

Forensics and counter anti-forensics of video inter-frame forgery

Xiangui Kang^{1,2} · Jingxian Liu² · Hongmei Liu² ·
Z. Jane Wang³

Received: 31 January 2015 / Revised: 14 May 2015 / Accepted: 17 June 2015 /
Published online: 12 July 2015
© Springer Science+Business Media New York 2015

Abstract Among different types of video manipulations, video inter-frame forgery is a powerful and common tampering operation. Several forensic and anti-forensic techniques have been proposed to deal with this challenge. In this paper, we first improve an existing video frame deletion detection algorithm. The improvement is attributed to the combination of two properties resulted from video frame deletion, the periodicity and the magnitude of the fingerprint in the P-frame prediction error. We then analyze a typical anti-forensic method of video frame deletion, and prove that the fingerprint of frame deletion still can be discovered after being anti-forensically modified. We thus further propose a counter anti-forensics approach by estimating the true prediction error and comparing it with the prediction error stored in videos. We show that the detection algorithm is not only useful in detecting video frame deletion, but also useful for detecting video frame insertion. Compared with the existing counter anti-forensics, our proposed approach is robust when different motion estimation algorithms are used in the initial compression. Furthermore, the forensics and counter anti-forensics are combined to perform a two-phase test to detect video inter-frame forgery. A Video Inter-frame Forgery (**VIF**) game, which is zero-sum, simultaneous-move, is defined to analyze the interplay between the forger and the investigator. Mixed strategy Nash equilibrium is introduced to solve the **VIF** game and we can obtain

✉ Xiangui Kang
isskxg@mail.sysu.edu.cn

Jingxian Liu
liujx3@mail2.sysu.edu.cn

Hongmei Liu
isslhm@mail.sysu.edu.cn

Z. Jane Wang
zjanew@ece.ubc.edu

¹ College of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, JS 210044, China

² School of Information Science & Technology, Guangdong Key Lab of Information Security technology, Sun Yat-Sen University, Guangzhou, GD 510006, China

³ Electrical and Computer Engineering Department, University of British Columbia, Vancouver, Canada

the optimal strategies for both players. Experimental results show that the proposed forensic and counter anti-forensic methods not only outperform existing methods in detecting frame deletion and anti-forensics, but also outperform them in the **VIF** game.

Keywords Video forensics · Inter-frame forgery · Counter anti-forensics · Mixed strategy Nash equilibrium

1 Introduction

In recent years, with the advances of multimedia devices (such as digital cameras, cell phones and laptops), digital video contents have profoundly changed our daily life. Digital video is widely used for security purposes, news report, as well as judicial evidences in court. However, powerful digital editing software allows for easy copying, editing and distributing digital video contents. Consequently, the authentication and validation of a given digital video have become increasingly difficult, due to possible diverse sources and the potential manipulations that could have been operated [15]. Integrity and authenticity of video contents have been an active topic in digital multimedia forensics [18].

Due to the mass storage requirements of uncompressed digital videos, most digital videos will be compressed before storage and transmission. Because existing video editing tools do not work directly in the compressed domain, every time a video is to be manipulated, it has to be decompressed first, manipulated and then recompressed. Several methods [2, 10, 13, 14, 22, 25] have been proposed to detect video recompression. The work in [22] presented a method to estimate the size of Group of Pictures (GOP) during the first compression based on the Variation of Prediction Footprint (VPF), and [4] further increased the robustness of VPF so that it can be exploited to detect inter-frame video tampering. Inter-frame forgery is one of the most common manipulations. For example, in order to conceal the appearance of a suspicious object or human in a surveillance video, the forger would delete frames from the video. Papers [3, 24] exposed inter-frame forgery based on the consistency of the optical flow and the velocity field. However these methods are limited to be applicable moving targets in videos. The work in [23] exposed inter-frame forger with the P-frame prediction error sequence. Based on the P-frame prediction error sequence, [12] proposed a time-domain feature of video frame deletion.

Although, these forensic techniques are quite effective in detecting digital manipulations, many of them may fail if a forger uses anti-forensic techniques. Anti-forensic techniques are designed to mislead forensic analysis by concealing or removing fingerprints left by tampering operations. An anti-forensic technique can't introduce obvious distortion into the tampered multimedia content. Reference [21] proposed a frame deletion anti-forensic technique by purposely increasing the prediction error, and [19] ameliorated the process of increasing the prediction error. Nevertheless, the operation of modifying videos anti-forensically may leave detectable fingerprints, so the forger must balance the anti-forensic strength. Meanwhile, the forensic investigator attempts to detect the fingerprints left by tampering and anti-forensic modification. Game theoretic frameworks [1, 19, 20, 26] had been explored to analyze the interplay between a forensic investigator and a forger.

