Image steganographic scheme based on pixel-value differencing and LSB replacement methods

H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang

Abstract: In order to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality, a novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented. First, a different value from two consecutive pixels by utilising the PVD method is obtained. A small difference value can be located on a smooth area and the large one is located on an edged area. In the smooth areas, the secret data is hidden into the cover image by LSB method while using the PVD method in the edged areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess, the security level is the same as that of a single using the PVD method of the proposed method. From the experimental results, compared with the PVD method being used alone, the proposed method can hide a much larger information and maintains a good visual quality of stego-image.

1 Introduction

Today, we can communicate with one another in different places of the world through the Internet. Before sending a message, we can encrypt the message so as to protect the contents of the message by using DES, RSA [1, 2] etc. Furthermore, we can modify the contents of the message to achieve the purpose of the message encryption [3, 4]. However, the ciphertext is easier causing to notice others when the communication channel was monitored. Thus, another method to deliver secret messages by exchanging the plaintext was widely studied in the past two decades. This method is called steganography (i.e. data/information hiding) and it can be traced back to a 'prisoner's problem' [5]. The prisoner's problem described two prisoners who wanted to escape from prison and they only secretly communicated with each other by one image. As long as the communication tool (i.e. image) detected the spoil by human eyes of the warden, the escape plan would be defeated. In a word, information hiding techniques supply a secret communication channel by conveying a plaintext. What is more, the application of the information hiding can be used in military, commercial, and anti-criminal-related applications and so forth [6].

Many steganographic methods have been proposed to hide secret data into an image. The most common method is called least-significant-bits (LSB), which utilises some least bits of pixels in the cover image to embed secret data [7]. Wang *et al.* proposed a method of exhaustive least-significant-bit substitution to improve the security and the quality of the stego-image [8]. Furthermore, Chang *et al.* proposed an efficient method of dynamic programming strategy [9]. According to the characteristics of the human visual system, embedding the variable sizes of the LSBs was presented in [10]. Fu and Au proposed some data hiding methods for halftone images that not only can embed a large amount of secret data but also maintain good visual image quality [11]. To raise the capacity of hiding, and to ensure more security, better quality of stego-image for embedding data into binary image is presented in [12, 13]. Wu and Tsai [14] utilised the difference between the two consecutive pixels in the cover image to determine what size the secret message is to be hidden. And their method provided the stego-image has an imperceptible quality.

From the above-mentioned various methods we can evaluate a steganographic technique by two benchmarks — the secret message capacity of hiding and the quality of the stego-image. In general, if we can embed a great deal of secret data into a cover image and maintain a high similarity between the cover image and the stego-image, it will not be easily suspected by illegal users when carrying out the process of the information delivered. Wu and Tsai's scheme possesses both high capacity of secret data and high quality of the stego-image. Nevertheless, we consider it can embed much greater amounts of secret data, if the high quality of the stego-image is disregarded. For this reason, we present a method that can hide double the capacity of the secret data in Wu and Tsai's scheme with an acceptable quality of the stego-image.

In Wu and Tsai's method, a pixel-value differencing (PVD) method is used to discriminate between edged areas and smooth areas. The capacity of hidden data in edged areas is higher than that of smooth areas. However, to take account of the capacity of hidden data in the smooth areas, we propose a method to increase the capacity of hidden data by using a fixed-size least-significant-bits (LSB) method; we still employ the PVD method to determine the size of the hidden data in the edged areas.

IEE Proceedings online no. 20059022

doi: 10.1049/ip-vis:20059022

Paper first received 27th February and in revised form 8th November 2004. Originally published online 3rd June 2005

H.-C. Wu is with the Department of Information Management, National Taichung Institute of Technology, 129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C.

N.-I. Wu is with the Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.

M.-S. Hwang and C.-S. Tsai are with the Department of Management Information Systems, National Chung Hsing University, 250 Kuo-Kuang Road, Taichung, Taiwan 402, R.O.C.

