基於視覺密碼之彩色機密隱藏機制

戴維良[1*]、廖子鈞[2]
[1, 2] 中國文化大學資訊傳播學系
[1]dwl@ulive.pccu.edu.tw、[2]A1271469@ulive.pccu.edu.tw

摘要

傳統的加密法需要大量且複雜的運算才能將秘密訊息予以解密，然而視覺密碼學有別於其他加密機制，其利用秘密分享的概念，將秘密訊息藏至數張分享影像內，解密的動作不需要透過電腦的計算輔助，只需將數張分享影像利用人工加以疊合，藉由人眼便可解讀出機密訊息，在安全性方面，任何一方都無法從任何一張分享影像中解讀出隱藏的機密訊息。目前已有許多研究是透過產生不具意義的亂碼分享影像來確保分享影像不會洩露機密影像的資訊，而本研究透過半色調技術將視覺密碼隱藏在兩張具有意義的分享影像上，有意義的分享影像將不會造成有心人士的猜疑，不僅保有視覺密碼的特性，且亦可應用於複雜度高的彩色影像。

關鍵詞：視覺密碼、半色調、人類視覺系統

Color Secret Hiding Based on Visual Cryptography

Wei-Liang Tai[1*], Zi-Jun Liao[2]
[1, 2] Department of Information Communications, Chinese Culture University
[1]dwl@ulive.pccu.edu.tw, [2]A1271469@ulive.pccu.edu.tw

Abstract

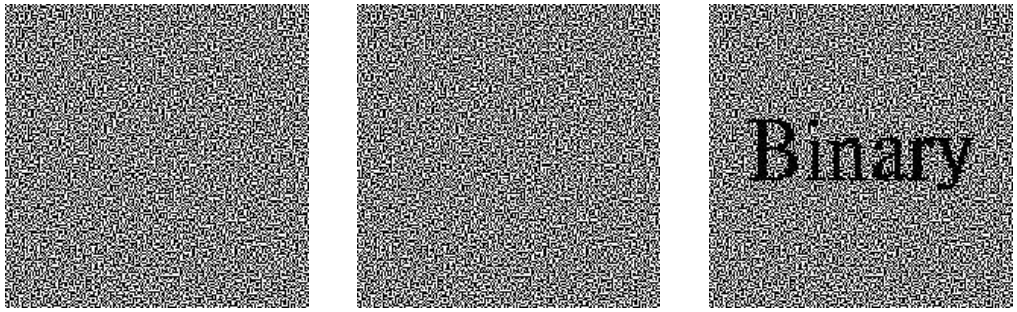
Visual cryptography is different from traditional cryptography. Neither time-consuming computation nor complex cryptographic knowledge is needed. Stacking is the only operation required to recover a secret image. Note that the individual image does not give the hackers any information about the secret image. Most researches tried to deal with non-meaningful color share images. Hence, we propose a color secret hiding method based on visual cryptography for hiding a color image in two meaningful color share images in this paper. The color decomposition approach and halftone technology are applied to cope with secret color images. Then the concept of the human visual system is utilized to generate two color meaningful share images.

* 通訊作者 (Corresponding author.)

Keywords: Visual cryptography, halftone, human visual system

壹、前言

傳統的加密法提供了相當高的安全性，例如 DES 和 RSA 等加密技術，然而其加解密的運算卻相當地複雜且需要龐大的運算，因此為了解決複雜的運算問題，在 1994 年，Noar 和 Shamir，提出 (t, n) 視覺秘密分享技術 [5] (Visual secret sharing, VSS) 或稱為視覺密碼學 (Visual cryptography)，其主要特色只要將多張分享偽裝影像重疊疊合，即可還原出機密影像，其解密的動作不需要經過任何複雜的計算，僅利用人類視覺系統的特性，就能透過人眼直接解讀機密影像上的資訊。如圖一所示，在 (t, n) 視覺秘密分享機制下，在總共 n 張分享影像中，必須大於或等於 t 分享影像重疊疊合才能解讀出機密影像，只要重疊的分享影像數量少於 t 張，便無法對其進行解密。然而，其只適用於黑白的二元影像，且所產生的分享影像是不具任何意義的，此外因產生分享影像的規則是以 4 個像素表示 1 個原像素的黑或白，所以分享影像與還原影像的尺寸都必須擴張成原影像的 4 倍大。

