www.ietdl.org

Published in IET Signal Processing
Received on 6th August 2012
Revised on 1st November 2013
Accepted on 5th November 2013
doi: 10.1049/iet-spr.2012.0233

ISSN 1751-9675

Reversible video data hiding using neighbouring similarity

Hsiu-Lien Yeh[1], Shu-Tsai Gue[2], Piyu Tsai[2], Wei-Kuan Shih[1]

[1]Institute of Information Systems and Applications, National Tsing Hua University, Hsinchu 30013, Taiwain
[2]Department of Computer Science and Information Engineering, National United University, Miaoli 36003, Taiwan
E-mail: pytsai_1862@hotmail.com

Abstract: Recently, digital multimedia has become widely distributed in computer and network technology. For digital multimedia distribution applications, issues surrounding information security have received significant attention. Data hiding has been one of most researched issues in information security. In this paper, reversible video data hiding based on neighbouring similarity is proposed. Prediction encoding was used to compute the prediction errors. All prediction errors were explored to develop a histogram-based reversible video data hiding algorithm. The results show that the proposed approach has a higher capacity and similar embedding distortion compared with other related schemes. Also, the original video frame could be recovered after the hidden information was extracted.

1 Introduction

With the rapid development of computer and network technology, digital multimedia distribution and applications are becoming increasingly popular. After all, digital information is easily accessed, modified, and intercepted on open channels. Information security has, consequently, become an issue. Since data hiding technology provides a feasible and efficient solution, it is widely applied in applications such as copyright protection, secret communication, content authentication, and so on [1, 2].

In data hiding, the original material is taken as a cover and then secret message is embedded in it. The cover material with the secret message in it is called stego-material. The cover material can be text, image, audio, video, etc. Currently, video is one of the most popular distributed multimedia due to advances in both the Internet and portable devices. This can be seen in the popularity of the Youtube website, event data recorder (EDR) and surveillance cameras etc. Specifically, for some specialised fields disallows any kind of modifications, for instance law enforcement, military, medical diagnosis and so on. It is important to design an integrity and sensitivity of approach for these fields. Such an EDR completely records actual situations in a video content. If video data hiding support to authenticate content and protect ownership, EDR can give a more persuasive evidence in law enforcement.

Several proposed video data hiding schemes are based on motion vector [3–11]. Some of them focus on selecting candidate motion vectors (CMVs) according to a motion vector's attributes such as magnitude, phase angle [6–9]. In Zhang *et al.*'s [6] video watermarking, the watermark is embedded in the motion vector's magnitude with minimal distortion. Their scheme shows significant improvement for hiding information in the MPEG video sequence. Fang and Chang [7], like Zhang *et al.*, also selected CMVs, and utilised the phase angles between neighbouring CMVs to embed secret data. The magnitude-based selection rule is generated according to the assumption that modifications applied to MVs with larger magnitudes introduce less distortion. He and Luo's [8] scheme embedded the secret data in the phase angle difference between two consecutive CMVs. First, their scheme utilised the phase angle difference of the motion vector to analyse a data-hiding algorithm. Then they proposed a novel steganographic algorithm based on the phase of the motion vector. Hao *et al.* [9] proposed a video steganographic algorithm based on motion vector and matrix encoding. Their scheme employed the phase angle of the optimal component of the motion vector to embed the secret data. In this way, they can maintain the advantage of high utilisation rate and reduce the motion vector's modification rate.

In contrast with magnitudes-based selection, another approach was based on the associated prediction error. In Zhao *et al.*'s [10] video watermarking scheme, the watermark embedding was determined according to the optimal and minor optimal motion vectors. The motion vector is computed by using prediction algorithm. Aly's scheme [11] is directly associated with macro block (MB) prediction errors to achieve a minimum distortion. That is, the CMVs give higher prediction errors and the secret data is embedded in the least significant bits of optimal components of the CMVs.

Some data hiding schemes involve cover media recovery. When the secret is extracted, the original media can be reconstructed without distortion. This function is preferable and required in applications such as medical diagnosis, law enforcement, military affairs, and so forth. After all, reversible authentication is important to validate the originality and to verify the integrity of the media. Several reversible data hiding schemes for image and video have been proposed [12–19]. In Facciol *et al.*'s [12] scheme, an error detection codeword is embedded and detected to check the correctness of the video content and reverse the process by extracting the payload. Lin *et al.* [13] propose reversible H.264/AVC based video data hiding for error resilience. Their scheme involves the I-frame, which is the most critical frame in a GOP (Group-of-Pictures). The decoded video can recover the original video without losing any video quality.

Inspired by Ni *et al.*'s [16] and Tsai *et al.*'s [17] reversible data hiding schemes, this paper aims at designing reversible video data hiding according to neighbouring similarity. In video encoding, the motion vector and the prediction error are computed using a prediction algorithm. Accordingly, the prediction errors of similar frames are explored to develop reversible data hiding. The remainder of this paper is organised as follows: Section 2 reviews the histogram-based reversible data hiding scheme. Next, the proposed scheme is described in Section 3. In Section 4, the experimental results and analysis of the proposed scheme are demonstrated. Finally, the conclusions are given in Section 5.

2 Histogram-based reversible data hiding

In the proposed scheme, the neighbouring frames were encoded using a prediction algorithm. The prediction errors were explored to design a histogram-based reversible data hiding scheme. The histogram-based reversible data hiding scheme was proposed by Ni *et al.* [16]. They statistically calculated the occurrences of all possible image pixel values to create an image histogram. A peak and zero points pair $P(p,z)$ was selected from the histogram to determine the secret embedding. Furthermore, when the secret information was extracted the original image was fully recovered.

