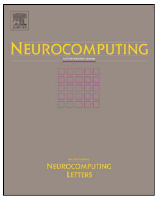
Neurocomputing 188 (2016) 63–70

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom



A reversible data hiding method for H.264 with Shamir's (t, n)-threshold secret sharing

Yunxia Liu [a,*], Liang Chen [c], Mingsheng Hu [a], Zhijuan Jia [a], Suimin Jia [a], Hongguo Zhao [b]

[a] Zhengzhou Normal University, Zhengzhou 450044, China
[b] Huazhong University of Science and Technology, Wuhan 430074, China
[c] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China

ARTICLE INFO

Article history:
Received 6 July 2014
Received in revised form
1 October 2014
Accepted 15 October 2014
Available online 11 December 2015

Keywords:
Reversible data hiding
H.264/advanced video coding (AVC)
Shamir's (tn)-threshold secret sharing
Intra-frame distortion drift

ABSTRACT

This paper proposes a new robust reversible data hiding scheme for H.264. The embedded data is first distributed into n sub-secrets with matrix equation by using Shamir's (t, n)-threshold secret sharing to improve the robustness of the embedded data. Then we choose the block with prediction mode and embed the sub-secrets into the coefficients of the 4×4 discrete cosine transform (DCT) block of the selected frames which meet our conditions to avert the distortion drift. The experimental results show that this new robust reversible data hiding algorithm can get more robustness, effectively avert intra-frame distortion drift and get good visual quality.

1. Introduction

Data hiding is a technique for embedding secret data into cover media, which can be used in many applications, such as law enforcement, perceptual transparency, medical systems, user identification, copyright protection, video indexing, and access control, etc. There exists a drawback in many data hiding methods that the cover media is permanently distorted since irreversible operations such as quantization and truncation, etc. which makes the application of data hiding prohibited in the fields of law enforcement, medical systems and perceptual transparency, etc. Then it is desired to reverse the marked media back to the original cover media without any distortions after the hidden data are extracted. The algorithm presented in [1] is the earliest reversible data hiding method. After that, many reversible data hiding schemes are proposed in [2–8]. H.264/advanced video coding (AVC) is the latest standard for video compression with high compression efficiency. It is well-adapted for network transmission which is poised to replace the existing video coding standards [9]. However, a thorough investigation of reversible data hiding scheme shows only in [10–13] for H.264 (H.264/AVC) video. Therefore, research on H.264 reversible data hiding methods is very valuable.

The robust data hiding algorithm in video is proposed since the embedded information sometimes cannot survive from network transmission, packet loss, videoprocessing operations, various attacks, and so on. The embedded data can be recovered correctly because the embedded bits can be recovered without any error. Shamir's (t, n)-threshold secret sharing(Secret sharing) has been implemented in the literature [14,15]. However, it was not built on H.264. The infinite video sequences of H.264 just meet the redundancy properties of Secret Sharing. To the best of our knowledge, the robust reversible data hiding method based on secret sharing has not been investigated to be compatible with H.264 standard. Consequently, further study and investigation are required.

Intra-frame distortion drift is a huge problem of data hiding in H.264 because this technique increases the correlation of the neighbouring blocks. When one frame is changed by data hiding, the reconstructed pixels of related frames will be influenced, i.e, intra-frame distortion drift happens. The distortion drift problem is first discussed in data hiding for compressed videos and a drift compensation method to counteract this problem is provided by Hartung and Girod [16]. Although many data hiding studies for compressed videos have employed H&G's method to restrain distortion in stego-video, the original video cannot be obtained in that schemes and those schemes are not applicable to the reversible data hiding [17–20].

The DCT coefficient of a block in an intra-frame technique is one of the most popular transform domain techniques and adopted in H.264. Data hiding for compressed media usually focuses on DCT domain since DCT is a widely used mechanism in edge-cutting compression standards such as JPEG and MPEG. A consensus intraditional algorithms for hiding data into images is "the less

[*] Corresponding author.
E-mail address: liuyunxia0110@mail.hust.edu.cn (Y. Liu).

http://dx.doi.org/10.1016/j.neucom.2014.10.109
0925-2312/© 2015 Elsevier B.V. All rights reserved.

number of modification to the DCT coefficients, the less amount of distortion in the image" [22] . However, the scheme that embed the information into the DCT coefficients of I frames into image for hiding data is not correct for H.264 video streams because of the intra frame distortion drift. Thus, it is necessary to introduce a mechanism which can hide data into in H.264.

In this section, we briefly discuss some related works on reversible data hiding,the methods presented in [10,11] and [12] are reversible data hiding, but they cannot avert the distortion drift. The method presented in [13] is a reversible data hidingmethod, which embeds the data into the DCT coefficients and can avert the distortiondrift, but it is not robust enough. Till now, there is no specific robust reversible datahiding algorithm to avert distortion drift for H.264.

In this paper, a new robust reversible data hiding scheme for H.264 is presented. In order to correct the error bits, we first use Shamir's (t, n)-threshold secret sharingbefore data hiding. In order to avert the distortion drift, we use the directions of I traframe prediction to choose 4×4 blocks which meet our conditions and embed the data into the DCT coefficients of the blocks.