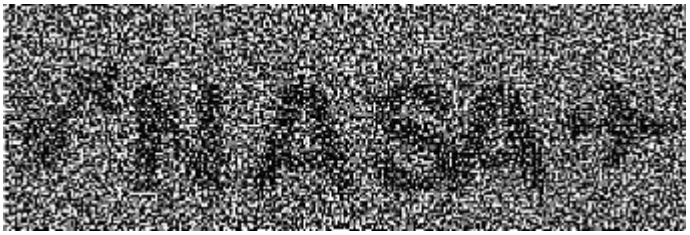


(a) 分享影像 1　(b) 分享影像 2　(c) 疊合影像

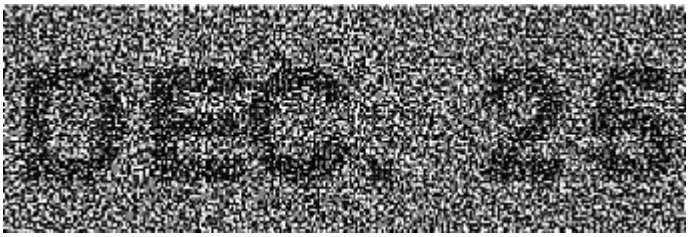
圖一：(2, 2) 視覺秘密分享技術

Noar 和 Shamir 方法所產生的分享影像是呈現亂碼樣式，不具有任何意義，然而如果可以把分享影像變成有意義的影像時，那將不會造成有心人士的猜疑，更具偽裝功能和美觀的效果了，在 2001 年，Hwang 和 Chang 提出一個改進的 (t, n) 視覺秘密分享機制 [3]，可以產生出兩張具有意義的分享影像，如圖二所示，其採用 3×3 像素擴張法而非 2×2 像素擴張法，使得黑白定義更加彈性，產生出有意義的分享影像。在 2003 年，Hou 提出了彩色視覺密碼分享機制 [2]，其原理是先將彩色影像轉換成 3 張對應 C、M、Y 三色的半色調分享影像，再依據視覺密碼分享規則，將影像分解成 6 張分享影像 C_1、M_1、Y_1 及 C_2、M_2、Y_2 後，接著把 C_1、M_1、Y_1 組成第一張分享影像，而 C_2、M_2、Y_2 組成第二張分享影像，其解密過程同樣無須經過電腦計算，只須將兩張分享影像重疊即可解密。然而，即便 Hou 的方法能處理灰階和彩色影

像，但其產生的分享影像卻是無意義的亂碼影像，這樣容易引起攻擊者的懷疑。



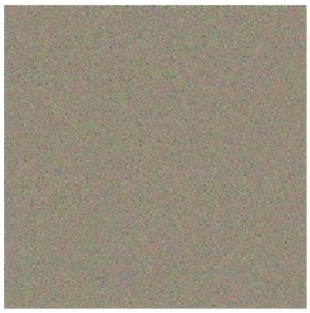
(a) 分享影像 1



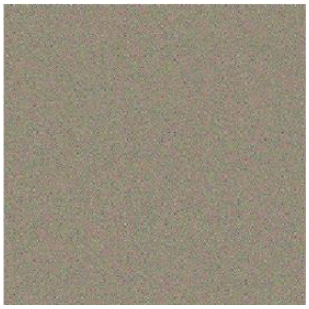
(b) 分享影像 2

(c) 疊合影像

圖二：有意義的偽裝圖像 [3]



