植基於差值擴張的高品質可逆式資訊隱藏技術

李金鳳
朝陽科技大學資訊管理系
副教授
lcf@cyut.edu.tw

黃郁霖
朝陽科技大學資訊管理系
研究生
s9714624@cyut.edu.tw

摘要

資訊隱藏是一種高科技的隱藏機密訊息技術。運用人類感官的局限性，將訊息藏在常見的掩蔽媒體(例如影像)中來傳遞訊息。資訊隱藏會對原始影像造成一定程度的破壞，但在一些特定領域的應用上(例如：軍事、醫療...等)需要在取出所嵌入之機密訊息後還能無失真的將偽裝影像還原為原始影像。本篇論文提出一個植基於差值擴張法(Difference Expansion, DE)的可逆式資訊隱藏技術，實驗結果顯示，此方法在藏入機密訊息後的影像品質優於 Chang 及 Shang 的方法。

關鍵詞：可逆式資訊隱藏、差值擴張法、直方圖修改法、溢位問題

Abstract

Steganography is the art and science of hiding confidential messages in such a way that no one from the third party knows the existence of the message. Hiding secret messages in digital cover images is the most widely used because it can take advantage of the limitation of human visual system (HVS) by employing the way that there is no major difference between the original cover image and the corrupted image (also called stego-image). However, for some applications like military, medical domains and etc., the even little distortion introduced to the image is not acceptable. Therefore, this paper introduces one lossless data hiding scheme based on difference expansion technique. It computes the smallest distortion between an overlapped pixel pair and hence has higher PSNR values while the payload is the same compared with Chang and Shang's scheme.

Keywords: Reversible Data Hiding, Difference Expansion

1. 前言

拜資訊科技及網際網路蓬勃發展所賜，網際網路儼然已成為一個被用來傳遞訊息的管道，無論是日常生活上或商業上也好，人們常使用網際網路來分享檔案、傳遞郵件或即時通訊等。但網際網路是一個公開的環境，任何人只要具備相關的技術就可以自網際網路上擷取他人的資料，因此如何安全地傳遞資訊便成為一個重要的議題。

資訊隱藏技術可以保護使用者的資料不讓非法使用者取得。資訊隱藏技術又分為不可逆式資訊隱藏技術[5] [6] [7]及可逆式資訊隱藏技術[2][1][8]兩種。不可逆式資訊隱藏通常資訊藏量較高且偽裝影像品質較好，但由於原始影像無法還原取回因此在一些特定領域的應用上(例如：軍事、醫療...等)受到限制，而可逆式資訊隱藏技術為了要紀錄還原成原始影像所需的資訊，通常資訊藏量較低且偽裝影像品質較差。

在可逆式資訊隱藏技術當中，Tian學者於 2003 提出差值擴張法 (Difference Expansion) [9]來達成可逆式資訊隱藏。差值擴張法主要是利用鄰近像素值相似的特性取兩相鄰像素間的差值，再將差值擴大兩倍使其擴大後的差值必定為偶數並將機密資訊嵌入其中。因偶數值的最小影響位元(Least Significant Bit, LSB)[3]必定為0，當嵌入的資料為0時，經擴大後的差值仍維持偶數；若嵌入的資料為1時，擴大後的差值會變為奇數。利用此原理接收者只要將偽裝影像兩相鄰像素之差值的LSB取出，便能取得所嵌入的機密訊息。

Chang 及 Shang 學者於 2005 年提出一個基於差值擴張法的可逆式資訊隱藏技術[4]，此方法利用重疊(Overlap)的方式取兩相鄰像素來嵌入資料。以 (p_1, p_2, p_3, p_4) 四個像素來說，Chang 及 Shang 的方法可以取相鄰的 (p_1, p_2)、(p_2, p_3) 及 (p_3, p_4) 等 3 個像素對。故對於 n 個像素的影像而言，共有 $(n-1)$ 組像素對來藏入機密訊息。然而，Tian 的方法僅能取 $(n/2)$ 組像素對來藏入機密