The structure of the paper is organized as follows. Section 2 describes the theoretical framework of the proposed data hiding algorithm and the proposed Shamir's (t,n)-threshold algorithm. Experimental results are presented in Section 3 and we draw the conclusions of this paper in Section 4.

2. The proposed method

Since this paper focuses on the robustness and the without intra-frame distortion drift for H.264, we first introduce the correlation theory of our method, and then present the proposed algorithm as well as the corresponding theoretical analysis in detail.

2.1. Embedding procedure analysis

The integer discrete cosine transform (ICT) which is developed from the DCT is used in H.264 standard. The transform based on 4×4 blocks is shown in (1). $W_{4\times4}$, which is the 'core' part of the transform, is the matrix of unscaled DCT coefficients corresponding to the residual block.

$$W = C_f Y C_f^T \tag{1}$$

Where

$$C_f = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{pmatrix}$$

The basic forward quantizer operation is given in (2) as follow:

$$\tilde{Y} = W\cdot round\left(\frac{PF}{Q_{step}}\right) \tag{2}$$

Where Q_{step} is the quantizer step size which is determined by QP (QP is the quantization parameter) and PF is a^2 ,$\frac{ab}{2}$ or $\frac{b^2}{4}$ depending on the position (i, j) of the matrix PF as follows:

$$PF = \begin{pmatrix} a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \\ a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \end{pmatrix} \tag{3}$$

In order to simplify the arithmetic, the factor (PF/Qstep) is implemented in the reference model software as a multiplication by a factor MF and a right-shift, avoiding any division operations:

$$\tilde{Y} = round\left(W\cdot\left(\frac{MF}{2^{15+floor(\frac{QP}{6})}}\right)\right) \tag{4}$$

where

$$\frac{MF}{2^{15+floor(\frac{QP}{6})}} = \frac{PF}{Q_{step}}$$

At the decoder, after the re-scaling step as depicted in (5), the inverse ICT and the post-scaling step as described in (6), we can get the residual block.

$$W' = \tilde{Y}\cdot Q_{step}\cdot PF\cdot 64 \tag{5}$$

$$R' = round(C_i^T W' C_i/64) \tag{6}$$

In data hiding algorithm, the encoded information is embedded into the quantized luminance DCT coefficients as in (7):

$$\tilde{Y}' = \tilde{Y} + \Delta \tag{7}$$

Where $\Delta_{4\times4}$ is the error matrix added to the quantized DCT coefficient matrix $\tilde{Y}_{4\times4}$ by data hiding $\Delta = (\alpha_{i,j})_{4\times4}$.

After the re-scaling step as depicted in (8), the inverse ICT and the post-scaling step as described in (9) of the decoder, we can get R″ the residual block after embedding.

$$W' = \tilde{Y}\cdot Q_{step}\cdot PF\cdot 64 = \tilde{Y}\cdot Q_{step}\cdot PF\cdot 64 + \Delta\cdot Q_{step}\cdot PF\cdot 64 \tag{8}$$

$$R'' = round(C_i^T W' C_i/64) = round((C_i^T(\tilde{Y}\cdot Q_{step}\cdot PF)C_i) + C_i^T(\Delta\cdot Q_{step}\cdot PF)C_i) \tag{9}$$

The deviation of the pixel luminance value between the original block and the one after embedding is $E_{4\times4}$, where $E_{4\times4} = (e_{ij})_{4\times4}$, which can be calculated according to (10).

$$\begin{aligned} E = R'' - R' &= round((C_i^T(\tilde{Y}\cdot Q_{step}\cdot PF)C_i) + C_i^T(\Delta\cdot Q_{step}\cdot PF)C_i) \\ &\quad - round(C_i^T(\tilde{Y}\cdot Q_{step}\cdot PF)C_i) \end{aligned} \tag{10}$$

Using B ($B = (b_{ij})_{4\times4}$) to express $C_i^T(\Delta\cdot Q_{step}\cdot PF)C_i$, we have

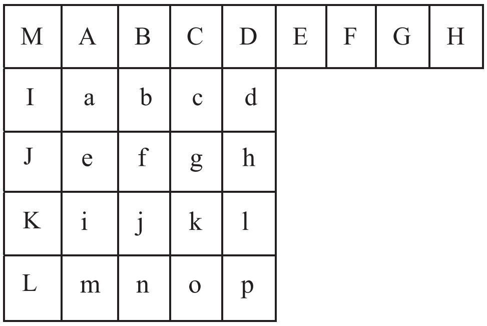
$$e_{i,j} = round(b_{i,j})\cdot or\cdot round(b_{i,j}) \mp 1 \tag{11}$$

Especially if $b_{i,j} = 0$, then $e_{i,j} = 0$.

2.2. Intra-frame prediction

A prediction block of H.264 intra prediction method is formed based on previously encoded adjacent blocks [9].The sixteen pixels in the 4×4 block ((from a to p in Fig.1) are predicted by using the boundary pixels of the upper and left blocks which are previously obtained (from A to M), which use a prediction formula corresponding to the selected optimal prediction mode.

There are nine prediction modes for each luminance 4×4 block and four modes for each 16×16 luminance block. Fig.2 and Fig.3 describe these prediction modes respectively [9].



M	A	B	C	D	E	F	G	H
I	a	b	c	d				
J	e	f	g	h				
K	i	j	k	l				
L	m	n	o	p				

Fig. 1. Labeling of prediction samples [9].