E-mail: mshwang@nchu.edu.tw

2 Review of Wu and Tsai's method

In Wu and Tsai's steganographic method, a grey-valued cover image is partitioned into non-overlapping blocks of two consecutive pixels, states p_i and p_{i+1}. From each block we can obtain a different value d_i by subtracting p_i from p_{i+1}. All possible different values of d_i range from -255 to 255, then $|d_i|$ ranges from 0 to 255. Therefore, the pixel p_i and p_{i+1} is located within the smooth area when the value $|d_i|$ is smaller and will hide less secret data. Otherwise, it is located on the edged area and embeds more data. From the aspect of human vision it has a larger tolerance that embeds more data into edge areas than smooth areas. In Wu and Tsai's method, first, the range table has to be designed to fabricate a range table with n contiguous ranges (n contiguous ranges, e.g. R_i where $i = 1, 2, \ldots, n$). The range table ranges from 0 to 255. The lower and upper bound values of R_i, e.g. l_i and u_i, then $R_i \in [l_i, u_i]$. The width of R_i e.g. w_i, then $w_i = u_i - l_i + 1$. How many bits were hidden in two consecutive pixels depended on w_i, respectively. Considering the aspect of security, the fabricating range table is useful, because R_i of the range table is variable, so that, it cannot extract the identical secret data without the original range table.

In Wu and Tsai's system, the secret data is a long-bit stream, and the cover image is a grey-level image. The hidden algorithm is described as follows:

1. Calculate the difference value d_i for each block of two consecutive pixels p_i and p_{i+1} which is given by $d_i = |p_i - p_{i+1}|$.
2. Find the optimal R_i of the d_i such that $R_i = min(u_i - k)$, where $u_i \geq k, k = |d_i|$ and $R_i \in [l_i, u_i]$ is the optimum R_i for all $1 \leq i \leq n$.
3. Compute how many bits t of the secret data, which are hidden in each block of two consecutive pixels, depend on each w_i of the R_i is defined as $t = \lfloor \log_2 w_i \rfloor$, where w_i is the width of the R_i.
4. Read t bits binary secret data one by one according to Step 3, and then transform t into decimal value b. For instance, assume $t = 101$, then $b = 5$.
5. Calculate the new difference value d' which is given by $d'_i = l_i + b$.
6. Modify the p_i and p_{i+1} by following formula:

$$(p'_i, p'_{i+1}) = \begin{cases} (p_i + \lceil m/2 \rceil, p_{i+1} - \lfloor m/2 \rfloor), & \text{if } p_i \geq p_{i+1} \text{ and } d'_i > d_i; \\ (p_i - \lfloor m/2 \rfloor, p_{i+1} + \lceil m/2 \rceil), & \text{if } p_i < p_{i+1} \text{ and } d'_i > d_i; \\ (p_i - \lceil m/2 \rceil, p_{i+1} + \lfloor m/2 \rfloor), & \text{if } p_i \geq p_{i+1} \text{ and } d'_i \leq d_i; \\ (p_i + \lceil m/2 \rceil, p_{i+1} - \lfloor m/2 \rfloor), & \text{if } p_i < p_{i+1} \text{ and } d'_i \leq d_i, \end{cases}$$

where $m = |d'_i - d_i|$. Finally, the purpose of secret data hiding with the (p'_i, p'_{i+1}) in place of the (p_i, p_{i+1}) is achieved.

Repeat Steps 1-6 until all secret data are hidden in the cover image and the stego-image is obtained. For example, assume $p_i = 100, p_{i+1} = 162, R_4 = [32, 63]$ and secret data is $00000_{(2)}$. So $|d_i| = 62, w_i = 32, b = 0, d'_i = 32, m = 30$, $\lceil m \rceil = 15$, $\lfloor m \rfloor = 15$. Owing to $p_i < p_{i+1}$ and $d'_i \leq d_i$ such $p'_i = 100 + 15 = 115$ and $p'_{i+1} = 162 - 15 = 147$. Finally, replace pixel values (100, 162) with (115,147) so as to hide 5-bits secret data $00000_{(2)}$ into the cover image.

In the extracting phase, the original range table is necessary. It is used to partition the stego-image by the same method used for the cover image. Calculate the different value $d'(p'_i, p'_{i+1})$ for each block of two consecutive pixels p'_i, p'_{i+1}, where $d'(p'_i, p'_{i+1}) = |p'_i - p'_{i+1}|$. Then, find the optimum R_i of the $d'(p'_i, p'_{i+1})$ just as in Step 2 in the hiding phase. Subtract l_i from $d'(p'_i, p'_{i+1})$ and b' is obtained. The b' value represents the secret data by decimal. Transform b' into binary with t bits, where $t = \lfloor \log_2 w_i \rfloor$. The t bits can stand for the original secret data of hiding. For instance, assume that $b' = 7$ and $t = 3$, the secret data is 111. If $t = 5$, that secret data is 00111.