In this paper, we deal with the problem of video inter-frame forger. The main contributions of this work can be summarized as follows. Firstly, we analyze the frame deletion detection algorithm in [12], and propose an improved algorithm by addressing the potential weakness in [12]. Secondly, a robust counter anti-forensic technique is proposed. Although papers [19, 21]

modify the prediction errors stored in the video, the true prediction errors presented in the video do not change. In the proposed counter anti-forensics, we estimate the true prediction error and analyze the discrepancies between the true prediction error and the prediction error stored in the video. Compared with the counter anti-forensic technique in [19], the proposed technique is robust to different motion vector searching algorithms. Thirdly, forensics and counter anti-forensics are combined into a two-phase test to determine whether a video has been manipulated. A Video Inter-frame Forgery (VIF) game is formulated to analyze the interplay between the forensic investigator and the forger. Different from the game in [19], the proposed VIF game removes the assumption that the forensic investigator moves first and then the forger responds. In our case, the investigator and the forger simultaneously move, which is more suitable in practical scenarios. The game theoretic analysis is performed under *Mixed Strategy Nash Equilibrium*.

The rest of this paper is structured as follows. In Section 2, we propose an improved frame deletion detection algorithm based on [12]. In Section 3, a counter anti-forensic technique is proposed. Section 4 evaluates the performance of both players under mixed strategy Nash Equilibrium. Section 5 shows the experimental results of the proposed methods. Finally, the conclusions are drawn in Section 6.

2 The improved frame deletion detection algorithm

We begin this section with a brief overview of the video frame deletion fingerprints left in the P-frame prediction error sequence. Then a popular frame deletion detection algorithm [12] is introduced and an improved version of [12] is proposed.

2.1 Video frame deletion fingerprint

Nowadays, though a variety of different video compression techniques exist, such as MPEG-2 [7], MPEG-4 [8], H.264 [9] and HEVC [11], they share the same basic idea. In each Group of Pictures (GOP), frames are assigned to one of the three types according to the manner in which they are predicted and compressed. These frame types are: intra-frames (I-frame), predicted-frames (P-frame) and bidirectional-frames (B-frame).

When frames are deleted from a digital video, each GOP in the recompressed video will correspondingly contain frames belonging to different GOPs defined in the initial compression, which can be declared as the offset of frame phases. It was demonstrated in [23] that, because these P-frames and their anchor frames are not correlated, the prediction errors become relatively larger. The P-frame prediction error sequence can be measured as follows [19]:

$$e(n) = \frac{1}{N_{xy}} \sum_x \sum_y |P_{x,y}(n)| \quad (1)$$

where N_{xy} is the number of pixels in each frame, $P_{x,y}(n)$ is the prediction error of the n^{th} P-frame, at pixel location (x, y) , $n \in [1, N]$ and N is the total number of P-frames in a video.

The variation in the P-frame prediction error sequence is periodic, which leads to peaks in the Discrete Fourier Transform (DFT) $\{E(k)\}$ of the sequence $\{e(n)\}$. Figure 1 shows an example of frame deletion. The video ‘Akiyo’ is compressed using a fixed GOP structure *IBBPBBPBBPBP*, QP (Quantization Parameter) is 8 for I-frames and QP is 10 for P-frames

and B-frames. Figure 1a is the P-frame prediction error sequence of 250 frames of a compressed version of the video ‘Akiyo’, and Fig. 1b shows the corresponding DFT of this P-frame prediction error sequence. Figure 1c is the P-frame prediction error sequence of the same video after the first frame is deleted, and we can see two peaks in the DFT of this sequence as shown in the Fig. 1d.

2.2 An existing detection algorithm

As mentioned above, the P-frame prediction error sequence $e(n)$ increases periodically after frame deletion. The period T of $e(n)$ is equal to the total number of P-frames within a GOP [19]. In this paper, we limit to the scenario that the forger delete or insert frames from a video and then recompress it with the same GOP, so T is known for both the investigator and the forger. Reference [12] proposed a frame deletion detection algorithm by measuring the periodicity of the P-frame prediction error sequence.

Denote N_G to be the number of GOPs within a video, and partition $e(n)$ into N_G portions with the period T . Consequently, each portion contains T elements. Then the index positions of the maximum element in each portion are stored in a vector \mathbf{v} ($v_i \in \mathbf{v}, i \in \{1, 2, \dots, N_G\}$). The vector \mathbf{s} ($s_j \in \mathbf{s}, j \in \{1, 2, \dots, T\}$) is the occurrence frequency of $v_i=j$ in the vector \mathbf{v} . μ is the mean value of \mathbf{s} and σ^2 is the variance of \mathbf{s} . The relationship among them is:

$$\sum_{j=1}^T s_j = N_G \tag{2}$$

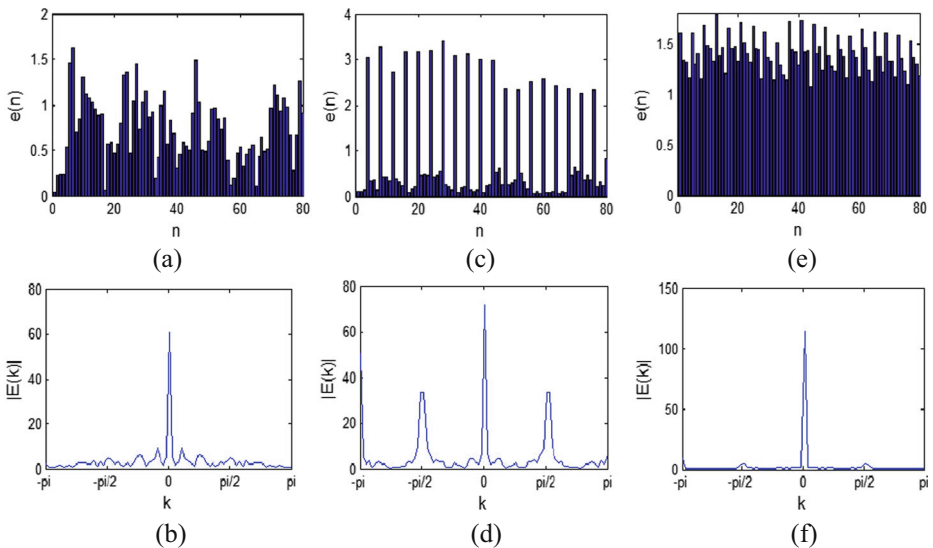


Fig. 1 (a) P-frame prediction error sequence of the unaltered compressed video ‘Akiyo’. (b) The corresponding DFT of the error sequence in (a). (c) P-frame prediction error sequence of the same video after the first frame was deleted followed by recompression. (d) The corresponding DFT of the sequence in (c). (e) P-frame prediction error sequence of the unaltered compressed video ‘Bridge-close’. (f) The corresponding DFT of the sequence in (e)

$$\mu = \frac{\sum_{j=1}^T s_j}{T} = \frac{N_G}{T} \tag{3}$$

$$\sigma^2 = \frac{\sum_{j=1}^T (s_j - \mu)^2}{T-1} \tag{4}$$

If frames are deleted from a video, the index positions of the maximum element in each portion are relatively consistent, so a certain element in s will be obviously larger than other elements in s . If and only if one element in s is equal to N_G and all other elements in s are equal to zero, σ^2 reaches its maximum:

$$\sigma_{\max}^2 = \frac{(N_G - N_G/T)^2 + (T-1)(N_G/T)^2}{T-1} \tag{5}$$

Equation (5) can be easily derived from (2) - (4). Finally, the time-domain feature is defined as:

$$Q_t = \frac{\sigma^2}{\sigma_{\max}^2} \tag{6}$$

It is easy to demonstrate that $Q_t \in [0, 1]$. The time-domain feature Q_t of a video with frame deletion is much larger than that of the video without frame deletion [12].

2.3 The improved detection algorithm

Although the aforementioned frame deletion detection can effectively measure the periodic increase in the P-frame prediction error sequence, it does not examine the magnitude of the increase. Figure 1e presents the prediction error of the unaltered video ‘Bridge-close’ which is compressed with the same setting as in the video ‘Akiyo’, and Fig. 1f shows the corresponding DFT. For this example, accidentally, the largest prediction errors have the same index in each GOP (e.g., the first prediction error is the largest one within every GOP in this video). As a result, $Q_t=1$ for this video, meaning that this video will be misclassified as a tampered video.

Actually, the maximum prediction error caused by frame deletion will be obviously larger than other prediction errors within a GOP. In order to avoid the above misclassification, we measure the maximum prediction error in each portion. If the maximum prediction is not big enough, the position of the maximum element in that portion is replaced by a random value, so the accidental periodicity is destroyed. Denote that e_1 is the maximum prediction error in one portion, and e_2 is the minimum prediction error in the same portion. The vector v' is obtained as follows.

$$v'_i = \begin{cases} v_i, & \text{if } e_1 > \alpha e_2 \\ \text{Rand}(T), & \text{otherwise} \end{cases} \tag{7}$$

where $i \in \{1, 2, \dots, N_G\}$. $\text{Rand}(T)$ is a stochastic function, which randomly chooses one value from the uniform distributed set $\{1, 2, \dots, T\}$. $\alpha > 0$ is an empirical constant, and we set $\alpha=1.5$ in our experiments.

Then, we use v' instead of v and repeat the above procedure in 2.2. An improved time-domain decision statistic I_t is calculated via (6), i.e., $I_t = \frac{\sigma^2}{\sigma_{\max}^2}$. A threshold τ_d is used to classify

the video in question. If $I_t < \tau_d$, the video is classified as unaltered. Otherwise, the video is classified as tampered with frame deletion. Additionally, frame insertion can be regarded as deleting a negative number of frames, so this detection algorithm is also applicable for video frame insertion. We define this improved frame deletion detection algorithm as δ_d .

3 Counter anti-forensics of frame deletion

Anti-forensics is designed to remove the fingerprint of tampering operation; meanwhile, anti-forensic operations may inadvertently leave behind their own fingerprints. In this section, we first introduce a typical anti-forensics [19, 21] for video frame deletion, and then a counter anti-forensic method is proposed to detect this anti-forensics.