In their embedding procedure, $P(p,z)$ was determined according to its histogram. Assume the pixel value of the zero point is greater than that of the peak point. All of pixel (px) were scanned for secret embedding. In the first stage embedding, if the pixels whose value is greater than the peak point and less than or equals to the zero point, these pixel values are added by 1 according to (1). In the second stage embedding, all pixels scanned again. The pixel value (px) equals to the peak point, the to-be-embedded secret bit is checked according to (2). If the to-be-embedded secret bit is '1', the pixel value is changed to $px+1$. If the to-be-embedded secret bit is '0', this pixel value remains px.

$$px' = \begin{cases} px+1, & \text{if (peak} < px \leq \text{zero)} \\ px, & \text{otherwise} \end{cases} \tag{1}$$

$$px' = \begin{cases} px+1, & \text{if } (sb=1) \\ px, & \text{if } (sb=0) \end{cases}, \quad \text{if } (px = \text{peak}) \tag{2}$$

To extract the hidden secret and recover the image, $P(p,z)$ must be known by the receiver sides. The $P(p,z)$ can be attached into image file or transmitted by security channels. The pixels located at the peak point can extract the hidden secret bit 1 with the pixel value remaining. If the pixels located between $P(p,z)$ and near to the peak point by one, a hidden secret bit valued at 0 is extracted and these pixels are modified to the peak point. The other pixels located between $P(p,z)$ are shifted to the direction of the peak point by one and no secret is extracted. The remaining pixels are skipped and their values remain. After that, the secret is extracted and the original image is recovered.

The hiding capacity of this scheme is determined by the number of pixels in the peak point. The more pixels in the peak point, the higher the hiding capacity. Furthermore, the embedding distortion is small since the pixel modification is only one.

3 Proposed scheme

In the proposed scheme, the similarity of neighbouring frames is explored to obtain numerous similar prediction errors. The sharply distributed histogram of prediction errors is useful to develop a histogram shifting based reversible video data hiding scheme. The overview of the proposed scheme is shown in Fig. 1.

3.1 Embedding procedure

A video sequence generally has a high similarity between neighbouring frames. Prediction encoding is always employed to explore the similarity of neighbouring frames. In video encoding, a video sequence is generally partitioned into GOP. A GOP generally consists of IBBPBBPBBI frames. I-frames are intra-frames and encoded independently. B- and P-frames are inter-frames and encoded by using the prediction algorithm with neighbouring frames. In prediction encoding, each inter-frame is partitioned into non-overlapped macro-blocks with size of $n \times n$ pixels. The macro-block finds a closer macro-block from the referenced frames I-, B- or P-frame to encode it according to the searching algorithm.

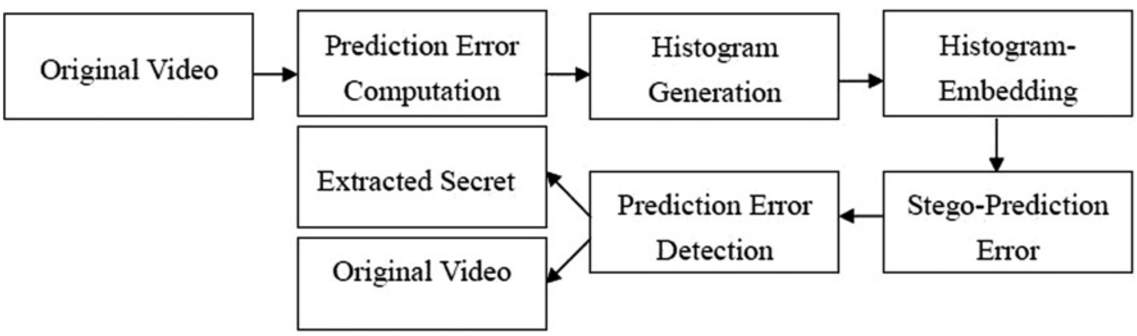

Fig. 1 *Overview of the proposed scheme*

IET Signal Process., 2014, Vol. 8, Iss. 6, pp. 579–587
doi: 10.1049/iet-spr.2012.0233

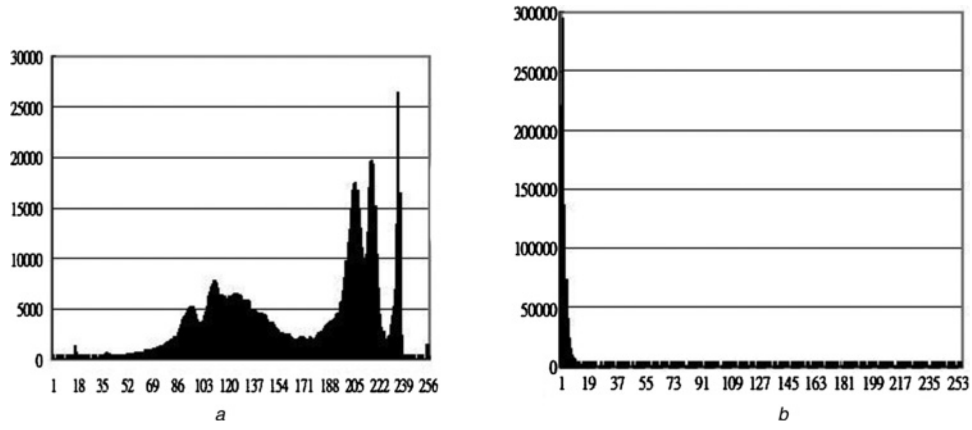

Fig. 2 *Histograms of original frame pixels and proposed prediction errors*

a Original frame pixels
b Proposed prediction errors

Several searching algorithms are proposed to determine the closest macro-block or to reduce the searching time. The motion vector and prediction error (*pe*) are computed in the encoding procedure.

Since there is a higher similarity between neighbouring frames, most of prediction errors are concentrated on a few of small and similar values. In other words, the distribution of prediction errors is abnormal and focuses on a small range. So, a sharply distributed histogram of prediction errors can be obtained. Fig. 2 showed the histograms of the original pixels and the prediction errors. From Fig. 2, it is clearly seen that shape of the prediction errors generated histogram is sharper than the original pixel generated histogram. The sharper shape histogram is used to develop a histogram shifting based reversible data hiding.

To generate a sharper shape histogram, the prediction errors of inter-frames in a GOP are collected and statistical to generate a histogram. Since, the prediction error is ranged from −255 to 255, an absolute histogram (AH) ranging from 0 to 255 can be obtained by using absolute prediction errors or one positive histogram (PH) ranging from 0 to 255 and another negative histogram (NH) ranging from −1 to −255 can be created.