3 The proposed method

In this Section, we aim to smooth areas posing an improved method to increase capacity by using a LSB method and still use Wu and Tsai's scheme for edge areas. The division between the 'lower-level i.e. smoothness areas' and 'higher-level i.e. edge areas' of the range table is controlled by the users. Anyone who has extracted the secret data from a stego-image must use the original division. A division is the key of the extracted secret data. In the lower level of the range table, each block of two continuous pixels will hide 6-bit secret data (i.e. each pixel hides 3-bit secret data), otherwise (such as the higher-level of the range table), the bit-number of hidden data depends on w_i. Next, we present the embedding algorithm.

3.1 The embedding algorithm

Figure 1 shows the block diagram of the embedding algorithm. First, we must assume a division *Div* of the 'lower-level' and 'higher-level'. For example, let $Div = 15$, so we can set the 'lower-level' to be R_1 and R_2, 'higher-level' to be R_3, R_4, R_5, and R_6 which are shown in Fig. 2. The detailed secret data hiding steps are as follows.

Step 1: Calculate the difference value d_i for each block of two consecutive pixels p_i, p_{i+1}, which is given by

$$d_i = |p_i - p_{i+1}| \qquad (1)$$

Step 2: Find the optimal R_i of the d_i such that $R_i = min(u_i - k)$, where $u_i \geq k$ and $k = |d_i|, R_i \in [l_i, u_i]$ is the optimum R_i for all $1 \leq i \leq n$.

Steps 1 and 2 are the same as Wu and Tsai's first two steps in Section 2.1. After Step 2, we must judge the level of the optimal R_i, if R_i belongs to a higher-level, and proceed with the next step by using Wu and Tsai's method until

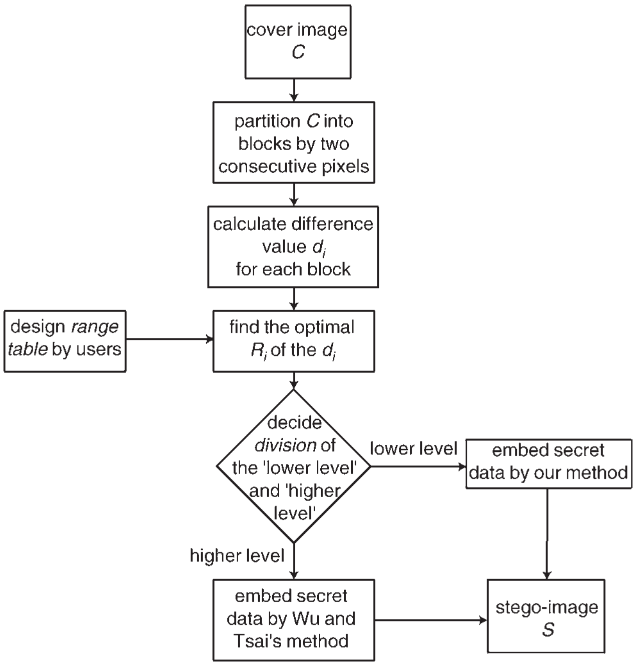
cover image C
partition C into blocks by two consecutive pixels
calculate difference value d_i for each block
design range table by users
find the optimal R_i of the d_i
decide division of the 'lower level' and 'higher level'
lower level
embed secret data by our method
higher level
embed secret data by Wu and Tsai's method
stego-image S