3.1 Frame deletion anti-forensics

In order to make the manipulation of frame deletion undetectable, the forger must remove the footprint that can be revealed by the P-frame prediction error sequence. Generally, video encoders attempt to minimize the total prediction error, so that they would create a highly accurate prediction for each frame. When a less accurate prediction technique is used, the total prediction error for a certain frame would increase. In other words, the prediction error for a frame can be increased by purposefully choosing motion vectors that yield a poor predicted frame. Reference [19, 21] proposed an anti-forensic method by modifying the encoding process so that the P-frame prediction error sequence stored in the video would conceal the fingerprint of frame deletion. The procedure is as follows:

Firstly, a target P-frame prediction error sequence $\tilde{e}(n)$ that is independent of the fingerprint of frame deletion is constructed. An example of $\tilde{e}(n)$ is illustrated in Fig. 2a, where the fingerprint of frame deletion has been removed. Secondly, the motion vectors of certain macro-blocks are selectively set to zero and then the prediction error associated with those macro-blocks is recalculated so that the actual prediction error matches the target one. If the target prediction error for a particular P-frame is larger than the error incurred by setting all of the frame's motion vectors to zero, the corresponding set of motion vectors that maximize the prediction error associated with each macro-block are searched first. The work in [19] modified the method of increasing the prediction error. Rather than setting several of its motion vectors to zero, [19] instead fix a search radius with an initial value of one pixel around the true motion vector. If the target prediction error is not achievable using current motion vector search radius, the search radius is increased by one pixel and the search procedure is repeated.

Figure 2a shows the P-frame prediction error sequence of 'Akiyo' that has been anti-forensically modified after the first frame is deleted, and Fig. 2b shows its corresponding DFT. It is observed that DFT peaks disappear after using the anti-forensic technique, meaning that the aforementioned technique can effectively conceal the fingerprint left by frame deletion.

3.2 Counter anti-forensics of video frame deletion

Though the anti-forensics in [19, 21] work effectively in concealing the periodic fingerprint in the P-frame prediction error sequence, it does not change the true prediction error presented in the tampered video, indicating that the frame deletion fingerprint still can be extracted. We

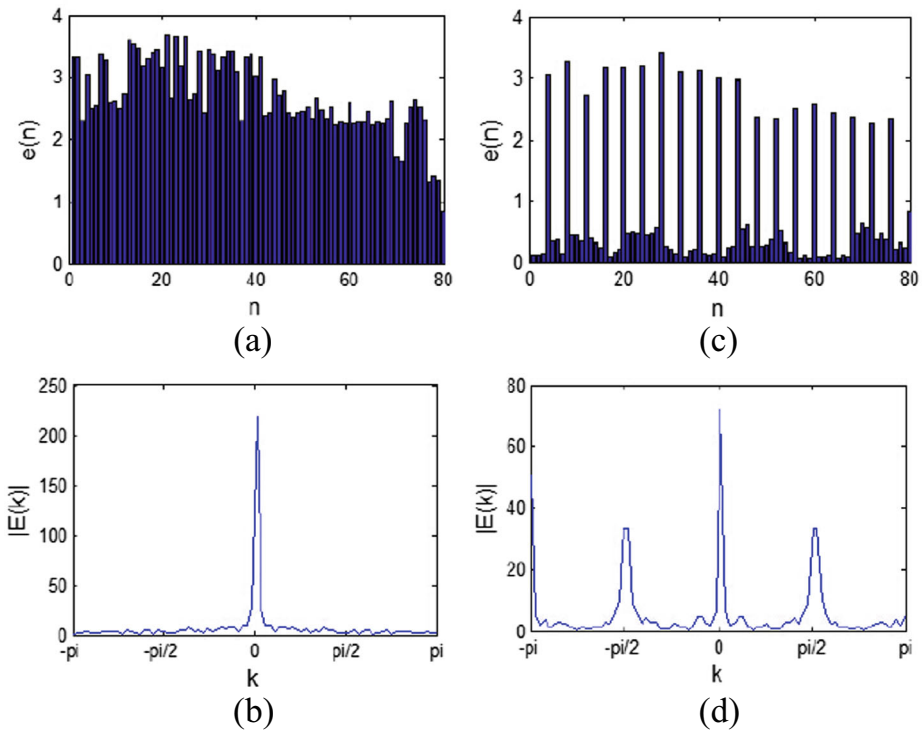


Fig. 2 (a) The P-frame prediction error sequence of the anti-forensically modified video ‘Akiyo’. (b) The corresponding DFT of the sequence from (a). (c) The estimated P-frame prediction error sequence of the anti-forensically modified video ‘Akiyo’. (d) The corresponding DFT of the sequence from (c)

propose a counter anti-forensics of frame deletion by estimating the true prediction error and measuring the discrepancies between the estimated prediction error and the stored prediction error.

The true P-frame prediction error sequence estimated from the anti-forensically modified video will have similar properties as the one without using anti-forensics. This observation is justified as follows.