Once the histogram of prediction error is generated, $P(p,z)$ pair can be determined and then a histogram shifting based reversible video data hiding scheme can be developed. In the proposed embedding procedure, we observed that we can only select the peak point and no zero point is required. In other words, the peak point and the zero point pair $P(p, z)$ used in Ni's [16] scheme can be modified to one peak point $P(p)$. This is because that most of prediction error values are nearer to the peak point and many zero points are founded. Therefore, zero point selection is unnecessary. So, the secret embedding can be performed according to (3).

$$pe' = \begin{cases} pe+1, & \text{if } (pe > p_{(p)}) \\ pe+1, & \text{if } (pe = p_{(p)} \& sb = 1) \\ pe, & \text{if } (pe = p_{(p)} \& sb = 0) \end{cases} \quad (3)$$

An example shown in Fig. 3 and Table 1 are used to demonstrate the proposed histogram generation and secret embedding/extraction and recovery procedures. Assume prediction errors, NH, PH and AH histograms are shown in Figs. 3*a*–*d*, respectively. When the histogram is generated, the peak point $P(p)$ can be determined. The selected $P(p)$ for Figs. 3*b*–*d* are (−1), (0) and (1), respectively.

Once the $P(p)$ is determined, all of prediction errors are scanned for secret embedding, according to (3). In the first stage embedding, all of prediction errors are scanned and whose values are greater than the peak point ($pe > P(p)$), these prediction error values are added by 1. In the second stage embedding, all of prediction errors are scanned again. If the prediction error value equaled the peak point ($pe = P(p)$), the to-be-embedded secret bit is checked. If the to-be-embedded secret bit is '1' ($sb = 1$), this prediction error value is modified to $pe + 1$. If the to-be-embedded secret bit is '0' ($sb = 0$), the prediction error value remains *pe*.

To demonstrate the proposed secret embedding, the PH histogram shown in Fig. 3*c* was employed and $P(p) = 0$ was determined. The stego-prediction errors were shown in Table 1(a) in which an 18-bit secret $(011010000111001000)_2$ was embedded. By comparing Figs. 3*a* and Table 1(a), it is found that the number of modified *pe* is 24 and each value modification is one. So, the embedding distortion of squared Euclidean distance (SED) is only 24.

The hiding capacity of the proposed scheme is determined according to the number of prediction errors in the selected peak point. When a higher capacity was required, both NH and PH histograms shown in Figs. 3*b* and *c* with $P(p) = -1$ and $P(p) = 0$ can provide a higher hiding capacity of 29 bits (11 bits in NH and 18 bits in PH).

To further increase the hiding capacity, the second, third, fourth peaks can be determined to extend the hiding capacity according to [17]. In our experiments, the first peak point is pixel value of 0 in PH. We can select the second and third peaks from NH and PH with peak value of −1 and 1, respectively. In multiple peak points embedding, the prediction error modification should be further considered. Assume two peak points are selected, the prediction error values located between overlapped ranges of two peaks should be added by 2. The others are only added by 1. Such that, a higher hiding capacity can be obtained but a great amount of embedding distortion incurred. For example, two peak points $P(p) = 0$ and $P(p) = 1$ are selected in PH. If $pe = 0$, which matches $P(p) = 0$, the modification of *pe* is from 0 to 1. If $pe \geq 1$, the modification of *pe* is 2 ($pe' = pe + 2$). Furthermore, if three peak points are determined, $pe \geq 2$ is modified to $pe + 3$.

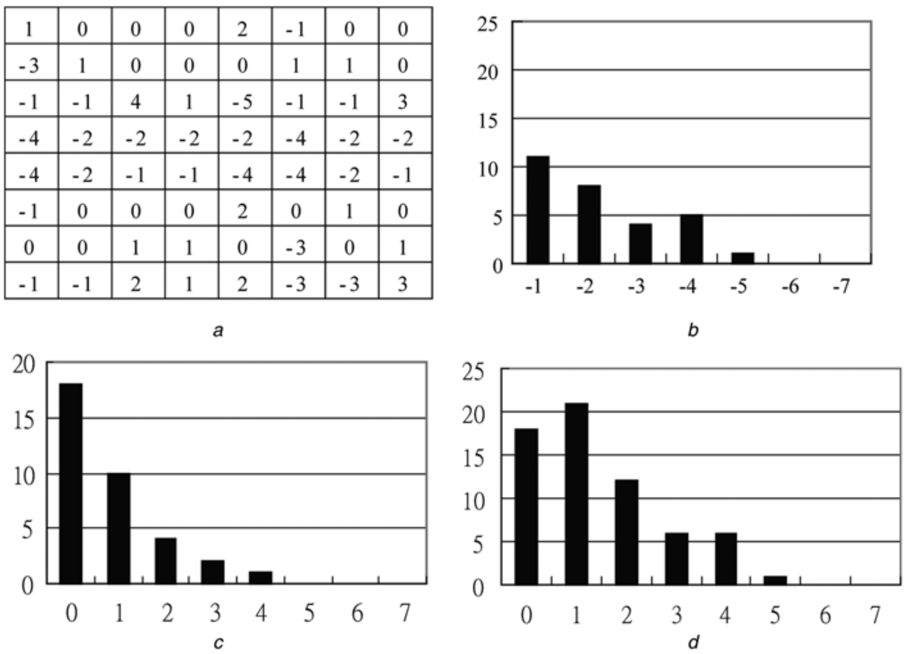

Fig. 3 *Histograms of prediction errors*

a Prediction errors
b NH histogram
c PH histogram
d AH histogram

Table 1 Sample stego- and recovered prediction errors

(a) stego-prediction error							
2	0	1	1	3	−1	0	1
−3	2	0	0	0	2	2	0
−1	−1	5	2	−5	−1	−1	4
−4	−2	−2	−2	−2	−4	−2	−2
−4	−2	−1	−1	−4	−4	−2	−1
−1	1	1	1	3	0	2	0
1	0	2	2	0	−3	0	2
−1	−1	3	2	3	−3	−3	4
(b) recovered prediction error							
1	0	0	0	2	−1	0	0
−3	1	0	0	0	1	1	0
−1	−1	4	1	−5	−1	−1	3
−4	−2	−2	−2	−2	−4	−2	−2
−4	−2	−1	−1	−4	−4	−2	−1
−1	0	0	0	2	0	1	0
0	0	1	1	0	−3	0	1
−1	−1	2	1	2	−3	−3	3