訊息。由此可知，Chang 及 Shang 學者的方法在資訊藏量上優於 Tian 學者的方法。

Chang 及 Shang 學者的方法乃是取一對像素值 (p_i, p_{i+1}) 來進行計算，其方法以 p_i 為基準再加上差異值來改變 p_{i+1} 以攜帶 1 位元機密訊息，然而此方法未考慮“像素差值之方向性”以至於當像素值 p_{i+1} 小於 p_i 時所求得的偽裝像素會產生『較大失真度』而使得影像品質下降。因此本文提出一個方法藉由“像素差值之方向性”的概念來改變像素值 p_{i+1} 以攜帶機密資訊並且避免『較大失真度』產生，使得影像的品質得以提升。

在本文中的第 2 節將針對 Chang 及 Shang 學者的方法加以說明並進一步分析其方法對影像失真的影響；第 3 節裡則詳述本文藉由“像素差值之方向性”的概念所提出來方法的內容及步驟說明；第 4 節裡採用 512×512 灰階圖進行實驗並列出資訊藏量及影像品質以呈現本文所提方法之優異性，第 5 節則為結論及未來研究。

2. 相關技術

在本節中將針對 Chang 及 Shang 學者所提出的差值修改方法加以詳述說明，其中包含機密訊息嵌入的方法和直方圖修改的技巧。

Chang 及 Shang 學者於 2005 年提出一個使用差值修改(Difference Modification)的可逆式資訊隱藏技術[4]，此技術並分為直方圖修改(Histogram Modification)和差值修改(Difference Modification)兩部分如圖 1。

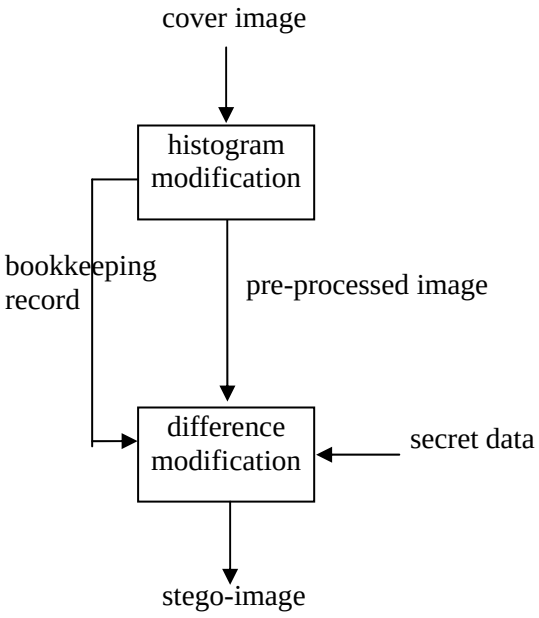
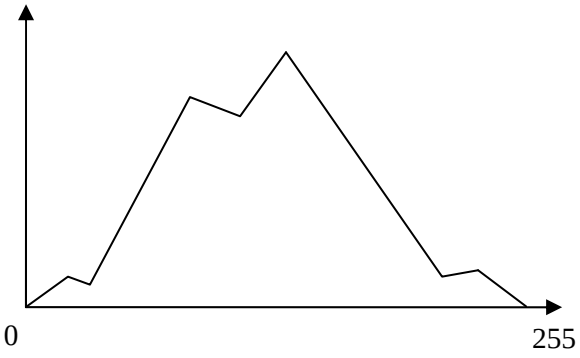
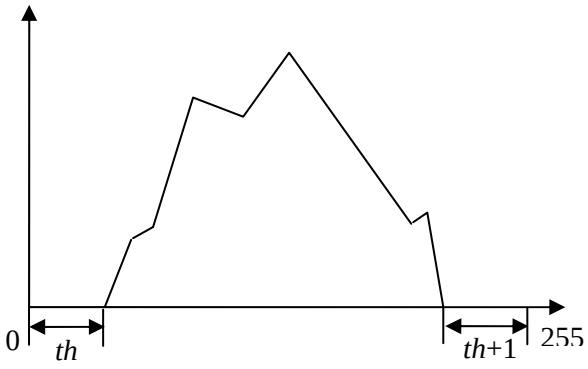


圖 1 Chang 和 Shang 提出的資訊隱藏方法

一般灰階影像以 8 bits 表示其像素值介於 0~255 間，而影像像素值經修改後可能會低於 0 或高於 255 以至於發生溢位(overflow)或下溢(underflow)的情況。Chang 和 Shang 學者利用失真門檻 th 控制偽裝影像的影像品質，在訊息藏入前將原始影像的像素值以直方圖修改的方式先做調整，再以修改後的影像作為掩護影像來嵌入機密訊息以避免偽裝像素值發生上溢或下溢的狀況。經直方圖修改後的影像如圖 2(b)其像素值會介於 $th \sim (255 - th - 1)$ 之間，以此經修改後的影像作為掩護影像再經由差值修改法(Difference Modification)嵌入機密資訊便不會發生溢位的情況。