Let P_j be a frame to be predicted. F_i is an anchor frame, and E_j is the prediction error of P_j . The relation among them is:

$$E_j = P_j - M(F_i) \tag{8}$$

where $M(\cdot)$ denotes the process of standard motion estimation and motion compensation. Ref. [19, 21] used a low accurate motion estimation to increase the prediction errors, and this process is denoted as $M'(\cdot)$. So we have:

$$E'_j = P'_j - M'(F'_i) \tag{9}$$

where P'_j and F'_i denote the frame to be predicted and the anchor frame in the anti-forensically modified video respectively. E'_j is the prediction error. E'_j can be converted into a single indicator for the P-frame prediction error sequence $e'(n)$ with (1). By compressing the whole

video in this way, $e'(n)$ will not present the periodic fingerprint of frame deletion, and the effect can be seen in Fig. 2(a) and (b).

However, as mentioned in Section 1, an anti-forensic technique must not introduce an unacceptable amount of distortion into the anti-forensically modified video. It means that the anti-forensically modified frame should be almost the same as the standard compressed frame. As a result, we get $\mathbf{P}'_j \approx \mathbf{P}_j$, $\mathbf{F}'_j \approx \mathbf{F}_j$. To estimate the true P-frame prediction error, we recompress the questionable video with a standard motion estimation and motion compensation:

$$\mathbf{E}''_j = \mathbf{P}'_j - M(\mathbf{F}'_i) \quad (10)$$

where \mathbf{E}''_j is the estimated prediction error. Comparing (8) with (10), we get $\mathbf{E}''_j \approx \mathbf{E}_j$. In another word, the true P-frame prediction error sequence is almost the same as that of the tampered video without anti-forensic modification. Therefore, it still exhibits a periodic pattern induced by frame deletion.

An example is presented in Fig. 2, where we estimate the true prediction error sequence from the anti-forensically modified video ‘Akiyo’ and calculate the DFT of this sequence. In Fig. 2d, in addition to the DC component, two more peaks occur again. Therefore, we can use this to detect the anti-forensic technique. The procedure of our counter anti-forensics is presented as follows:

Firstly, the estimated true prediction error sequence is obtained by recompressing the video in question with a standard motion estimation and motion compensation approach. Secondly, the improved time-domain statistic of the prediction error stored in the video and estimated error recalculated from the questioned video are computed using the algorithm in Section 2. Let $e'(n)$ denote the stored P-frame prediction error sequence and $e''(n)$ denote the recalculated estimated sequence. I'_t and I''_t are the improved time-domain statistic computed with $e'(n)$ and $e''(n)$ respectively. Finally, we measure the Absolute Deviation of these two statistics as:

$$d_t = |I'_t - I''_t| \quad (11)$$

The value of I'_t is relatively small for both unaltered video and anti-forensically modified video. If the video in question has not been anti-forensically modified, $e''(n)$ will not present the periodic pattern, so I''_t should be close to I'_t . Hence, d_t will be close to zero. However, if the video in question has been anti-forensically modified, d_t will be relatively large. A threshold τ_c is used to classify the video in question. If $d_t < \tau_c$, the video is classified as without being anti-forensically modified. Otherwise, the video is classified as being anti-forensically modified. We define this counter anti-forensics as δ_c for further discussion.

4 Game theoretic evaluation of video forensics and anti-forensics

By integrating forensics and counter forensics, a two-phase test is established, which is illustrated in Fig. 3. The forensic investigator will balance the false alarm rate for both detecting frame deletion and detecting the use of anti-forensics that maximizes the probability of detecting a forgery under a given total false alarm rate. On the other side, the forger must choose a proper anti-forensic attack strength to minimize the probability that either the frame deletion or the use of anti-forensics will be detected. In this section, we use Game theory [6, 16] to analyze the interplay between the forensic investigator and the forger.

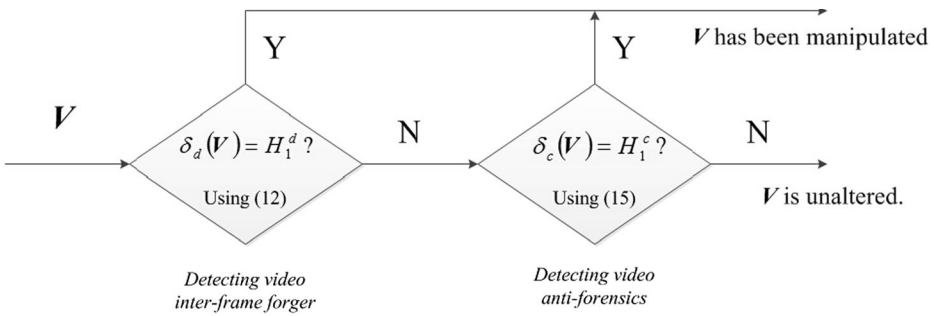


Fig. 3 The diagram of the proposed two-phase test

4.1 The two-phase test

1) The first phase. The forensic investigator firstly determines whether a digital video V has undergone frame deletion using the detection algorithm δ_d in Section 2. The problem can be expressed as a hypothesis test.

$\delta_d(\mathbf{V})=H_0^d$ The compressed video V has not undergone frame deletion. The subscript ‘0’ denotes the null hypothesis and the superscript ‘d’ denotes detecting the manipulation of frame deletion.