Fig. 1 *Block diagram of embedding algorithm*

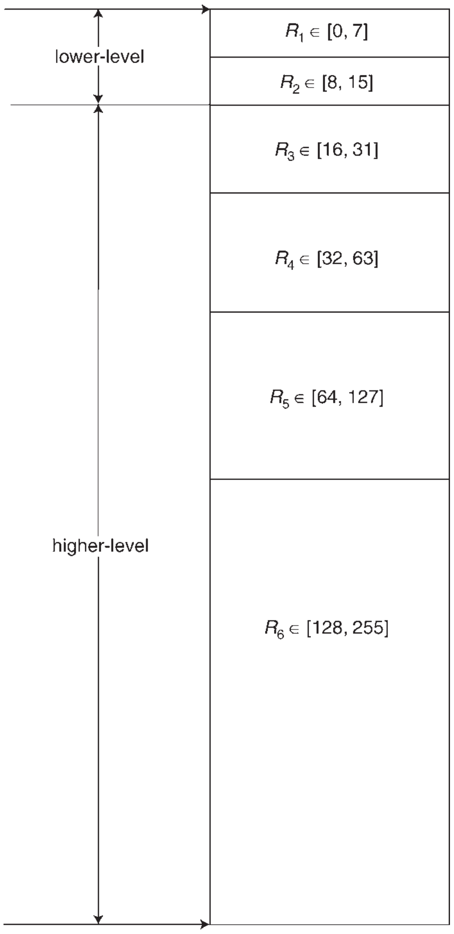

Fig. 2 *Example of division of 'lower-level' and 'higher-level'(if Div = 15)*

the secret data is hidden (such as that in Section 2.1). Or hide 6-bit secret data into two successive pixels by carrying out the next step.

Step 3: If R_i belongs to lower-level, read six bits from secret data stream, and transform grey-level value p_i, p_{i+1} into a binary value. For instance if $p_i = 30_{(10)}$, the binary value of p_i is $00011110_{(2)}$; if $p_{i+1} = 15_{(10)}$, the binary value of p_{i+1} is $00001111_{(2)}$. Next, we hide 6-bit secret data into cover image by modifying p_i and p_{i+1} according to the following procedure:

Make the 6-bit secret data $S = m_1, m_2, m_3, m_4, m_5, m_6$.

(1) Convert p_i to be p'_i by substituting 3-LSB of p_i by m_1, m_2, m_3.

(2) Convert p_{i+1} to be p'_{i+1} by substituting 3-LSB of p_{i+1} by m_4, m_5, m_6.

(3) Calculate the new difference value d'_i as follows:

$$d'_i = |p'_i - p'_{i+1}| \qquad (2)$$

(4) If $d'_i > Div$ (i.e. $d'_i \in higher - level$), then re-adjust p'_i and p'_{i+1} considering the following rule:

$$(p'_i, p'_{i+1}) = \begin{cases} (p'_i - 8,\ p'_{i+1} + 8), & if\ p'_i \geq p'_{i+1} \\ (p'_i + 8,\ p'_{i+1} - 8), & if\ p'_i < p'_{i+1} \end{cases} \qquad (3)$$

For instance, assume $p_i = 30, p_{i+1} = 15, S = 111000_{(2)}$ and $Div = 15$. After hiding, $p_i = 31, p_{i+1} = 8$, so $d'_i = 23 > Div = 15$. After re-adjusting, $p_i = 23$ and $p_{i+1} = 16$. Of course, it should be omitted with step (4) if p'_i and p'_{i+1} still belonging to the lower level.

3.2 The extracting algorithm

The following steps are executed to recover the original secret data.

Step 1: Partition the Stego-image into blocks of two consecutive pixels, and the partition procedure is identical with embedding.

Step 2: Calculate the difference value d'_i for each block of two consecutive pixels (p'_i, p'_{i+1}) of the stego-image which is given by

$$d'_i = |p'_i - p'_{i+1}| \qquad (4)$$

Step 3: Find the optimal R_i of the d'_i according to the original range table and judge the level of the optimal R_i depend by using the original set Div value. Extract secret data by using Wu and Tsai's method if R_i belongs to the higher-level and carry out the next step to extract secret data; otherwise, proceed to Step 4.

Step 4: Extract the 3-LSB of the p'_i and p'_{i+1} of the stego-image directly, so the 3-LSB of the p'_i and p'_{i+1} is represented by the hidden secret data. For instance, if $p'_i = 23$, the 3-LSB (i.e. secret data of hiding) is $111_{(2)}$; if $p_{i+1} = 16$, the 3-LSB is $000_{(2)}$.

