可逆式雙影像資訊隱藏法－結合最低位元替換法及改良的像素差值藏匿法

冷輝世[1*]、黃瑄惠[2]

[1]國立彰化師範大學數學系、[2]國立彰化師範大學統計資訊研究所

摘要

Chang等學者於2007年首先提出可逆式雙影像資訊隱藏法，將機密訊息分別藏入兩張相同的掩蔽影像中成為偽裝影像，接收方必須同時取得兩張偽裝影像才能正確擷取出機密訊息並還原掩蔽影像。本研究基於可逆式雙影像資訊隱藏法的特徵，重新定義邊緣偵測的方法將兩張相同的掩蔽影像中的非邊緣像素和邊緣像素分別以最低位元替換法及改良的像素差值藏匿法藏入機密訊息。實驗結果顯示本研究相較於其他學者有較高的藏入量及良好的偽裝影像品質。

前言

最低位元替換法(以下簡稱LSB法)、像素差值藏匿法(以下簡稱PVD法)和探索方向修改法(以下簡稱EMD法)為常見的不可逆式資訊隱藏法。其中LSB法是將掩蔽影像中像素的最低位元直接替換成機密位元，具有低失真與高藏入量的特性，而PVD法則建立量化區間並藉由維持兩兩像素間的差值大小在同一量化區間並藏入機密訊息，具有高品質的偽裝影像特性。差異擴張法、直方圖位移法和像素值排序法為傳統的可逆式資訊隱藏法，缺點是機密訊息的藏入量不高。近年來，部份學者提出雙影像資訊隱藏技術。Lee等學者[8]透過座標空間位置，將機密位元兩兩成對藏入，達到高品質的偽裝影像。Lin等學者[9]使用龜殼法(EMD法的一種)得到高品質的偽裝影像與高藏入量。

文獻探討

OPAP法

x：掩蔽影像中的目標像素

x'、x''：經LSB法藏匿機密訊息後得到的偽裝像素、經OPAP最佳化後得到的新偽裝像素

k：LSB法中每個像素藏入的機密訊息長度

d'、d''：藏入誤差，為x'和x的差值及x''和x的差值

OPAP法針對藏入誤差$d' = x' - x$可再進一步區分為三個區間：

當$2^{k-1} < d' < 2^k$

$$x'' = \begin{cases} x' - 2^k, if\ x' \geq 2^k \\ x',\ otherwise \end{cases} \quad (1)$$

當$-2^{k-1} \leq d' \leq 2^{k-1}$

$$x'' = x' \quad (2)$$

當$-2^k \leq d' \leq -2^{k-1}$

$$x'' = \begin{cases} x' + 2^k, if\ x' < 256 - 2^k \\ x',\ otherwise \end{cases} \quad (3)$$

最佳化調整藏入誤差$d'' = x'' - x$說明如下：

若$2^{k-1} < d' < 2^k$，且$x' \geq 2^k$

$$\begin{gathered} d'' = x'' - x = x' - 2^k - x = d' - 2^k \\ 2^{k-1} - 2^k < d'' < 2^k - 2^k \\ 2^{k-1} - 2^k < d'' < 0 \end{gathered} \quad (4)$$

若$2^{k-1} < d' < 2^k$，且$x' < 2^k$

$$\begin{gathered} d'' = x'' - x = x' - x = d' \\ 2^{k-1} < d'' < 0 \end{gathered} \quad (5)$$

若$-2^{k-1} \leq d' \leq 2^{k-1}$

$$\begin{gathered} d'' = x'' - x = x' - x = d' \\ 2^{k-1} \leq d'' \leq 0 \end{gathered} \quad (6)$$

若$-2^k < d' < -2^{k-1}$，且$x' < 256 - 2^k$

$$\begin{gathered} d'' = x'' - x = x' + 2^k - x = d' + 2^k \\ -2^{k-1} + 2^k < d'' < -2^k + 2^k \\ 0 < d'' < 2^{k-1} \end{gathered} \quad (7)$$

若$-2^k < d' < -2^{k-1}$，且$x' \geq 256 - 2^k$

$$\begin{gathered} d'' = x'' - x = x' - x = d' \\ -2^k < d'' < -2^{k-1} \end{gathered} \quad (8)$$