(a) 分享影像 1



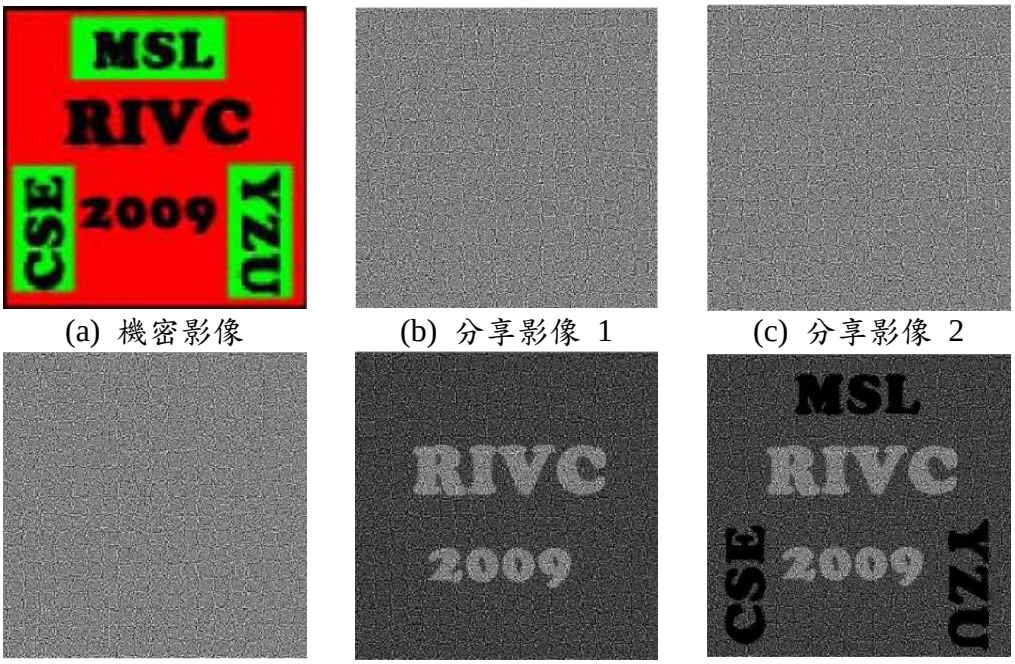
(b) 分享影像 2

(c) 疊合影像

圖三：(2, 2) 彩色視覺秘密分享技術 [2]

在視覺密碼學的發展上，大部分研究 [4][7][9][11] 著重於加強影像的對比度、像素擴張以及疊合影像的解析度，在 2009 年，Wang 提出了新的視覺密碼學架構 [8]，稱為 (2, n) 區域累進式視覺密碼技術 (Region incrementing visual cryptography, RIVC)，可以逐步重建機密在具有多個安全階層的單一影像，在區域累進式視覺密碼的架構下，將機密影像依據安全階層區分為多個區域，任何 t 張分享影像 ($2 \le t \le n+1$) 疊合，可以解密第 t-1 階區域的機密，如圖四所示，以 (2, 3) RIVC 架構為例，假設有兩階層 L_2, L_3

與兩機密 S_2, S_3，則任兩張分享影像在階層 L_2 中可以解密 S_2，任三張分享影像在階層 L_3 中可以解密 S_2, S_3。後續也有許多研究 [7][9] 基於累進式視覺密碼架構來改善效能與臨界值。在 2015 年，Dutta 與 Adhikari 提出了非單調 (Non-monotone) 視覺密碼學架構[1]，其利用了線性代數來產生分享影像，並使用 XOR 運算來解密機密，在 (t, n) 非單調視覺密碼學機制下，只有剛好 t 張分享影像疊合才可以解密出機密影像，當分享影像數量不為 t 時，則疊合結果之對比度為 0，無法疊合出機密影像。