$\delta_d(\mathbf{V})=H_1^d$ The compressed video V has undergone frame deletion, and recompressed with the same GOP as the previous compression.

Let $I_t(\mathbf{V})$ be the improved time-domain statistic of the video V . The acceptance region of H_1^d is:

$$\mathbf{V} : I_t(\mathbf{V}) > \tau_d \tag{12}$$

where the threshold τ_d is chosen according to the false alarm rate P_{fa}^d , which is defined as:

$$P_{fa}^d = P(\delta_d(\mathbf{V}) = H_1^d | \mathbf{V} \text{ has not undergone frame deletion}) \tag{13}$$

2) Second phase. If the videos are accepted in H_0^d , the investigator will further adopt the counter anti-forensics δ_c in Section 3 to test if the video had been anti-forensically modified. Just like the previous stage, this problem can also be modeled as a hypothesis test.

$\delta_c(\mathbf{V})=H_0^c$ The compressed video V is unaltered, i.e., V has neither undergone frame deletion nor anti-forensically modified. The superscript ‘c’ denotes the counter anti-forensics.

$\delta_c(\mathbf{V})=H_1^c$ The compressed video V has undergone frame deletion and anti-forensically modified and recompressed with the same GOP as the initial compression.

For the proposed counter anti-forensics in Section 3, the acceptance region of H_1^c is:

$$\mathbf{V} : d_t(\mathbf{V}) > \tau_c \tag{14}$$

where the decision threshold τ_c is chosen based on the false alarm rate P_{fa}^c , which is defined as:

$$P_{fa}^c = (\delta_c(\mathbf{V}) = H_1^c | \mathbf{V} \text{ is unaltered}) \tag{15}$$

The total decision rate of the complete forensics can be denoted as:

$$P_d = P(\delta_d(\mathbf{V}) = H_1^d \cup \delta_c(\mathbf{V}) = H_1^c | \mathbf{V} \text{ has been manipulated}) \tag{16}$$

It is the probability that we detect the compressed \mathbf{V} has undergone frame deletion or anti-forensically modified under the condition that \mathbf{V} has been modified. Obviously, the forger wants to minimize the detection rate P_d , while the investigator wants to maximize the detection rate P_d . The total probability of false alarm rate is defined as:

$$P_{fa} = P(\delta_d(\mathbf{V}) = H_1^d \cup \delta_c = H_1^c | \mathbf{V} \text{ is unaltered}) \tag{17}$$

For a given total false alarm rate $P_{fa} = \xi$, the investigator's strategy is to allocate the false alarm rate for $P_{fa}^d = \hat{\xi}$, ($\hat{\xi} \in [0, \xi]$) to detect video frame deletion. The corresponding false alarm rate $P_{fa}^c = \xi - \hat{\xi}$ allocated to detect anti-forensics is the maximum false alarm rate such that

$$P_{fa}^{(\xi)} = P\left(\delta_d^{(\hat{\xi})} = H_1^d \cup \delta_c^{(\xi - \hat{\xi})} = H_1^c | \mathbf{V} \text{ is unaltered}\right) \leq \xi \tag{18}$$

4.2 Game model

Game theory [6, 16] is a mathematical tool for analyzing the interactions between rational decision-makers. A thorough review of game theory would be overwhelming here, so we limit our discussion to a two-player zero-sum game [6], which is related to our work.

In a practical scenario of video inter-frame forgery, the forger has to determine his strategy without knowing the strategy of the investigator. In order to simulate a more practical scenario, we relax the assumption in [19] that the forensic investigator (who is denoted as player 1) moves first, then the forger (who is denoted as player 2) responds. Instead, our game model is a simultaneous-move game in which player 1 and player 2 can simultaneously choose their strategies. Furthermore, it is assumed that both player 1 and player 2 have complete information about the game. They know the payoff matrix of the other, and they know their opponent knows the payoff matrix [6]. For a given total false alarm rate P_{fa} , $P_{fa}^d, P_{fa}^c \in [0, P_{fa}]$, player 1 chooses a P_{fa}^d to achieve the maximum P_d (outcome), while player 2 seeks a $k, k \in [0, 1]$, the strength of anti-forensics, to achieve the minimum P_d . Here $k=1$ means that using anti-forensics at full strength and $k=0$ corresponds to the scenario that no anti-forensics is adopted [19]. The objectives of the two players are strictly competitive, therefore the interplay between the forensic investigator and the forger can be modeled as a zero-sum game.

