square error (MSE) 為計算一影像大小為 $O_H \times O_W$ 像素：

$$MSE = \frac{1}{O_H \times O_W}\sum_{i=1}^{O_H \times O_W}(p_i - p_i')^2 \tag{7}$$

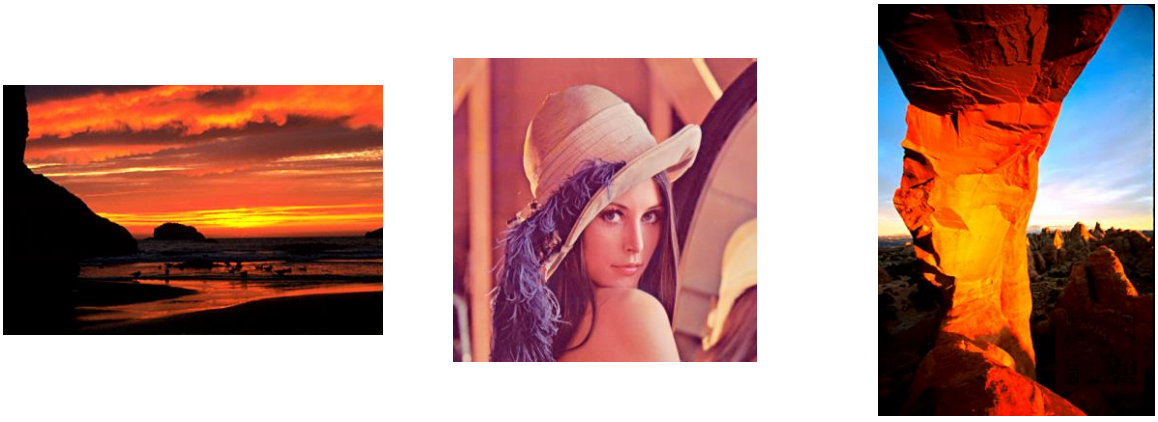
p_i 與 p'_i 分別代表原始影像與嵌入後偽裝影像之像素值。

透過 PSNR 評估方法來檢視我們所提出的行動裝置媒體保護機制之品質可行度，根

據表一可以明顯的看出此隱藏方法具有高度的隱密性。亦可從視覺上來觀察，其嵌入後之偽裝影像如圖五(a)所示。圖五(b)為將圖五(a)進行裝置之直方圖模組調整後的機密顯示結果。

表一：靜態影像以 PSNR 評估方法分析

原始測試影像	影像尺寸		PSNR 值 (dB)
	測試影像, *O*	所有權圖像\機密分享資訊, *W*	
Bandon	610×403	112×112	61.32
Lena	512×512	192×192	40.47
Skyline arch	400×594	112×112	44.56