(a) 機密影像　(b) 分享影像 1　(c) 分享影像 2

(d) 分享影像 3　(e) 任兩張分享影像疊合結果　(f) 三張分享影像疊合結果

圖四：(2, 3) 區域累進式視覺密碼技術 [8]

大部分的研究皆產生無意義的亂碼式分享影像，雖然亂碼形式可以保證從單一分享影像中無法得知機密的樣貌，但亂碼形式也給了攻擊者合理的猜疑機密的存在，給予攻擊的機會，為了解決這種缺點，我們將結合色彩分解的原理、半色調技術以及視覺密碼解密機制，提出加密機制將彩色機密影像隱藏在兩張有意義的彩色分享影像中，透過視覺密碼學的特性，解密過程不需要額外的計算，也能確保所產生分享影像亦不會洩漏機密影像的資訊。

貳、方法

為了將彩色機密影像隱藏在兩張有意義的彩色分享影像中，且利用視覺密碼學的疊合特性，解密過程不需要額外的計算，我們採用印刷 CMY 色彩空間以及半色調技術，

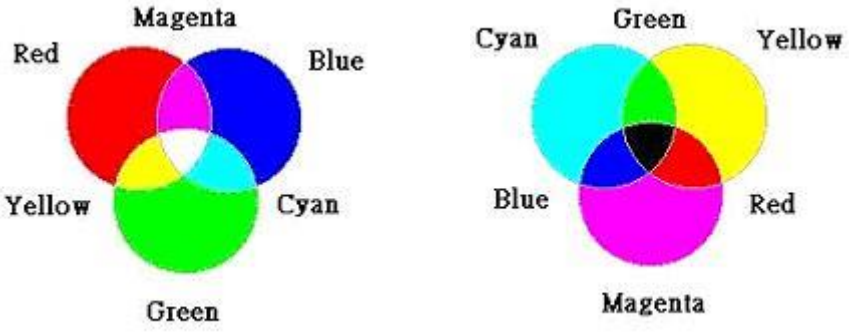
將分別於 2.1 與 2.2 介紹，而 2.3 提出將彩色機密影像隱藏在兩張有意義的彩色分享影像之完整隱藏步驟。

2.1 色彩空間轉換

在色彩學上，紅色、綠色和藍色為 RGB 模型的三原色，將此三種主要顏色依照不同的比例和強度組合，便可形成各種不同顏色，如圖五(a)所示。然而像 RGB 色彩空間這種加法式色彩模式無法應用於印刷，如印製報紙和雜誌，因此，為了使用視覺密碼學的疊合特性，我們將採用減法式色彩模式 CMY，也就是顏料吸收光之後，反射出未被吸收的色光，如圖五(b)所示。RGB 與 CMY 的轉換公式如下：

$$\begin{bmatrix} C \\ M \\ Y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{1}$$

其中，所有彩色值 (R、G、B、C、M、Y) 皆標準化於 [0, 1] 範圍內。



(a) RGB 色彩空間　　(b) CMY 色彩空間

圖五：色彩空間模式

2.2 半色調技術

由於我們使用視覺密碼學的疊合特性來解密機密，因此，無法使用灰階色彩空間來當作分享影像，我們必須借重半色調技術來呈現連續色調的樣貌，灰階影像轉成半色調影像大致分為有序抖色法 (Order dithering) 及誤差擴散法 (Error diffusion)，其中又以誤差擴散法所產生出來的半色調影像效果最佳。如圖六所示，誤差擴散法有兩種著名的誤差擴散模型 Steinberg kernel 與 Jarvis kernel。由於 Steinberg kernel 所產生出來的半色調影像會比較細膩且好看，我們將採用 Steinberg kernel 來產生分享影像。

我們以臨界值為 128 為例說明誤差擴散的技術，圖七(a)為大小為 3×3 的原始灰階影像，首先我們先處理最左上角位置 (0, 0) 的像素值 170，然後比較此像素值和臨界值