The utility (outcome) of player 1 is denoted as:

$$U_1(P_{fa}^d, k) = P_d(P_{fa}^d, k) \tag{19}$$

On the other hand, for player 2, his utility is denoted as:

$$U_2(P_{fa}^d, k) = -P_d(P_{fa}^d, k) \tag{20}$$

We denote the simultaneous-move, zero-sum game between player 1 and player 2 as the Video Inter-frame Forgery (VIF) game. The VIF game can be summarized as follows: Player 1 and player 2 simultaneously choose their strategies. One player’s gain of utility is exactly balanced by the loss of his opponent’s utility. The strategies and payoff matrix are defined as:

- S_1 The strategy of player 1 is the false alarm rate P_{fa}^d that can be allocated to δ_d , the forensics of video inter-frame forgery.
- S_2 The strategy of player 2 is k , the strength of anti-forensics.
- u The payoff matrix is defined in terms of the total detection rate:

$$U(P_{fa}^d, k) = P_d(P_{fa}^d, k) \tag{21}$$

4.3 Mixed strategy Nash equilibrium

Nash Equilibrium (NE) is a profile of strategies such that each player’s strategy is an optimal response to the other players’ strategies. The game between the forensic investigator and the forger is a finite strategic, zero-sum and simultaneous-move game, which may not have pure strategy NE, therefore we resort to *Mixed Strategy Nash Equilibrium* that well resolves a finite strategy-form game [16]. The mixed strategy of player 1 $\mathbf{P}_{fa}^d = [x_1, x_2, \dots, x_m]$ is a probability distribution over different false alarm rates P_{fa}^d , and the mixed strategy of player 2 $\mathbf{k} = [y_1, y_2, \dots, y_n]$ is a probability distribution over different anti-forensic strength values.

To solve the VIF game, we formulate it as a linear optimization problem [6, 27]. The strategy for player 1 is to find the maximum v which is subject to

$$\begin{aligned} x_i &\geq 0, & i = 1, 2, \dots, m \\ \sum_i x_i &= 1 \\ \sum_i u_{ij}x_i - v &\geq 0, & j = 1, 2, \dots, n \end{aligned} \tag{22}$$

where $u_{ij} = P_d(P_{fa}^d, k_j)$ is the total detection rate when player 1 adopts P_{fa}^d and player 2 adopts k_j . v is the objective function. By solving the optimization problem over $m + 1$ parameters (v, x_1, x_2, \dots, x_m), we can obtain the solution v^* to the VIF game and the strategy \mathbf{P}_{fa}^{d*} for player 1.

The strategy for player 2 can be obtained by solving a dual problem of (22), i.e., to find the minimum v which is subject to

$$\begin{aligned} y_j &\geq 0, & j = 1, 2, \dots, n \\ \sum_j y_j &= 1 \\ \sum_j u_{ij}y_j - v &\leq 0, & i = 1, 2, \dots, m \end{aligned} \tag{23}$$

The optimization can be solved with using the linear programming method [5].

For a given total false alarm rate P_{fa} , the Nash Equilibrium of the **VIF** game can be derived, and the corresponding outcome $U(\mathbf{P}_{fa}^{d*}, \mathbf{k}^*)$, i.e., the total detection rate, is P_d . A ROC curve as a function of P_{fa} can be obtained to show the detection rates under the NE. It is called NE ROC curve in short form [20].

5 Experimental results

We conduct several experiments to evaluate the performances of the improved forensic and the proposed counter anti-forensic techniques. The dataset in our experiments includes 32 QCIF video sequences in YUV-uncompressed format. The complete list of the names of these video sequences is shown in the Appendix. The motion compensated video compression and decompression are simulated in Matlab. Without loss of generality, we use a fixed GOP structure *IBBPBBPBBPBP* with $G=12$ and the standard MPEG DCT coefficient quantization tables in our experiments. We set $QP=8$ for I-frames, $QP=10$ for P-frames and B-frames. All parameters for compression are the same in our experiments. We compress the first 250 frames of the 32 video sequences with the aforementioned parameters, thus creating the singly compressed videos as the unaltered video dataset.

The unaltered videos are regarded as negative samples, and the altered videos are regarded as positive samples. A threshold is chosen to maximize the classification accuracy (Acc):

$$Acc = \frac{TPR + TNR}{2} \quad (24)$$

where TPR denotes the true positive rate and TNR denotes the true negative rate.

5.1 Forensics of video inter-frame forgery

To simulate the process of forgery, we decompress the 32 unaltered videos and delete 1 to $G - 1$ frames from the beginning of each unaltered video, and then recompress the tampered videos with the same GOP. Totally, we get $32 \times 11 = 352$ videos which have undergone frame deletion.

We compare the performances of the frame deletion detection algorithm in [12] and our improved detection algorithm in distinguishing 352 forged videos which have undergone frame deletion from the 32 unaltered videos. The Area Under the ROC Curve (AUC) along with the Acc are used to evaluate the performance of the forensic techniques. In Fig. 4, the ROC curve in blue is for the detection algorithm in [12], yielding $Acc=93.8\%$, and $AUC=96.9\%$. The ROC curve in red is for our improved algorithm in detecting video frame deletion, yielding $Acc=96.9\%$ and $AUC=99.3\%$. We also compare results in Table 1. Our improved algorithm yields better performance in detecting video frame deletion, where an improvement of 3.1% and 2.4% is obtained for Acc and AUC respectively. The improvement is due to our modification to the algorithm in [12], e.g., we take the magnitude of the predicted error caused by frame deletion into consideration. By integrating the magnitude of and the periodicity of the predicted errors, the improved algorithm can better detect the manipulation of video frame deletion.