4 Experimental results

In order to prove the feasibility of our method to raise the capacity of hiding with an acceptable quality of the stego-image, we used the MATLAB program language tool to implement the proposed idea and Wu and Tsai's scheme. The secret data stream S is generated by pseudo-random numbers. We set the range table with $w_i \in \{8, 8, 16, 32, 64, 128\}$, and Div is 15., the lower-level range is R_1, R_2, and higher-level range is R_3, R_4, R_5, and R_6. All the cover images used are sized 512×512. We utilised the peak signal-to-noise ratio (PSNR) value to evaluate the quality of the stego-images. The experimental results of the stego-images are shown in Figs. 3 and 4. Finally, the comparison of message capacity (in bytes) and PSNR value of the proposed method and Wu and Tsai's method is shown in Table 1. In order to obtain more objectivity PSNR values in Wu and Tsai's and our scheme are shown in Table 1. The PSNR value of each experimental figure is an average value by executing 1000 times in which each time the secret data stream S is different.

5 Analyses and discussions

From Table 1 we clearly see the proposed scheme has about $1.57 \sim 1.97$ greater hiding capacity than Wu and Tsai's, however, the PSNR value dropped between $0.8 \sim 5.17$ dB. Therefore, we will further analyse Wu and Tsai's method in terms of the modified rate of the cover image in this Section. There is a higher modified rate and lower PSNR values that modify more bits of the cover image than the embedding bits of the secret data. Certainly, it has higher PSNR values with lower modified rates by modifying less bits of the cover image than the hiding bits of the secret data. Generally, we consider that Wu and Tsai's method uses more bits of cover image to hide less secret data. Alternatively, their method may employ redundant bits of the cover image for hiding secret data. Hence, we can classify the quality of the stego-image in Wu and Tsai's scheme according to the following two cases.

- *Case 1:* The high PSNR value by modifying less cover image pixels. In this case, we can also comment that Wu and Tsai's scheme uses the least bit of the cover image to embed the maximum secret data. In the process of the hiding secret data, shown in Section 2.1, if the new difference value $d'_i \cong d_i$, i.e. the $m \cong 0$, the original two consecutive pixels p_i and p_{i+1} of the cover image are not completely modified. That is to say, the quality of the stego-image after embedding secret

Fig. 3 *Cover image and stego-image*

a Cover image Lena
b Stego-image after embedding secret data 95755 bytes; PSNR is 37.11 dB

Fig. 4 *Cover image and stego-image*

a Cover image Elaine
b Stego-image after embedding secret data 95023 bytes; PSNR is 37.11 dB

Table 1: Comparison of results of the proposed and Wu and Tsai's methods

	Wu-Tsai's Method		Our Method	
Cover images (512 × 512)	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)
Lena	51219	38.94	95755	36.16
Baboon	57146	33.43	89731	32.63
Peppers	50907	37.07	96281	35.34
Jet	51224	37.42	96320	35.01
Tank	50499	41.99	96089	37.38
Airplane	49739	40.13	97790	36.60
Truck	50065	42.72	96678	37.55
Elaine	51074	41.18	95023	37.11
Couple	51604	38.81	95294	36.13
Boat	52635	34.89	94596	33.62

data can still possess a high PSNR value. For example, if $d_i' = 3, d_i = 2$, then $m = 1$; only one bit will be modified of the two pixels and 3-bit secret data can be embedded into the cover image. It goes without saying that under this case Wu and Tsai's scheme can achieve high a PSNR value after hiding the secret data.

- *Case 2:* The lower PSNR value owing to modifying more cover image pixels. While the m value is larger, the amplitude of two consecutive pixels p_i and p_{i+1} will be modulated greatly. Thus, the PSNR value will reduce after hiding all secret data. In general, we can hide large secret data by modulating more bits of the cover image pixels. However, in Wu and Tsai's case, the probability of using unnecessary bits of the cover image to embed secret data may occur and then result in the drowning of the PSNR value especially in smoother areas. For instance, if $p_i = 120$ and $p_{i+1} = 120$, then $d_i = 0$. Assume $w_i = 8$ and $l_i = 0$, thus 3-bit secret data will be embedded; if the binary secret data is $111_{(2)}$, then decimal value b is 7, and thus $d_i' = 7$ and $m = d_i' - d_i = 7$. The P_i will subtract 4, while the P_{i+1} will add 3. The amount of the modified bits in the two consecutive pixels is 5 bits. Hence, in order to hide 3-bit secret data, it must use 5 bits to accomplish that. Consequently, Wu and Tsai's method will have a lower PSNR value by modifying more cover image pixels in Case 2.