大小，由於 170 大於臨界值，因此像素值 170 將更改為數值 255，並且將所產生的誤差值 170 - 255 = -85，依照 Steinberg kernel 中的權重來擴散分配到其他像素，例如 (0, 1) 像素值 150 經由錯誤擴散後變成 150+(7/16)×(-85) = 113；而 (1, 0) 像素值 160 經由錯誤擴散後變成 160+(5/16)×(-85) = 133；另外 (1, 1) 像素值 100 經由錯誤擴散後將變成 100+(1/16)×(-85) = 94，其轉換結果如圖七(b)所示。接下來轉換 (0, 1) 的像素值 113，轉換結果如圖七(c)。依序將每一個灰階像素轉換後，便可產生出一張半色調影像，如圖七(d)。

$$\frac{1}{16}\begin{bmatrix} & X & 7 \\ 3 & 5 & 1 \end{bmatrix} \qquad \frac{1}{48}\begin{bmatrix} & & X & 7 & 5 \\ 3 & 5 & 7 & 5 & 3 \\ 1 & 3 & 5 & 3 & 1 \end{bmatrix}$$

(a) Steinberg kernel (b) Jarvis kernel

圖六：兩種誤差擴散模型

$$\begin{bmatrix} 170 & 150 & 120 \\ 160 & 100 & 100 \\ 135 & 100 & 100 \end{bmatrix} \quad \begin{bmatrix} 255 & 113 & 120 \\ 133 & 94 & 100 \\ 135 & 100 & 100 \end{bmatrix} \quad \begin{bmatrix} 255 & 0 & 169 \\ 154 & 129 & 107 \\ 145 & 100 & 100 \end{bmatrix} \quad \begin{bmatrix} 255 & 0 & 255 \\ 255 & 0 & 0 \\ 255 & 0 & 255 \end{bmatrix}$$

(a) 灰階影像 (b) (0, 0) 轉換 (c) (0, 1) 轉換 (d) 半色調影像

圖七：誤差擴散法例子

2.3 加密步驟

我們觀察到如果彩色偽裝影像的色階過亮或過暗時，會造成產生出來的分享影像解密發生誤判，因此，我們首先將選定好的彩色偽裝影像與彩色機密影像進行色階調整，接著將 RGB 色彩空間轉換為 CMY 色彩空間，利用半色調技術分別對 C、M、Y 頻道進行半色調轉換，最後使用所提出的加密演算法產生兩張分享影像。以下為演算法詳細步驟：

輸入：兩張偽裝影像 C^1、C^2，一張機密影像 S 與臨界值 CT_1、CT_2、ST_1、ST_2

輸出：兩張分享影像 $Share^1$、$Share^2$

步驟 1： 調整偽裝影像色階至 $[CT_1, CT_2]$ 與機密影像色階至 $[ST_1, ST_2]$，並計算 $T = (CT_1 + CT_2)/2$。

步驟 2： 將偽裝影像進行 CMY 色彩空間轉換，分別得到 C^1C, C^1M, C^1Y, C^2C, C^2M, C^2Y, 單色調影像。將機密影像進行 CMY 色彩空間轉換與半色掉轉換，得到 SC, SM, SY 半色調影像。

步驟 3： 針對每個位置 (i, j)，如果 $SC_{i,j} = 255$，設 $C^1C_{i,j} = 255$，$C^2C_{i,j} = 255$，跳到步驟 8。

步驟 4： 如果 $SC_{i,j} = 0$ 且 $C^1C_{i,j} \geq T$，$C^2C_{i,j} \geq T$，設 $\text{MAX}(C^1C_{i,j}, C^2C_{i,j}) = 255$，$\text{MIN}(C^1C_{i,j}, C^2C_{i,j}) = 0$，跳到步驟 8。

步驟 5： 如果 $SC_{i,j} = 0$ 且 $C^1C_{i,j} \geq T$，$C^2C_{i,j} < T$，設 $C^1C_{i,j} = 255$，$C^2C_{i,j} = 0$，跳到步驟 8。