Table 2 The example of proposed macro-block searching algorithm

(a) EMB			
126	126	132	127
154	157	163	156
143	154	164	147
126	152	167	151
(b) RMB_1			
116	116	139	120
146	150	168	150
149	147	157	141
132	159	160	159
(c) RMB_2			
126	126	152	157
151	151	160	126
149	156	161	141
136	142	171	131

To extend the hiding capacity, the closest macro-block searching algorithm in proposed prediction encoding is modified to which the similarity of pixels in each macro-block is evaluated by AE (Absolute Error) computed by

$$\mathrm{AE} = |\Sigma \mathrm{RMB}_{i,j} - \Sigma \mathrm{EMB}_{i,j}|, \quad 1 < i \leqq n, \quad 1 < j \leqq n \tag{4}$$

$$\mathrm{CMB}_{i,j} = \mathrm{Max}(\mathrm{Num}(\mathrm{AE})), \quad \mathrm{AE} \leqq \mathrm{TH} \tag{5}$$

RMB is the reference macro-block, EMB is the encoding macro-block and n is the row/column size of macro-block, i and j are coordinates of row and column. The function Num (AE) is the number of AE which value is less than a threshold (TH). CMB is the searched closest macro-block that has the maximum of Num(AE). For example, an EMB shown in Table 2(a) searches a CMB from two reference macro-blocks RMB_1 and RMB_2 shown in Table 2(b) and (c), respectively and threshold (TH = 5) is defined. The Num(AE) s between (EMB, RMB_1) and (EMB, RMB_2) are 1, 7, respectively. The closest macro-block RMB_2 is searched even though the RMB_1 provides the least SED ($RMB_1{}'$ SED = 840, $RMB_2{}'$ SED = 2955). This is because the RMB_2 has an advantage to enhance the hiding capacity in the proposed scheme. If the CMB with the largest Num(AE) is not found, a RMB with the least SED given macro-block is searched.

The pseudocode of embedding algorithm with one peak point $P(p)$: A cover video is first portioned into GOPs. Each GOP frame contains $M \times N$ grayscale pixels. In GOP frames, prediction encoding is performed to obtain prediction errors $(pe) \in [-255, 255]$.

1) Generate a PH histogram from (pe) in a GOP.
2) Find a peak point $P(p) \in [0, 255]$ from PH.
3) Scan prediction errors (pe) in the same GOP. If the prediction error value is greater than $P(p)$ $(pe > P(p))$, the prediction error value is added by 1 $(pe' = pe + 1)$. .

doi: 10.1049/iet-spr.2012.0233

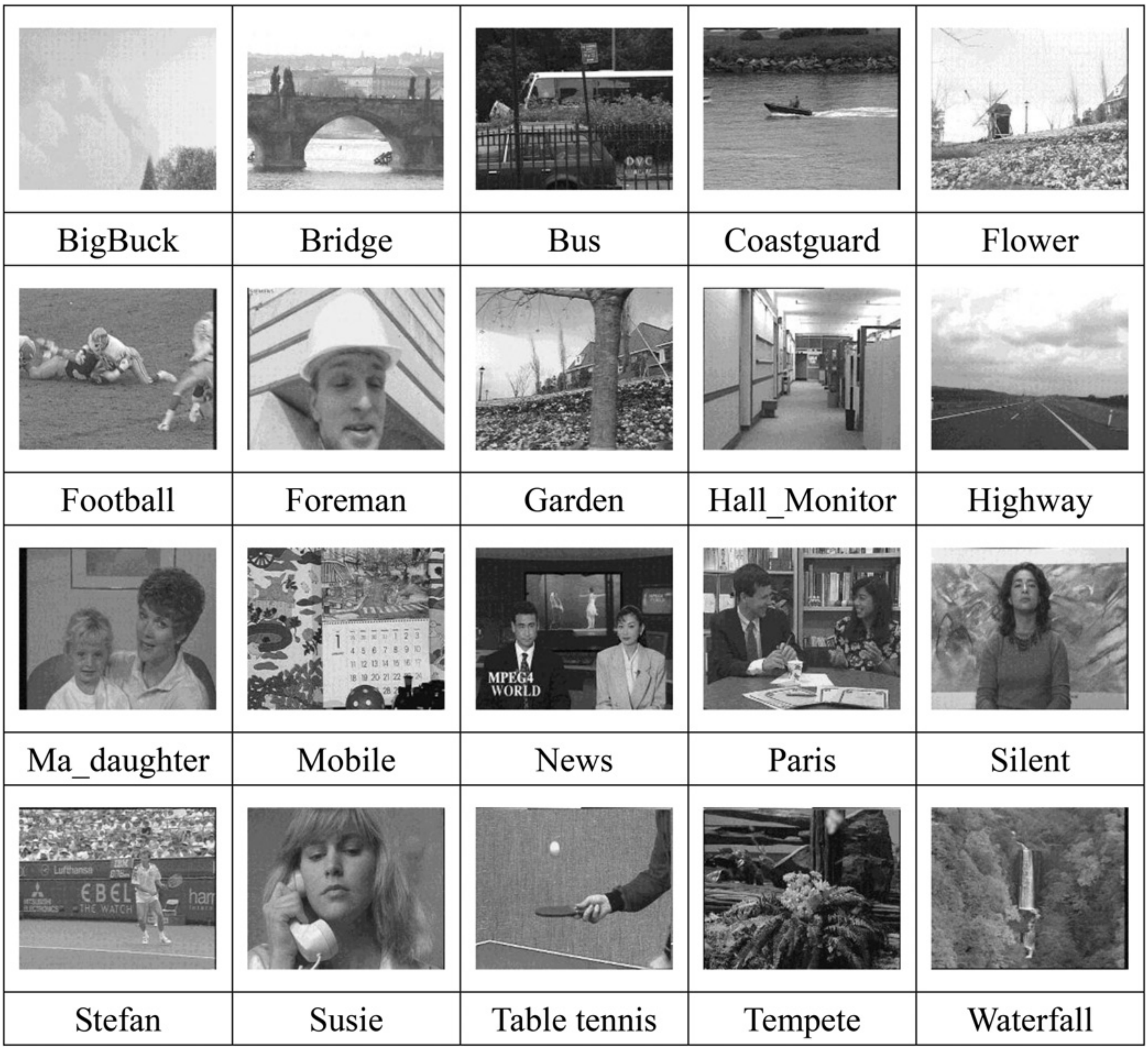

Fig. 4 *Original video frames*

4) Scan prediction errors again. If the prediction error value equals the peak point ($pe = P(p)$), check the to-be-embedded secret bit. If the to-be-embedded secret bit is '1', the prediction error value is changed to $pe + 1$ ($pe' = pe + 1$). If the to-be-embedded secret bit is '0', the prediction error value remains pe.