由上述可知OPAP法將LSB法的藏入誤差$d'' = x'' - x$限制在-2^k與2^k之間達到最佳化結果。

改良的PVD法

Hsiao和Chang學者[4]提出改良的PVD法，使用邊緣吻合法，掃描順序由左至右由上至下，其中第一行和第一列不藏入機密訊息。

$x_{i,j}$、$x_{i,j}$‘：掩蔽影像中第i列第j行目標像素、偽裝影像中第i列第j行偽裝像素

n、k：藏入機密訊息的長度、欲藏入的最小機密訊息長度

$s(n)_2$、$s(n)_{10}$：長度為n的機密訊息以二進位、十進位表示

藏入機密訊息過程採用邊緣吻合法預測，預測值$p_{i,j} = (x_{i-1,j} + x_{i,j-1})/2$。

令欲藏入最小機密訊息長度為k，則變數$n = k, k+1, \ldots, 8$，由公式(9)、(10)可計算出多個不同候選偽裝像素x^n，如圖1。由公式(11)計算候選偽裝像素與目標像素的最小差值d_{min}，其n值即為最終藏入機密訊息的長度，候選偽裝像素x^n為最終偽裝像素值$x'_{i,j}$。

$$d^n = 2^n + s(n)_{10} - 2^k \quad (9)$$

$$x^n = \begin{cases} p_{i,j} - d^n, if\ p_{i,j} \geq x_{i,j} \\ p_{i,j} + d^n, if\ p_{i,j} < x_{i,j} \end{cases} \quad (10)$$

$$d_{min} = \min_{n \in \{k, k+1, \ldots, 8\}} \{|x^n - x_{i,j}|\} \quad (11)$$

$$n = \lfloor log_2(d^n + 2^k) \rfloor \quad (12)$$

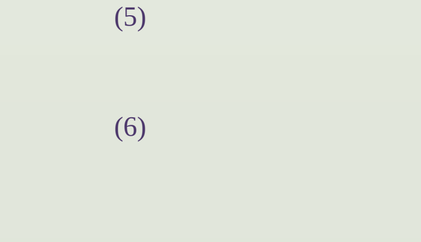


圖1. (a) $p_{i,j} < x_{i,j}$ (b) $p_{i,j} \geq x_i$

擷取機密訊息過程中，由已知的偽裝像素$x_{i,j}'$與預測值$p_{i,j}$，可推算出$d^n = |x_{i,j}' - p_{i,j}|$。由公式(12)可得到藏入的機密訊息長度$n$且藏入的機密訊息$s(n)_{10} = d^n - 2^n + 2^k$。

Chang等學者的可逆式雙影像資訊隱藏法

Chang等學者定義公式(13)

$$M(c,r) = (c + 2 \times r)\ mod\ 5 \quad (13)$$

並由此產生五進制二維對應矩陣如圖2。

S_1、S_2：兩張相同的掩蔽影像

S_1'、S_2'：S_1、S_2藏入機密訊息後的偽裝影像

x_i：掩蔽影像中第i個目標像素

x_i^1、x_i^2：S_1'中第i個偽裝像素S_2'中第i個偽裝像素

$M(c,r)$：對應矩陣第c行第r列的值

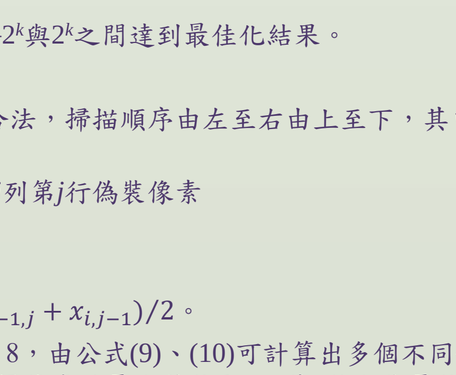


圖2. 五進制二維對應矩陣範例

採用EMD法藏入五進制機密數值，每次由掩蔽影像取出一組目標像素對(x_i, x_{i+1})為對應矩陣座標位置，令(x_i, x_{i+1})作為對應矩陣中心座標以選取候選值集合D_1、D_2如下:

$$D_1 = \{ M(x_i + 2, x_{i+1} - 2), M(x_i + 1, x_{i+1} - 1), M(x_i, x_{i+1}), M(x_i - 2, x_{i+1} + 2), M(x_i - 1, x_{i+1} + 1) \} \quad (14)$$

$$D_2 = \{ M(x_i + 2, x_{i+1} + 2), M(x_i + 1, x_{i+1} + 1), M(x_i, x_{i+1}), M(x_i - 1, x_{i+1} - 1), M(x_i - 2, x_{i+1} + 2) \} \quad (15)$$