步驟 6： 如果 $SC_{i,j} = 0$ 且 $C^1C_{i,j} < T$，$C^2C_{i,j} \geq T$，設 $C^1C_{i,j} = 0$，$C^2C_{i,j} = 255$，跳到步驟 8。

步驟 7： 如果 $SC_{i,j} = 0$ 且 $C^1C_{i,j} < T$，$C^2C_{i,j} < T$，設 $C^1C_{i,j} = 0$，$C^2C_{i,j} = 0$，跳到步驟 8。

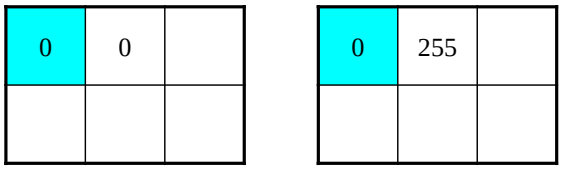
步驟 8： 針對位置 (i, j) 使用誤差擴散模型 Steinberg kernel 進行誤差擴散。

步驟 9： 重覆步驟 3 到 8，得到相對應的 $C^1M_{i,j}, C^2M_{i,j}, C^1Y_{i,j}, C^2Y_{i,j}$。

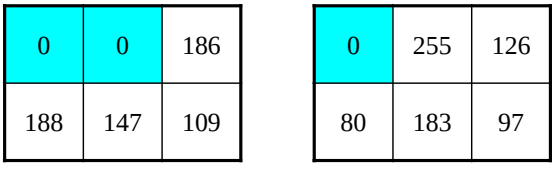
步驟 10： 將 C^1C, C^1M, C^1Y 疊合成 $Share^1$，C^2C, C^2M, C^2Y 疊合成 $Share^2$。

圖八提供了簡單的加密範例，圖八(a)為初始狀態，假設目前要處理位置 (1, 2)，圖八(b)描述了步驟 4 結果，由於 $SC_{1,2} = 0$，且 $C^1C_{1,2} \geq 128$，$C^2C_{1,2} \geq 128$，設 $\text{MAX}(C^1C_{1,2}, C^2C_{1,2}) = C^2C_{1,2} = 255$，$\text{MIN}(C^1C_{i,j}, C^2C_{i,j}) = C^1C_{1,2} = 0$，接著使用誤差擴散模型 Steinberg kernel 進行誤差擴散，圖八(c)描述了步驟 8 結果。

(a) 初始狀態



(b) 步驟 4 結果



(c) 步驟 8 結果

圖八：位置 (1, 2) 加密例子

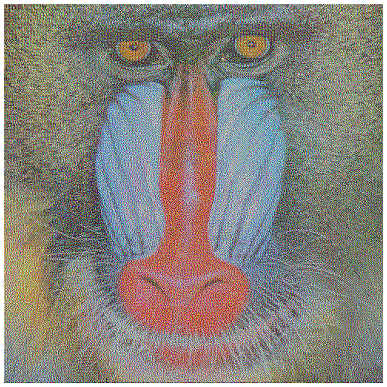
參、實驗結果與討論

我們以影像大小 512×512 做為實驗，臨界值的設定為 $CT_1 = 55$、$CT_2 = 200$、$ST_1 = 15$、$ST_2 = 100$，選定 Lena 當作偽裝影像 1，Mandrill 當作偽裝影像 2，如圖九(a)與圖九(b)所示，選定 Peppers 當作機密影像，如圖九(c)所示，所產生兩張有意義的分享影像，分別為圖九(d)與圖九(e)，而分享影像的疊合結果為圖九(f)，我們可以發現從任一分享影像中無法察覺機密影像的存在，且所提出的方法並不會擴張像素，因此，分享影像與偽裝影像的大小相同。另外我們選定 Mandrill 當作偽裝影像 1，Peppers 當作偽裝影像 2，Lena 當作機密影像，其所產生之有意義的分享影像與疊合結果如圖十所示，一樣從任一分享影像中無法察覺機密影像的存在，且解密不須要複雜的電腦計算，使用疊合即可利用人眼解密。