3.2 Extraction and recovery procedure

The proposed secret extraction and original recovery procedure is simple and efficient. To extract the hidden secret message and original reconstruction, the peak point $P(p)$ used in the embedding procedure should also be known in the extraction procedure. The stego-prediction error (pe') of a GOP was scanned to extract the hidden secret according to (6). When the hidden secret message is extracted, the original frame can be recovered according to (7). In the secret extraction procedure, the stego-prediction errors are scanned. If the stego-prediction error whose value is equal to the peak point +1 ($pe' = P(p) + 1$), a secret bit '1' is extracted ($sb = 1$). If the stego-prediction error equals the peak point ($pe' = P(p)$), a secret bit '0' is extracted ($sb = 0$). When the secret extraction is completed, the recovery procedure can be performed. If the stego-prediction error whose value is greater than the peak point ($pe' > P(p)$), the stego-prediction error is subtracted by 1 ($pe = pe' - 1$). Otherwise, the remained stego-prediction errors are preserved.

$$sb = \begin{cases} 1, & \text{if } (pe' = p_{(p)} + 1) \\ 0, & \text{if } (pe' = p_{(p)}) \end{cases} \tag{6}$$

$$pe = \begin{cases} pe' - 1, & \text{if } (pe' > p_{(p)}) \\ pe', & \text{otherwise} \end{cases} \tag{7}$$

The stego-prediction errors shown in Table 1(a) were used again to illustrate the proposed extraction and recovery procedure. The stego-prediction errors were scanned and the hidden secret message was extracted according to (6). The extracted secret $(011010000111001000)_2$ is the same as that of the embedded one. Next, the recovery procedure is performed according to (7). The recovered prediction error was shown in Table 1(b), which was the same as that of in Fig. 3*a*.

The pseudocode of extraction and recovery algorithm with one peak point $P(p)$: For each GOP, the stego-prediction errors and the peak point $P(p)$ are received before the extraction and recovery procedure is performed.

1) Scan the stego-prediction errors in the same sequential order as that used in the embedding procedure. If the stego-prediction error value equals the peak point $+1$ ($pe' = P(p) + 1$), a secret bit '1' is extracted. If the stego-prediction error value equals the peak point ($pe' = P(p)$), a secret bit '0' is extracted.
2) Scan stego-prediction error again, for any stego-prediction error whose value is greater than $P(p)$, the stego-prediction error value is subtracted by 1 ($pe = pe' - 1$).

4 Experimental results

In this experiment, twenty videos 'BigBuck', 'Bridge', 'Bus', 'Coastguard', 'Flower', 'Football', 'Foreman', 'Garden', 'Hall_Monitor', 'Highway', 'ma_daughter', 'Mobile', 'News', 'Paris', 'Silent', 'Stefan', 'Susie', 'Table tennis', 'Tempete', and 'Waterfall' with different types shown in Fig. 4 were employed to evaluate the performance of the proposed method. A GOP of each video contained 10 frames. The first frame is I-frame and the last 9 inter-frames are employed to carry the secret. Each frame contains 352×288 gray-level pixels. The encoding macro-block with different sizes of 32×32, 16×16, 8×8, and 4×4 pixels and a local searching ranged 2 pixels around the encoding macro-block were used. The proposed local searching algorithm improved the traditional local searching by considering the number of pixels with the similar values according to (5) and (6). When the number of pixels with the similar value was greater than a threshold TH, the closer macro-block was searched according to Max(Num(AE)), $\text{AE} \leq \text{TH}$. Otherwise, the traditional square Euclidean distance was computed. Then, prediction errors computed from prediction frames were used as statistics to create PH and NH histograms.

To evaluate the hiding capacity and quality of stego-frame, a bit-stream with size of 900×900 bits generated by a pseudo-random number generator (PRNG) was taken as secret message. The binary secret message was shown in Fig. 6*a*. The performance of the proposed scheme was shown in Table 3 in which only one $P(p)$ peak point was selected. From Table 3, it is seen that the average hiding capacities of different macro-block sizes provided are greater than 243 K bits and the stego-frame qualities of PSNR are larger than 51 dB. This result indicates that the proposed method can hide a large number of secret bits with imperceptibility. Also, it is noted that low motion videos 'BigBuck' and 'News' provide hiding capacity greater than 740 K, 580 K bits, respectively. Some high motion videos such as 'Bus', 'Coastguard', 'Football', 'Garden', 'Mobile', 'Table tennis' and 'Tempete' that generated hiding capacity is less than 130 K bits. Furthermore, the stego-frame qualities in all of videos are greater than 51 dB. From Table 3, it is shown that a lower motion video is useful in the proposed method to generate a higher hiding capacity and to preserve a lower embedding distortion in various macro-block sizes. In addition, the hiding capacity shown in Table 3 also indicated that the hiding capacity is decreased when the macro-block size increased. This is because the large macro-block provides a lower similarity between macro-blocks.

Fig. 5 showed the stego-frames of the proposed scheme with different secret sizes according to Table 3 by macro-block sized of 16×16 pixels. By comparing the frames shown in Figs. 4 and 5, it is difficult to distinguish the difference between the original frame and stego-frame by the human visual system.

The embedded secret message was extracted according to (6). Some of extracted secret messages were shown in Fig. 6 according to their embedded secret sizes. The extracted secret message is the same as the original one shown in Fig. 6*a*. When the embedded secret message is extracted, the prediction errors can also be recovered according to (6). The reconstructed videos were the same as the original ones as shown in Fig. 4.