In the proposed method, we make full use of the smooth areas of the cover image by using the 3-LSB replacement method to hide secret data. Thus, Case 2 will not take place in our scheme, but it is likely that Case 1 may occur. Nevertheless, the real PSNR value depends on the variety of the cover images and the secret data. In other words, the PSNR value of the cover images may be

Table 2: The same stego-image quality with more hiding capacity

	Wu-Tsai's Method		Our Method	
Cover images	Capacity	PSNR	Capacity	PSNR
(512 × 512)	(bytes)	(dB)	(bytes)	(dB)
Lena	51219	38.94	66064	38.80
Baboon	57146	33.43	68007	33.33
Peppers	50907	37.07	66032	37.50
Jet	51224	37.42	66256	37.63
Tank	50499	41.99	65695	42.80
Airplane	49739	40.13	65756	40.18
Truck	50065	42.72	65603	43.61
Elaine	51074	41.18	65724	42.16
Couple	51604	38.81	66167	39.07
Boat	52635	34.89	66622	35.01

different owing to the various types of secret data. In order to prove the use of PVD method alone may waste the PSNR value, we re-implemented the proposed scheme by using 2-LSB in smoothness. The experimental results are show in Table 2. From Table 2 we not only obtained more capacity but also the same stego-image quality as with Wu and Tsai's method.

6 Conclusions

In this paper, we have proposed a steganographic method to embed secret data into still images by using pixel-value differencing and least-significant-bit replacement methods. It embeds more secret data into edged areas than smooth areas in the cover image and has a better image quality by using PVD method alone. For the sake of increasing the capacity, we hid the secret data in the smooth areas by using an LSB method with the edged areas still using the PVD method. The experimental results demonstrate that the proposed method not only has an acceptable image quality but also can provide a large embedded secret data capacity.

7 Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC91-2213-E-324-003.

8 References

1 Hwang, M.S., Lu, E.J.L., and Lin, I.C.: 'A practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem', *IEEE Trans. Knowl. Data Eng.*, 2003, **15**, (6), pp. 1552–1560

2 Schneier, B.: 'Applied cryptography' (John Wiley & Sons, New York, 1996, 2nd Edn.)

3 Chang, C.C., Hwang, M.S., and Chen, T.S.: 'A new encryption algorithm for image cryptosystems', *J. Syst. Softw.*, 2001, **58**, (2), pp. 83–91

4 Chen, T.S., Chang, C.C., and Hwang, M.S.: 'A virtual image cryptosystem based upon vector quantization', *IEEE Trans. Image Process.*, 1998, **7**, (10), pp. 1485–1488

5 Simmons, G.J.: 'The prisoners' problem and the subliminal channel'. CRYPTO'83, 1983, pp. 51–67

6 Hartung, F., and Kutter, M.: 'Information hiding - a survey', *Proc. IEEE*, 1999, **87**, pp. 1062–1078

7 Walton, S.: 'Image authentication for a slippery new age', *Dr. Dobb's J.*, 1995, **20**, (4), pp. 18–26

8 Wang, R.Z., Lin, C.F., and Lin, J.C.: 'Image hiding by optimal LSB substitution and genetic algorithm', *Pattern Recognit.*, 2001, **34**, (3), pp. 671–683

9 Chang, C.C., Hsiao, J.Y., and Chan, C.S.: 'Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy', *Pattern Recognit.*, 2003, **36**, (7), pp. 1583–1595

10 Lee, Y.K., and Chen, L.H.: 'High capacity steganographic model', *IEE Proc., Vis. Image Signal Process.*, 2000, **147**, (3), pp. 288–294

11 Fu, M.S., and Au, O.C.: 'Data hiding watermarking for halftone images', *IEEE Trans. Image Process.*, 2002, **11**, (4), pp. 477–484

12 Tseng, Y.C., Chen, Y.Y., and Pan, H.K.: 'A secure data hiding scheme for binary images', *IEEE Trans. Commun.*, 2002, **50**, pp. 1227–1231

13 Tseng, Y.C., and Pan, H.K.: 'Data hiding in 2-color images', *IEEE Trans. Comput.*, 2002, **51**, (7), pp. 873–878

14 Wu, D.C., and Tsai, W.H.: 'A steganographic method for images by pixel-value differencing', *Pattern Recognit. Lett.*, 2003, **24**, (9-10), pp. 1613–1626