(a) 偽裝影像 1　(b) 偽裝影像 2　(c) 機密影像

(d) 分享影像 1　(e) 分享影像 2　(f) 疊合影像

圖九：加密結果


(d) 分享影像 1


(e) 分享影像 2


(f) 疊合影像

圖十：加密結果

肆、結論

不同於傳統加密機制的視覺密碼學讓資訊保護多了一種選擇，目前已有許多方法皆使用半色調技術將灰階影像轉換成二元影像，也有許多方法透過色彩分解來呈現更多色彩變化，但在這之中有不少方法都是產生無意義的分享影像，且其分解規則會連帶產生影像擴張，雖然上述兩點都不會洩漏機密影像的資訊，卻容易使有心人士猜疑亂碼形式之分享影像有鬼怪，進而造成機密影像的危機。因此本研究將一張彩色影像隱藏在兩張有意義的彩色影像上，所使用色彩分解與半色調的技術，其規則不會造成影像擴張，重疊後的影像仍能保持清晰。本研究不僅提供了另一種製作彩色視覺密碼的方法，也增加了機密影像的安全性。

[誌謝]

本研究感謝科技部「基於浮水印與盲偵測之 JPEG 影像驗證技術」研究計畫經費之支持(計畫編號 MOST 104-2221-E-034-004-)

參考文獻

[1] S. Dutta and A. Adhikari, “XOR based non-monotone t-(k,n)-visual cryptographic schemes using linear algebra,” *Information and Communications Security*, vol. 8958, pp. 230-242, 2015.

[2] Y. C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, vol. 36, pp. 1619-1629, 2003.

[3] R. J. Hwang, and C. C. Chang, "Hiding a picture in two pictures," *Optical Engineering*, vol. 40, no. 3, 2001, pp. 342-351, 2001.
[4] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349-358, 2003.
[5] M. Naor and A. Shamir, "Visual cryptography," *Eurocrypt94, Lecture Notes in Computer Science*, Springer-Verlag, Perugia, Italy, pp. 1-12, 1994.
[6] S. J. Shyu and M. C. Chen, "Optimum pixel expansions for threshold visual secret sharing schemes," *IEEE Transactions on Information and Forensics Security*, vol. 6, no. 3, pp. 960-969, 2011.
[7] S. J. Shyu and H. W. Jiang, "Efficient construction for region incrementing visual cryptography," *IEEE Transactions on Circuits System and Video Technology*, vol. 22, no. 5, pp. 769-777, 2012.
[8] R. Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Processing Letters*, vol. 16, no. 8, pp. 659-662, 2009.
[9] C. N. Yang and T. H. Chung, "A general multi-secret visual cryptography scheme," *Optics Communications*, vol. 283, no. 24, pp. 4949-4962, 2010.
[10] C. N. Yang, H. W. Shih, C. C. Wu, and L. Harn, "k out of n region incrementing scheme in visual cryptography," *IEEE Transactions on Circuits System and Video Technology*, vol. 22, no. 5, pp. 799-810, 2012.
[11] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Transactions on Image Processing*, vol. 15, pp. 2441-2453, 2006.

Biography

Wei-Liang Tai received the M.S. degree in computer science and information engineering from National Chung Cheng University, Taiwan, in 2004 and the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Taiwan, in 2008. He is currently Assistant Professor, Department of Information Communications, Chinese Culture University. His main interests are in information security and forensics and multimedia signal processing. He is currently an Editor of The Scientific World Journal for the "Signal Processing."

Zi-Jun Liao is a student at the Department of Information Communications, Chinese Culture University. He is currently pursuing the M.S. degree under the supervision of Dr. Wei-Liang Tai. His main interests are in information security and image processing.