Table 3 The performance of the proposed scheme with different macro-block sizes

Videos	32 × 32		16 × 16		8 × 8		4 × 4	
	Cap	PSNR	Cap	PSNR	Cap	PSNR	Cap	PSNR
BigBuck	753 203	51.00	741 019	50.90	735 090	50.81	773 121	50.53
bridge	275 791	51.14	275 791	51.15	278 707	51.16	294 788	51.15
bus	102 421	50.97	117 170	50.90	130 134	50.84	158 934	50.87
coastguard	95 486	51.14	101 481	51.15	108 525	51.18	112 137	51.17
flower	294 437	51.10	296 444	51.09	315 316	51.09	385 980	51.12
football	64 088	51.41	70 688	51.38	80 669	51.41	96 065	51.33
foreman	204 550	51.08	214 376	51.11	231 314	51.13	277 209	51.16
garden	125 895	51.11	132 137	51.13	141 808	51.12	167 098	51.14
hall_monitor	200 598	50.54	203 875	50.52	215 643	50.50	259 212	50.55
highway	218 477	51.21	226 332	51.19	244 078	51.15	285 961	51.13
ma_daughter	301 392	51.19	306 688	51.17	320 854	51.18	367 563	51.17
mobile	127 952	51.12	132 827	51.14	139 626	51.13	167 960	51.14
news	580 211	51.16	582 137	51.14	586 422	51.14	575 549	51.14
Paris	340 681	51.21	343 986	51.19	346 286	51.16	355 160	51.16
silent	342 513	51.29	342 960	51.27	346 066	51.25	369 018	51.24
Stefan	160 031	51.17	167 420	51.15	178 702	51.11	235 156	51.14
Susie	282 599	51.04	284 754	51.06	291 930	51.07	322 725	51.11
table tennis	145 448	51.09	147 871	51.08	151 329	51.08	166 659	51.09
tempete	111 996	51.10	114 267	51.02	121 045	50.95	138 112	51.04
waterfall	150 921	51.17	152 186	51.15	153 040	51.17	155 369	51.10
average	**243 930**	**51.11**	**247 721**	**51.09**	**255 829**	**51.08**	**283 189**	**51.07**

IET Signal Process., 2014, Vol. 8, Iss. 6, pp. 579–587
doi: 10.1049/iet-spr.2012.0233

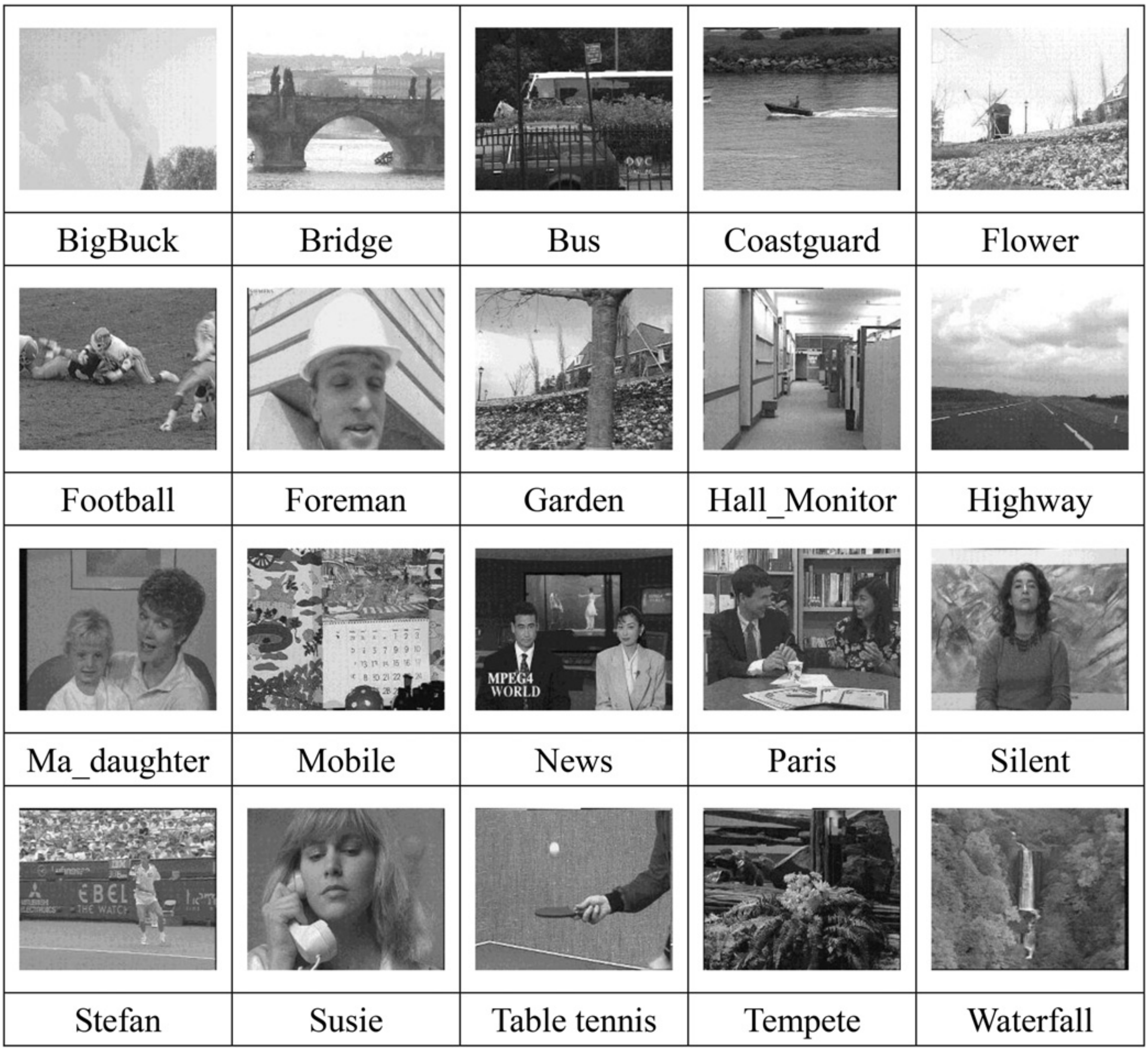

Fig. 5 *Stego-frames of the proposed scheme*

To increase the hiding capacity, more of $P(p)$ peaks could be selected in each GOP frames. The relationship between the average hiding capacity and the number of $P(p)$ peaks was shown in Fig. 7. From Fig. 7, it is shown that the hiding capacity is enhanced when the number of $P(p)$ peaks is increased. Also, it is noted that the hiding capacity is enhanced significantly when the selected $P(p)$ number is increased from 1 to 5. And then, the hiding capacity is enhanced smoothly when the $P(p)$ number is >6. This result indicates that most of prediction errors are located around peak point. Furthermore, it is shown that the smaller the macro-block size, the more the hiding capacity. However, the difference of hiding capacity among different macro-block sizes is small. In other words, the hiding capacity is stable when macro-block size is different.