(a)原始影像



(b)經直方圖修改後的影像

圖 2 原始影像及直方圖修改後之影像

經直方圖修改影像後，Chang 及 Shang 學者利用兩相鄰像素值 $f(i, j)$ 與 $f(i, j+1)$ 間的差異值 D(公式 1)來進行一個機密訊息 s 的藏入，並有可藏和不可藏兩種狀況。當兩相鄰像素的差值 D 小於等於預先設定的失真門檻值 th 時表示為『可藏』，並採用差值擴張(Difference Expansion)來修改差值並藏入訊息；當差值 D 高於門檻值 th 時為『不可藏』，採用差值位移(Difference Shifting)來修改差值以供辨識此處為不藏機密訊息。演算法如公式 2 所示。差值修改後再利用原始像素值 $f(i, j)$ 與修改後的差異值 D' 來求得偽裝像素，如公式 3。其嵌入步驟如下：

步驟 1.計算差值 D 如公式(1)所示

$$D = f(i, j+1) - f(i, j). \tag{1}$$

步驟 2.採差值擴張技術來進行機密訊息 s 的嵌入

$$D' = \begin{cases} 2|D| + s, & \text{if } |D| \le th, \\ D + th + 1, & \text{if } D > th, \\ D - th, & \text{if } D < th. \end{cases} \tag{2}$$

步驟 3.求一對偽裝像素值 $\left(f'(i, j), f'(i, j+1)\right)$

$$f(i, j)' = f(i, j),$$
$$f'(i, j+1) = f(i, j) + D'. \tag{3}$$

範例 1.

假設有 4 個掩護影像像素值(如圖 3(a))其為(122, 126, 129, 126)，並設定門檻值 $th = 3$。二元機密訊息 $s = 11$ 以 Chang 及 Shang 學者所提出的方法[4]進行資訊嵌入之步驟如下：

首先將四個原始像素值分成三對可重疊的像素對即(122, 126)、(126, 129)和(129, 126)。

計算第一對掩護影像像素值之差異值為

$D = 126 - 122 = 4$，

$\because D > th$, $\therefore D' = 4 + 3 + 1 = 8$，

第一對偽裝像素值不能藏機密訊息否則會造成過大失真，但仍要改變原始影像的像素值，以利收方回復原始影像之用。因此，

$\left(f'(1, 1), f'(1, 2)\right) = (122, 122 + 8) = (122, 130)$，

如圖 3(b)。

接著處理第二對掩護像素值，其差異值為

$D = 129 - 126 = 3$，

$\because |D| \le th$， $\therefore D' = 3 \times 2 + 1 = 7$，

故第二對偽裝像素值如圖 3(c)

$\left(f(1, 2), f(1, 3)\right) = (126, 126 + 7) = (126, 133)$，

並且藏入第一個機密訊息 1。

最後處理第三對掩護像素值，其差異值為

$D = 126 - 129 = -3$，

$\because |D| \le th$， $\therefore D' = 3 \times 2 + 1 = 7$，

故第三對偽裝像素值為

$\left(f(1, 3), f(1, 4)\right) = (129, 129 + 7) = (129, 136)$

並且藏入第二個機密訊息 1。

經由上述步驟進行機密訊息的藏入後，得到偽裝影像為(122, 130, 133, 136)如圖 3(d)。

122	126	129	126
…	…	…	…
…	…	…	…
…	…	…	…

(a)

122	**130**	129	126
…	…	…	…
…	…	…	…
…	…	…	…

(b)

122	130	**133**	126
…	…	…	…
…	…	…	…
…	…	…	…

(c)

122	**130**	**133**	**136**
…	…	…	…
…	…	…	…
…	…	…	…

(d)

圖 3 以 Chang 及 Shang 學者的方法嵌入機密資訊之步驟

3. 提出的方法

本研究引用 Chang 和 Shang 學者所提出的方法[4]並予以改良，本研究提出的方法讓 $f(i, j)$ 不再固定被視為為被加數，它也有可能為被減數再進行計算以求得偽裝像素，使得 $f'(i, j+1)$ 與 $f(i, j+1)$ 的差異不會有『較大失真度』。