取得欲藏入五進制機密數值，在D_1中找出和機密數值相等的矩陣元素$M(c,r)$後，將偽裝像素(x_i^1, x_{i+1}^1)設為(c, r)；在D_2中找出和機密數值相等的矩陣元素$M(c,r)$後，將偽裝像素(x_i^2, x_{i+1}^2)設為(c, r)，重複以上步驟，最終得到兩張偽裝影像S_1'、S_2'。

擷取機密訊息過程首先從S_1'、S_2'中取出偽裝像素對(x_i^1, x_{i+1}^1)及(x_i^2, x_{i+1}^2)並由公式(13)得到機密數值，利用取出的偽裝像素對作為對應矩陣中心座標計算出兩組候選值集合D_1、D_2，找出D_1、D_2交集的元素$M(c,r)$即為所藏入的五進制機密數值，(c,r)為目標像素對。

研究方法

本研究使用可逆式雙影像技術並採取黑白格模式進行藏入，如圖3。

S_1、S_2：兩張相同的掩蔽影像

$x_{i,j}$、$x_{i,j}$‘：掩蔽影像中的目標像素、偽裝影像中的偽裝像素

x_{edge}、$x_{nonedge}$：邊緣像素、非邊緣像素

d_{max}：與目標像素相鄰的四邊像素中兩兩間差值的最大值

d_{median}：所有d_{max}經排序後取中位數作為新的邊緣像素判斷標準

黑	白	黑	白	黑
白	黑	白	黑	白
黑	白	黑	白	黑
白	黑	白	黑	白
黑	白	黑	白	黑

圖3. 黑白格模式

藏入機密訊息過程中對S_1、S_2中分別進行藏入，機密訊息在影像S_1只能藏入黑格位置，在影像S_2只能藏入白格位置。首先對掩蔽影像做邊緣偵測(Canny)找出邊緣像素，得到邊緣影像I_{edge}將像素分為邊緣像素x_{edge}與非邊緣像素$x_{nonedge}$兩大類。本研究假設像素的邊緣特性是由相鄰四邊像素兩兩間的差值所造成的，利用公式(16)求得邊緣像素x_{edge}的最大差值d_{max}。將所有x_{edge}的最大差值d_{max}排序後找出中位數d_{median}作為定義新邊緣像素x_{edge}的標準：若$d_{max} \geq d_{median}$即判定為邊緣像素，否則為非邊緣像素。

$$d_{max} = \max\{ |x_{i-1,j} - x_{i+1,j}|, |x_{i,j-1} - x_{i,j+1}|, |x_{i-1,j} - x_{i,j-1}|, |x_{i-1,j} - x_{i,j+1}|, |x_{i+1,j} - x_{i,j-1}|, |x_{i+1,j} - x_{i,j+1}| \} \quad (16)$$

將機密訊息分別藏入S_1、S_2影像的步驟：藉由d_{median}的定義，若屬於邊緣像素則進行改良的PVD法藏入至少k位元機密訊息，並採用目標像素相鄰像素的平均值作為預測值；若屬於非邊緣像素則進行LSB法藏入k位元機密訊息並進行OPAP最佳化，重複上述過程得到兩張偽裝影像S_1'、S_2'。

擷取機密訊息過程中接收方持有兩張偽裝影像S_1'、S_2'與判斷標準d_{median}，並可由另外的掩蔽通道得知S_1'、S_2'分別將機密訊息藏入白格與黑格。黑白格模式下S_1'的白格位置與S_2'的黑格位置不曾被藏入機密訊息，透過影像重疊的方法，即可還原得到掩蔽影像。擷取機密訊息時採用公式(16)計算偽裝像素$x_{i,j}'$的相鄰像素間最大差值d_{max}，經判斷準則d_{median}(接收方必須經由掩蔽管道另外取得)來判定$x_{i,j}'$是否為邊緣像素，倘若$x_{i,j}'$經判定為邊緣像素，可判斷其藏入機密訊息的方法為改良的PVD法，若為非邊緣影像則為LSB法(OPAP)，從而擷取機密訊息。