To compare the performance of Tsai *et al.*'s [17], Yao *et al.*'s [18], Jeni *et al.*'s [19], and the proposed methods, a lot of simulations were performed. In Tsai *et al.*'s [17] method, the macro-block was sized of 4×4 pixels and only the macro-block self-similarity was employed in which the similarity between frames was not explored. In Yao *et al.*'s [18] scheme, integer DCT coefficients with value of 0 were used to embed the secret bit. The remained DCT coefficients larger than 0 were added one that was similar to histogram shifting modification. In Jeni *et al.*'s [19] scheme, each frame was divided into blocks sized of 2×2 pixels. Each block could embed a secret bit and the modified pixel value should be in ranged 0 to 255. The proposed method employed macro-block size of 16×16 pixels and only one peak point $P(p)$ is selected.

The experimental results of the hiding capacity (Cap) and stego-frame quality (PSNR) by Tsai *et al.*'s [17], Yao *et al.*'s [18], Jeni *et al.*'s [19], and proposed methods were shown in Table 4. In Table 4, Jeni *et al.*'s [19] method supported the largest hiding capacity and also caused the greatest embedding distortion. The other three methods preserved the similar stego-frame quality but only half hiding capacity was provided in Tsai *et al.*'s [17] method. The comparison between Yao *et al.*'s [18] and the proposed methods, it was found that the proposed scheme had a

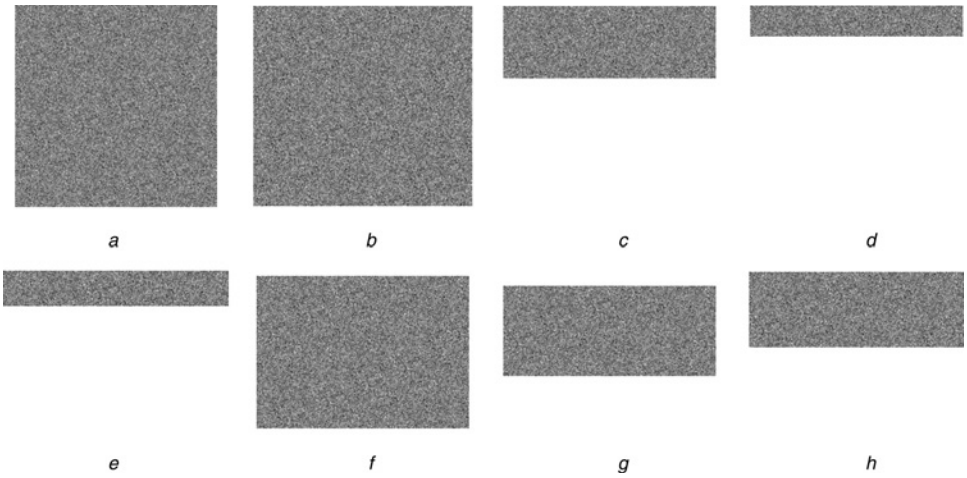

Fig. 6 *Original and extracted secret messages by the proposed scheme*

a Original secret
b From BigBuck
c From Bridge
d From Bus
e From Mobile
f From News
g From Paris
h From Susie

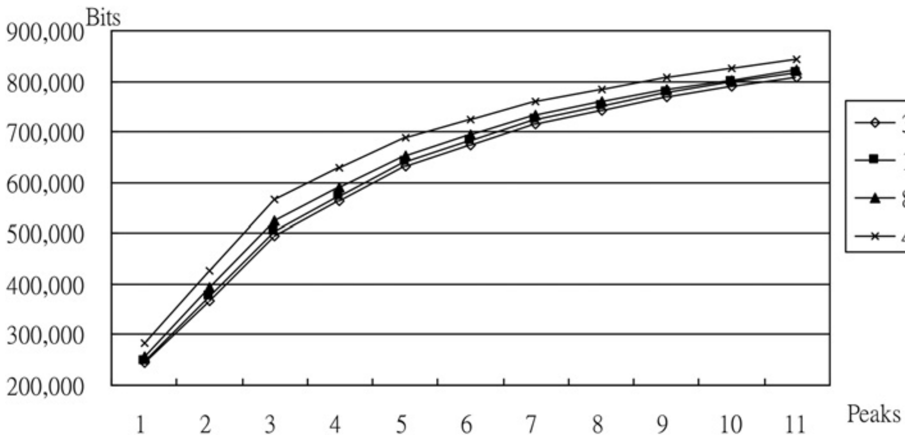

Fig. 7 *Relationship between the hiding capacity and the number of P(p) peaks*

Table 4 The performance of Tsai *et al.* [17], Yao *et al.* [18], Jeni *et al.* [19] and proposed methods