3.1 嵌入方法

本研究所提出的方法進行機密資訊嵌入時有以下步驟：

步驟 1.取一掩護像素值對計算其差值 D

$$D = f(i, j+1) - f(i, j).$$

步驟 2.求修改後的差值 D' 以進行機密訊息 s 的嵌入

$$D' = \begin{cases} 2|D| + s, & \text{if } |D| \le th, \\ D + th + 1, & \text{if } |D| > th. \end{cases}$$

步驟 3.求該對偽裝像素值 $(f'(i, j), f'(i, j+1))$

$f'(i, j) = f(i, j)$ ，

$$f'(i, j+1) = \begin{cases} f(i, j) + D', & if \quad D \ge 0, \\ f(i, j) - D' & if \quad D < 0. \end{cases}$$

步驟 4.調整偽裝像素值 $f'(i, j+1)$ ，以解決溢位問題

當 $0 \le f'(i, j+1) \le 255$ 時，

$f'(i, j+1) = f'(i, j+1)$ ；

當 $f'(i, j+1) > 255$ 時，

$f'(i, j+1) = 255 - (f'(i, j+1) \bmod 255)$ ；

當 $f'(i, j+1) < 0$ 時，

$f'(i, j+1) = 0 - (f'(i, j+1) \bmod 0)$ 。

範例 2.

承範例 1，有一張掩護影像其前四個像素值如圖 4(a)為(122, 126, 129, 126)，並設定失真門檻值 $th = 3$ 。今令欲藏入的二元機密訊息 $s = 11$ 。以本研究所提出的方法進行資訊嵌入之步驟如下：

首先計算第一對掩護影像像素值 $(122, 126)$ 之差值位移 D' 。

$D = 126 - 122 = 4$ ，

$\because D > th \quad \therefore D' = 4 + 3 + 1 = 8$ ，

故第一對偽裝像素值為

$(f'(1, 1), f'(1, 2)) = (122, 122 + 8) = (122, 130)$

，如圖 4(b)所示。

接著處理第二對掩護像素值 $(126, 129)$ ，其差異值為 $D = 129 - 126 = 3$ ，

$\because |D| \le th \quad \therefore D' = 3 \times 2 + 1 = 7$ ，

故第二對偽裝像素值為

$(f(1, 2), f(1, 3)) = (126, 126 + 7) = (126, 133)$

如圖 4(c)，並且藏入第一個機密訊息 1。

最後處理第三對掩護像素值 $(129, 126)$ ，其差異值為 $D = |126 - 129| = 3$ ，

$\because |D| \le th \quad \therefore D' = 3 \times 2 + 1 = 7$ ，

故第三對偽裝像素值為

$(f(1, 3), f(1, 4)) = (129, 129 - 7) = (129, 122)$

如圖 4(d)並且藏入第二個機密訊息 1。

經由上述步驟進行機密訊息的藏入後，得到偽裝影像為(122, 130, 133, 122)如圖 4(d)。

122	126	129	126
…	…	…	…
…	…	…	…
…	…	…	…

(a)

122	**130**	129	126
…	…	…	…
…	…	…	…
…	…	…	…

(b)

122	130	**133**	126
…	…	…	…
…	…	…	…
…	…	…	…

(c)

122	**130**	**133**	**122**
…	…	…	…
…	…	…	…
…	…	…	…

(d)

圖 4 以本研究所提出的方法嵌入機密資訊

3.2 取出資訊及還原影像

本方法取出機密訊息及還原影像的步驟如下：

步驟 1.計算偽裝像素的差值 D'

查詢調整表檢查像素 $f'(i, j+1)$ 有無經過調整，當 $f'(i, j+1)$ 未經調整時，$D' = f'(i, j+1) - f'(i, j)$；

當 $f'(i, j+1)$ 經過調整且 $255 - f'(i, j+1) < f'(i, j+1) - 0$ 時，$D' = \left[255 + \left(255 - f'(i, j+1)\right)\right] - f'(i, j)$；

當 $f'(i, j+1)$ 經過調整且 $255 - f'(i, j+1) > f'(i, j+1) - 0$ 時，$D' = \left(0 - f'(i, j+1)\right) - f'(i, j)$。

步驟 2.求差值 D 並取出機密訊息 s

$$D = \left\lfloor \frac{|D'|}{2} \right\rfloor,$$

當 $D \le th$ 時取出機密訊息 $s = |D'| \bmod 2$。

步驟 3.還原原始像素值 $\left(f(i, j), f(i, j+1)\right)$

令 $f(i, j) = f'(i, j)$，

當 $D' \ge 0$ 時，$f(i, j+1) = f(i, j) + D$，

當 $D' < 0$ 時，$f(i, j+1) = f(i, j) - D$。

範例 3.