實驗結果

本研究採用SIPI影像資料庫標準測試圖形Baboon、Lena、Scene和Peppers四張大小為512×512的影像(圖12)並以隨機方式產生機密訊息。

機密訊息的藏入量(Payload)採用公式(17)的計算方式，實驗結果的評估採用常見的峰值信噪比(Peak Signal-to-Noise Ratio，以下簡稱PSNR)，如公式(19)。其中N為藏入機密訊息位元個數，H、W為影像的高與寬，$x_{i,j}$‘、$x_{i,j}$分別代表位於i、j位置的偽裝像素值與目標像素值。圖13為藏入後偽裝影像，相較於圖12在視覺上比較起來並無明顯差異。

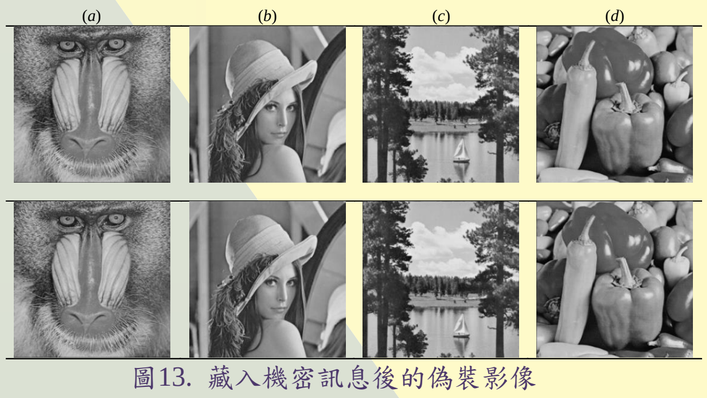
$$\text{Payload} = |N|/(2HW) \quad (17)$$

$$\text{MSE} = \frac{1}{HW} \sum_{i=1}^{H} \sum_{j=1}^{W} (x_{i,j}' - x_{i,j})^2 \quad (18)$$

$$\text{PSNR} = 10 \times log_{10}(255^2/\text{MES}) \quad (19)$$

(a) (b) (c) (d)

圖12. (a) Baboon (b) Lena (c) Scene (d) Peppers



(a) (b) (c) (d)

圖13. 藏入機密訊息後的偽裝影像

表2、表3為本研究方法與[8]、[9]比較，S_1‘、S_2’表示輸出的偽裝影像，其中影像品質PSNR以dB為單位，藏入量Payload以bpp為單位。

影像	[8]		[9]		實驗結果	
	S_1'	S_2'	S_1'	S_2'	S_1'	S_2'
Baboon	52.4	52.4	49.4	45.6	41.9	41.9
Lena	52.4	52.4	49.4	45.6	43.6	43.6
Scene	--	--	49.4	45.6	43.3	43.3
Peppers	52.4	52.4	49.4	45.6	43.5	43.5
Average	52.4	52.4	49.4	45.6	**43.1**	**43.1**

表2. PSNR(dB)值比較

影像	[8]	[9]	本研究
Baboon	0.75	1.25	1.54
Lena	0.75	1.25	1.50
Scene	--	1.25	1.51
Peppers	0.75	1.25	1.50
Average	0.75	1.25	**1.51**

表3. Payload(bpp)的比較

結論

本研究基於雙偽裝影像的特色運用黑白格模式，依掩蔽影像的特徵定義了新邊緣像素的判斷標準後重新區分邊緣像素與非邊緣像素並分別採用改良的PVD法與LSB法藏入機密訊息。實驗結果顯示本研究的平均藏入量1.51 bpp相較於其它學者的研究提高0.26~0.76 bpp，而且影像品質保持在人類視覺敏感度無法查覺其差異性(43.1 dB)。除了機密訊息的擷取外，掩蔽影像的還原可藉由疊合兩張偽裝影像中未藏入機密訊息的像素達成。