Videos	Tsai *et al.* [17]		Yao *et al.* [18]		Jeni *et al.* [19]		Proposed	
	Cap	PSNR	Cap	PSNR	Cap	PSNR	Cap	PSNR
BigBuck	552 938	51.52	104 492	54.47	253 440	46.90	741 019	50.90
bridge	200 305	51.50	123 508	52.75	253 418	39.10	275 791	51.15
bus	62 928	51.41	173 719	51.44	253 119	37.09	117 170	50.90
coastguard	34 687	51.54	184 148	51.34	253 277	40.77	101 481	51.15
flower	221 487	51.42	268 468	51.54	253 353	32.99	296 444	51.09
football	34 156	51.41	152 950	51.46	253 342	38.59	70 688	51.38
foreman	132 021	51.40	296 705	50.99	253 440	41.95	214 376	51.11
garden	68 021	51.59	197 224	51.37	252 221	29.98	132 137	51.13
hall_monitor	139 775	51.45	296 962	51.14	253 340	40.50	203 875	50.52
highway	176 789	51.31	301 699	51.09	253 440	44.43	226 332	51.19
ma_daughter	174 133	51.43	385 296	50.87	253 440	49.47	306 688	51.17
mobile	77 356	51.40	126 966	51.73	252 102	28.98	132 827	51.14
news	144 381	51.36	352 369	50.84	252 877	38.10	582 137	51.14
Paris	87 747	51.47	243 732	51.09	253 422	35.99	343 986	51.19
silent	90 881	51.33	240 280	51.11	253 393	40.50	342 960	51.27
Stefan	101 273	51.48	214 329	51.30	253 340	37.35	167 420	51.15
Susie	107 606	51.38	340 879	50.66	234 395	44.30	284 754	51.06
table tennis	42 191	51.42	110 970	51.75	253 409	36.03	147 871	51.08
tempete	54 845	51.33	159 808	51.48	251 541	30.11	114 267	51.02
waterfall	44 086	51.37	197 018	51.30	253 340	43.15	152 186	51.15
average	**127 380**	**51.43**	**223 576**	**51.49**	**252 182**	**38.81**	**247 721**	**51.09**

doi: 10.1049/iet-spr.2012.0233

better hiding capacity about 24 K bits and lost the stego-frame quality about 0.4 dB than Yao *et al.*'s [18] scheme. According that, the proposed method can provide a higher hiding capacity and preserve the similar quality with other methods.

5 Conclusions

In this paper, a reversible video data hiding based on prediction errors is presented. The improved searching algorithm is useful to obtain a larger number of similar prediction errors which is distributed in a small range. The histogram shifting scheme was applied to prediction errors and achieved the proposed reversible hiding method with a higher capacity and less embedding distortion. Only peak point is required in the histogram shifting embedding. Furthermore, the macro-block sizes and the number of peaks are adaptive to enhance the hiding capacity and to preserve the stego-video quality.

The experimental results showed that the average hiding capacity of each GOP provided is greater than 243 K bits and the average quality of stego-video is more than 51 dB. Also, the performance of the proposed method is better than the other related method in hiding capacity and preserves the similar quality.

6 References

1 Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G.: 'Information hiding — a survey', *Proc. IEEE*, 1999, **87**, pp. 1062–1078.
2 Katzenbeisser, S., Petitcolas, F.: 'Information hiding techniques for steganography and digital watermarking' (Artech House Publishers, 2000)
3 Cao, Y., Zhao, X., Feng, D., Sheng, R.: 'Video steganography with perturbed motion estimation'. Proc. Int. Conf. Information hiding, 2011, pp. 193–207
4 Pankajakshan, V., Doërr, G., Bora, P.K.: 'Assessing motion-coherency in video watermarking'. Proc. Int. Conf. ACM Multimedia and Security Workshop, 2006, pp. 114–119
5 Liu, Z., Liang, H., Niu, X., Yang, Y.: 'A robust video watermarking in motion vectors'. Proc. IEEE Int. Conf. Signal Processing, 2004, pp. 2358–2361
6 Zhang, J., Li, J., Zhang, L.: 'Video watermark technique in motion vector'. Proc. IEEE Int. Conf. Brazilian Symp. on Computer Graphics and Image Processing, 2001, pp. 179–182
7 Fang, D.Y., Chang, L.W.: 'Data hiding for digital video with phase of motion vector'. Proc. IEEE Int. Conf. Symp. on Circuits and Systems, 2006, pp. 1422–1425
8 He, X., Luo, Z.: 'A novel steganographic algorithm based on the motion vector phase'. Int. Conf. on Computer Science and Software Engineering, 2008, pp. 822–825
9 Hao, B., Zhao, L.Y., Zhong, W.D.: 'A novel steganography algorithm based on motion vector and matrix encoding'. Proc. IEEE Int. Conf. Communication Software and Networks (ICCSN), 2011, pp. 406–409
10 Zhao, Z., Yu, N., Li, X.: 'A novel video watermarking scheme in compressed domain based on fast motion estimation'. Proc. IEEE Int. Conf. Communication Technology Proc., 2003, no. (2), pp. 1878–1882
11 Aly, H.A.: 'Data hiding in motion vectors of compressed video based on their associated prediction error', *IEEE Trans. Inf. Forensics Sec.*, 2011, **6**, (1), pp. 14–18
12 Facciol, R., Farrugia, R.A.: 'Robust video transmission using reversible watermarking techniques'. Proc. IEEE Int. Conf. Symp. on Multimedia, 2010, pp. 161–166
13 Lin, S.D., Meng, H.C., Su, Y.L.: 'A novel error resilience using reversible data embedding in H.264/AVC'. Proc. IEEE Int. Conf. Information, Communications and Signal Processing, Singapore, 2007
14 Wong, K.S., Tanaka, K.: 'Complete video quality preserving data hiding with reversible functionality'. Communications, Control and Signal Processing, 2008. ISCCSP 2008. Third Int. Symp., 2008, pp. 1029–1034
15 Zeng, X., Chen, Z., Xiong, Z.: 'Issues and solution on distortion drift in reversible video data hiding', *Multimedia Tools Appl.*, 2011, **52**, (2–3), pp. 465–484
16 Ni, Z., Shi, Y.Q., Ansari, N., Su, W.: 'Reversible data hiding', *IEEE Trans. Circuits Syst. Video Technol.*, 2006, **16**, (3), pp. 354–361
17 Tsai, P., Hu, Y.C., Yeh, H.L.: 'Reversible image hiding scheme using predictive coding and histogram shifting', *Signal Process.*, 2009, **89**, (6), pp. 1129–1143
18 Yao, Y., Zhang, W., Yu, N.: 'Adaptive video error concealment using reversible data hiding'. IEEE Int. Conf. on Multimedia Information Networking and Security (MINES), China, 2012, pp. 658–661.
19 Jeni, M., Srinivasan, S.: 'Reversible data hiding in video using low distortion transform'. Int. Conf. on Information Communication and Embedded Systems (ICICES), India, 2013, pp. 211–214