假設有 4 個偽裝影像像素值(如圖 5(a))為 (122, 130, 133, 122)，並設定門檻值 $th = 3$。以本研究所提出的方法取出機密訊息並還原影像之步驟如下所示：

首先計算第一對偽裝影像像素值之差異值為 $D' = 130 - 122 = 8$ 則 $D = \left\lfloor \frac{8}{2} \right\rfloor = 4$，

$\because D > th$ $\therefore$ 無機密訊息 s 嵌入，

故第一對掩護像素值如圖 5(b)為 $\left(f(1, 1), f(1, 2)\right) = (122, 122+4) = (122, 126)$。

接著處理第二對偽裝像素值，其差異值為 $D' = 133 - 126 = 7$ 則 $D = \left\lfloor \frac{7}{2} \right\rfloor = 3$，

$\because D \le th$ $\therefore s = |7| \bmod 2 = 1$，

故第二對掩護像素值如圖 5(c)為 $\left(f(1, 2), f(1, 3)\right) = (126, 126+3) = (126, 129)$，

並且取出第一個機密訊息 1。

最後處理第三對偽裝像素值，其差異值為 $D' = 122 - 129 = -7$ 則 $D = \left\lfloor \frac{|-7|}{2} \right\rfloor = 3$，

$\because D \le th$ $\therefore s = |7| \bmod 2 = 1$，

故第三對掩護像素值為 $\left(f(1, 3), f(1, 4)\right) = (129, 129-3) = (129, 126)$

並且取出第二個機密訊息 1。

經由上述步驟進行機密訊息的取出後，得到二元機密訊息 $s = 11$ 並且還原原始影像為 (122, 126, 129, 126)如圖 5(d)。

122	130	133	122
…	…	…	…
…	…	…	…
…	…	…	…

(a)

122	**126**	133	122
…	…	…	…
…	…	…	…
…	…	…	…

(b)

122	126	**129**	122
…	…	…	…
…	…	…	…
…	…	…	…

(c)

122	**126**	**129**	**126**
…	…	…	…
…	…	…	…
…	…	…	…

(d)

圖 5 以本研究所提出的方法取出機密資訊

3.3 溢位像素值調整

由於使用差值修改法有可能導致偽裝像素值發生溢位(overflow/underflow)問題，因此本方法需再判斷偽裝像素值 $f'(i, j+1)$ 有無溢位並加以調整如 3.1 小節步驟 4，且經調整過的像素會記錄於一個調整表中，當取出資訊時需查詢此調整表確認偽裝像素值 $f'(i, j+1)$ 是否經過調整再進一步求得 D' 如 3.2 小節步驟 1。

舉例來說，假設一對掩護影像像素值為 (251, 254)，並設定門檻值 $th=3$，今欲藏入的機密訊息 $s=1_2$，以本研究所提出的方法進行機密資訊嵌入及溢位像素值調整其計算如下：

計算掩護像素值之差異值為

$D=254-251=3$，

$\because D\le th \ \ \therefore D'=3\times 2+1=7$，

故偽裝像素值為

$\left(f'(1, 1), f'(1, 2)\right)=(251, 251+7)=(251, 258)$；

因 $f'(1, 2)=258>255$ 表示像素值向上溢位 (overflow)，所以調整像素值為

$f'(1, 2)=255-(258 \bmod 255)=252$，

因此得到這對偽裝像素值為

$\left(f(1, 1), f(1, 2)\right)=(251, 252)$。

得到偽裝影像後採本研究提出的方法取出機密訊息並還原影像其計算如下：

經調整表知 $f'(1, 2)$ 曾經過調整

且 $255-f'(1, 2)<f'(1, 2)-0$，

所以 $D'=\left[255+(255-252)\right]-251=7$，

則 $D=\left\lfloor \frac{7}{2} \right\rfloor=3$。

$\because D\le th \ \ \therefore s=7 \bmod 2=1$，

故還原這對像素值為

$\left(f(1, 1), f(1, 2)\right)=(251, 251+3)=(251, 254)$。

4. 實驗結果

本研究以 Lena(如圖 6(a))、Baboon(如圖 6(b))兩張大小為 512×512 的灰階影像進行實驗，分別以 Chang 及 Shang 學者的的差值修改法[4]與本研究所提的方法進行測試，並以高峰影像信號雜訊比(Peak Signal to Noise Ratio, PSNR)來衡量影像品質及平均藏入位元來衡量機密訊息負載量，其定義如下：