(a) 嵌入不可察覺之偽裝影像

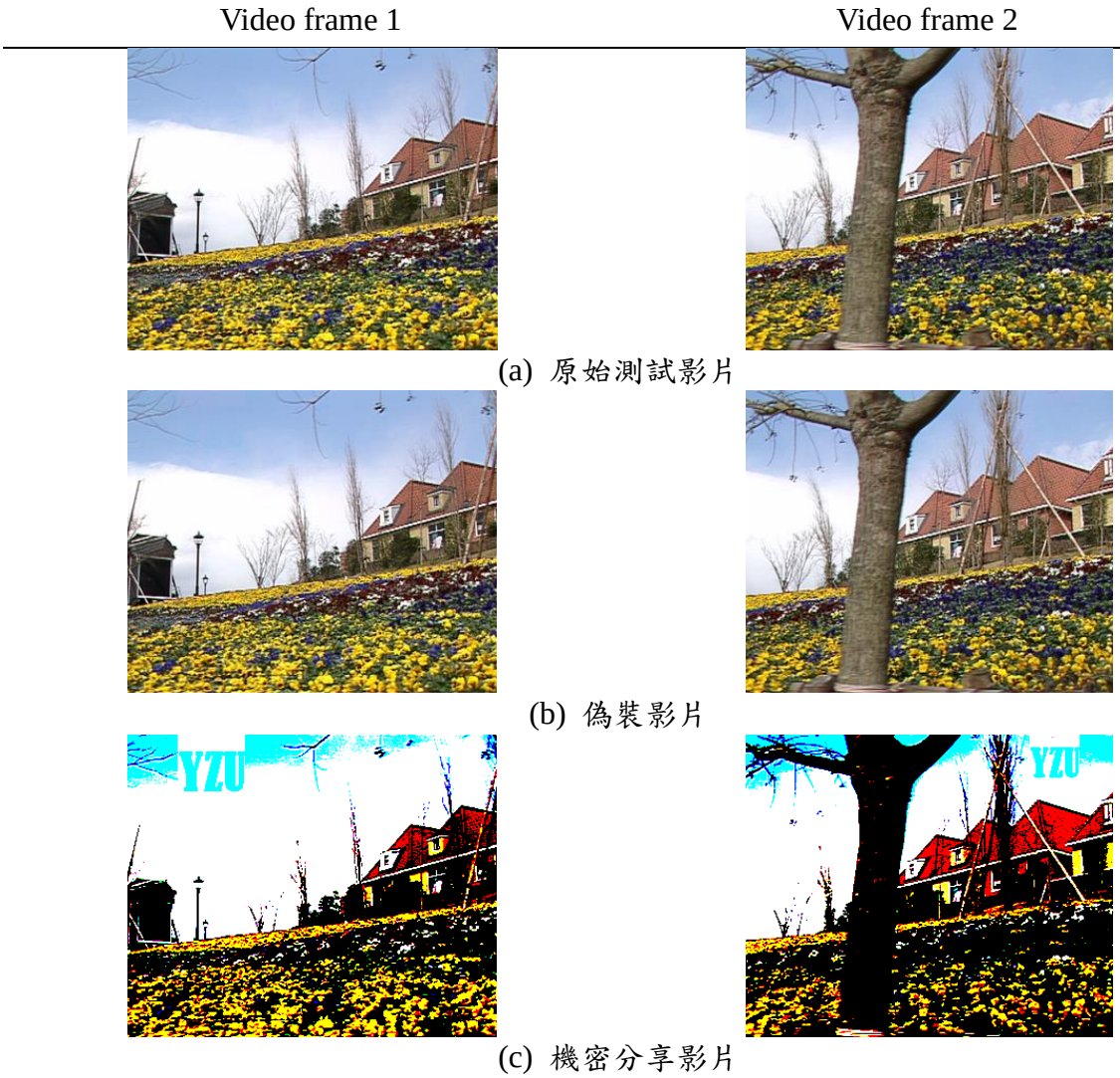
(b) 顯示之機密分享結果

圖五：偽裝影像及其顯示之機密影像比較

本研究方法除了應用在靜態影像，也可對動態影片進行機密資訊嵌入。圖六(a)為拍攝影片之連續畫面，frame 1 及 frame 2。由於研究方法可對影片動態偵測最大平滑區塊，故機密共享資訊的嵌入區域，也會隨影片的場景內容變換。

表二：動態影像以 PSNR 評估方法分析

原始測試影像	影像尺寸		PSNR 值 (dB)
	測試 frame, *O*	所有權圖像\機密分享資訊, *W*	
Video frame 1	352×288	64×64	51.48
Video frame 2	352×288	48×48	55.91



(a) 原始測試影片

(b) 偽裝影片

(c) 機密分享影片

圖六：動態影像與機密偽裝影像比較圖

表二為其影片 frame 相對應之 PSNR 值，PSNR 數值越高代表隱藏效果越好。一般而言，當 PSNR 數值大於 35 dB 時，其品質是不錯的。當 PSNR 數值小於 30 dB 時，代表人眼視覺可觀察到不良圖像品質，當值越低越不被人眼所接受。但 PSNR 評估方法只是個參考值，由於本架構針對行動裝置媒體之社群分享與雲端儲存，故主要還是以由人

眼視覺的觀察效果為主，以判別其隱藏品質的優劣。

技術之隱藏結果由表一與表二的 PSNR 值，可證實無論是靜態影像或是動態影片，其 PSNR 數值皆大於 40 dB，甚至高達 60 dB。由圖五及圖六的比較圖進行分析，人眼視覺幾乎是完全看不出機密分享影像潛藏的位置。透過人眼視覺無法察覺任何異樣，有效滿足良好的隱藏效果。再者並不是顏色越深的區域其隱藏效果越佳，只要平滑區域之間像素值的差異性越低，方法的隱蔽效果就會越好。

方法所提出之製作機密共享的偽裝影像過程，僅需要使用者的行動裝置即可操作，並且不會破壞原始媒體的可視品質。要擷取共享的機密資訊時也不需要額外安裝解碼裝置，運用行動裝置普遍都有的直方圖模組處理，即可完整的呈現出機密分享資訊。不僅是靜態的照片，動態影像也可利用相同的保護方法，來達到機密資訊傳輸與共享。且其低運算量適用於常見之行動裝置及數位相機，達到即時性的機密資訊保護與共享應用。

肆、結論

於現今人手一機的智慧型裝置 E 世代，加上社群通訊媒體的發展，裝置媒體的傳輸與共享必須受到保護，且在視覺上須能維護其可視品質與美感，以提升使用者接受度與應用廣度。本技術針對行動裝置與數位相機，設計可通用之保護機制，能滿足所有權宣示與機密共享需求外，其機密資訊也以人眼不可察覺方式完整的隱藏在媒體內，且不需要安裝任何額外設備，即可架構於行動裝置與數位相機，完成整個機制的機密保護與顯示操作。

[誌謝] Acknowledgment

This research was supported by the National Science Council, Taiwan, under contract No. NSC 102-2221-E-155-035-MY3 and MOST 104-3115-E-155-002.

參考文獻

[1] S. C. Chuang, C. H. Huang and J. L. Wu “Unseen visible watermarking,” *2007 IEEE International Conference on Image Processing*, vol. 3, pp. 261-264, 2007.

[2] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[3] C. H. Huang, S. C. Chuang, Y. L. Huang and J. L. Wu, "Unseen visible watermarking: a novel methodology for auxiliary information delivery via visual contents," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 2, pp. 193-206, 2009.

[4] A. Koz, C. Cigla and A. A. Alatan, "Watermarking of free-view video," *IEEE Transactions on Image Processing*, vol. 19, no. 7, pp. 1785-1797, 2010.

[5] X. Li, W. Zhang, X. Gui and B. Yang, "Efficient reversible data hiding based on multiple histograms modification," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 2016-2027, 2015.

[6] P. Y. Lin, "Imperceptible Visible Watermarking Based on Postcamera Histogram Operation," *Journal of Systems and Software*, vol. 95, pp. 194-208, 2014.

[7] P. Y. Lin and W. F. Hsieh, "Media Pattern Exhibition Mechanism via Mobile Devices," *Journal of Visual Communication and Image Representation*, vol. 25, no. 8, pp. 1856-1864, 2014.

[8] T. Y. Liu and W. H. Tsai, "Generic lossless visible watermarking—a new approach," *IEEE Transactions on Image Processing*, vol. 19, no. 5, pp. 1224-1235, 2010.

[9] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data Hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006.

[10] A. Swaminathan, M. Wu and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 101-117, 2008.

[11] J. Tian, "Reversible data embedding using difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.

[12] W. Zhang, X. Hu, X. Li and Y. Nenghai, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 294-304, 2015.

[13] Psytec QR code editor software, [Online]. Available: http://www.psytec.co.jp/docomo.html

[14] QR code, [Online]. Available: http://www.qrcode.com/en/index.html

[作者簡介] Biography

Pei-Yu Lin received the M.S. and Ph.D. degrees from National Chung Cheng University, Chiayi, Taiwan, in 2004 and 2009, respectively, both in computer science and information engineering.

Currently, she is an Associate Professor with the Department of Information Communication, Yuan Ze University, Taoyuan, Taiwan. Her research interests include image protection, data mining, and information security.

Wen-Shao Lan is currently pursuing her MS degree in Department of Information Communication, Yuan Ze University, Taoyuan, Taiwan. Her current research interests include image protection, and information security.