$$PSNR=10\times\log_{10}\left(\frac{255^2}{MSE}\right),$$

$$MSE=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{i=1}^{N}\left(f(i, j)-f'(i, j)\right)^2.$$

$$\text{平均藏入位元}=\frac{k}{M\times N}\ ,$$

其中 $M\times N$ 為影像大小，$f(i, j)$ 表示原始影像像素值，$f'(i, j)$ 表示偽裝影像像素值，k 表示機密訊息藏入總數，實驗結果分別列於表 1 及表 2。

經由實驗結果可發現，在相同門檻值下本研究所提出的方法在機密訊息負載量上與 Chang 及 Shang 學者的方法[4]相同，但影像品質卻有顯著的提升，平均提升 4.42db，達成了提高影像品質目的。

(a) (b)

圖 6 灰階影像 Lena 及 Baboon

表 1 Lena 的實驗結果

	門檻值	*th*=5	*th*=10	*th*=20
提出的方法	平均藏入位元(bpp)	0.66	0.84	0.94
	PSNR(db)	38.14	35.18	33.70
Chang 及 Shang 的方法	平均藏入位元(bpp)	0.66	0.84	0.94
	PSNR(db)	32.89	29.99	28.84

表 2 Baboon 的實驗結果

	門檻值	*th*=5	*th*=10	*th*=20
提出的方法	平均藏入位元(bpp)	0.40	0.62	0.82
	PSNR(db)	37.02	33.01	30.87
Chang 及 Shang 的方法	平均藏入位元(bpp)	0.40	0.62	0.82
	PSNR(db)	33.29	29.24	27.15

4. 結論

本研究改良 Chang 及 Shang 學者的方法[4]提出一個植基於差值擴張技術的可逆式資訊隱藏法，經由實驗結果可發現在相同門檻值下本研究所提出的方法在機密訊息負載量上與 Chang 及 Shang 學者的方法[4]相同，但影像品質上卻有顯著的提升。未來研究是希望在高品質高藏量的狀態在不需記錄額外資訊下改善溢位問題。

參考文獻

[1] Alattar, A. M., "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," ***IEEE Transactions on Image Processing***, Vol. 13, No. 8, pp. 1147-1156, 2004.

[2] Celik, M. U., Sharma, G., Tekalp, A. M., and Saber, E., "Reversible Data Hiding," ***Proceedings of IEEE International Conference on Image Processing***, Vol. 2, pp. 157-160, 2002.

[3] Chan, C. K. and Cheng, L. M., "Hiding Data in Images By Simple LSB Substitution," ***Pattern Recognition***, Vol. 37, No. 3, pp. 469-474, 2004.

[4] Chang, L. W. and Shang, T. T., ***Reversible Data Hiding Using Difference Modification***, Institute of Information Systems and Applications National Tsing Hua University, Thesis for the Degree of Master, 2005.

[5] Lee, C. F., Chang, C. C., and Wang, K. H., "An Improvement of EMD Embedding Method for Large Payloads by Pixel Segmentation Strategy," ***Journal of Image and Vision Computing***, Vol. 26, No. 12, pp. 1670-1676, 2008.

[6] Lee, C. F., Shen, J. J., and Chao, H. L., **"**Complete Double Layered Embedding Scheme for Information Hiding," ***The Eighth International Conference on Intelligent Systems Design and Applications***, Vol. 3, pp. 525-528, 2008.

[7] Mielikainen, J., "LSB Matching Revisited," ***IEEE Signal Processing Letters***, Vol. 13, No. 5, pp. 285-287, 2006.

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

[9] Tian, J., "Reversible Data Embedding Using a Difference Expansion," ***IEEE Transactions on Circuits and Systems for Video Technology***, Vol. 13, No. 8, pp. 890-896, 2003.