Furthermore, we test the ability of our improved algorithm on detecting video frame insertion. We decompress the 32 unaltered videos and insert six frames at the beginning of each video, and then recompress these tampered videos. Our improved detection algorithm is also utilized to distinguish the 32 unaltered videos from 32 altered videos that have undergone

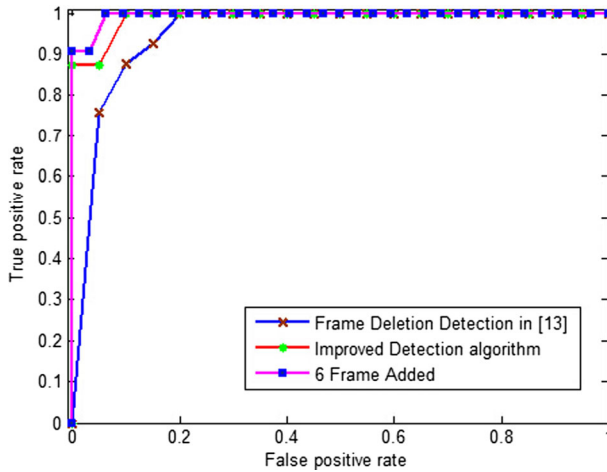


Fig. 4 ROC curves for detecting video frame deletion and video frame insertion

frame insertion. The pink ROC curve in Fig. 4 shows the corresponding performance of our improved algorithm. As frame insertion can be seen as deleting negative number frames, the performance of detecting this type of forgery is similar to that of detecting frame deletion. We have $Acc=96.9\%$ and $AUC=99.5\%$.

5.2 Counter anti-forensics of video frame deletion

To evaluate the performance of the proposed counter anti-forensics of video frame deletion, we use the anti-forensics in [19] to modify the 352 tampered videos that have undergone frame deletion. The ROC curves of video anti-forensics and counter anti-forensics are shown in Fig. 5, where the yellow line indicates the performance by a random classifier. The green ROC curve shows the performance of our improved video frame deletion algorithm when used to detect the anti-forensically modified videos. Compared with the performance of that without being anti-forensically modified, the accuracy decreases to 63.1% and AUC decreases to 64.4%.

Then our proposed counter anti-forensics and the counter anti-forensics in [19] are used to reclassify the anti-forensically modified videos and the unaltered videos. We compare the performances in Table 2. When unaltered videos and anti-forensically modified videos are obtained using exhaustive search in the initial compression, both our method and the method in [19] achieve perfect detection (i.e., $Acc=100\%$, $AUC=100\%$). If exhaustive search is used in motion estimation, motion vectors can reach a global optimum. The difference between an unaltered video’s stored and recalculated prediction errors is very small. By contrast, if a video

Table 1 Detection accuracy and AUC results of the algorithm in [12] and our improved algorithm

Items	Detecting frame deletion [12]	Improved algorithm in frame deletion	Improved algorithm in frame insertion
Acc	93.8 %	96.9 %	96.9 %
AUC	96.9 %	99.3 %	99.5 %

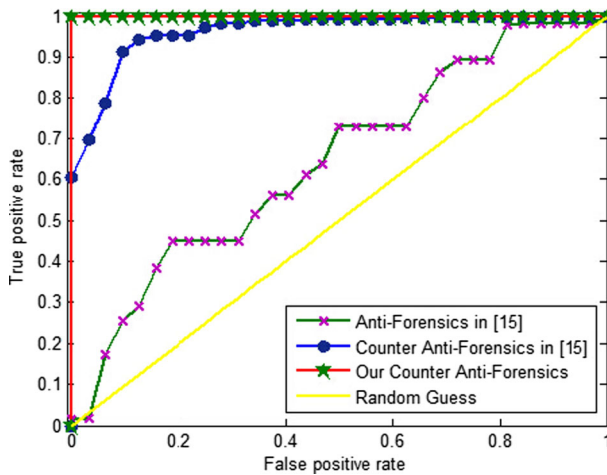


Fig. 5 ROC curves for video anti-forensics and different counter anti-forensics

has been anti-forensically modified, the difference will be relatively large, so it is easy to distinguish unaltered and anti-forensically modified videos.

In practice, if time-efficient motion searching algorithms [17] are adopted, motion vectors may not always reach the global optimum. This will increase the difficulty of distinguishing an unaltered video from anti-forensically a modified video. We employ a popular diamond searching algorithm in motion estimation, instead of exhaustive search, to evaluate the performance of the counter anti-forensics under less favorable conditions. In Fig. 5, the ROC curve in red shows the performance of the proposed method in distinguishing anti-forensically modified videos from unaltered videos. We note that our method can achieve perfect detection when diamond search is used. While we note the performance $Acc=90.1\%$ and $AUC=96.3\%$ for the method in [19], as shown by the blue ROC curve in Fig. 5.

The reason of the performance degradation of the counter anti-forensics in [19] when diamond search is used is explained as follows. As discussed above, the result of motion estimation depends on different searching algorithm. The method in [19] directly analyzes the difference in motion vectors, so its detection rate drops under less favorable condition (e.g., when diamond search is adopted). By contrast, our counter anti-forensics is based on the time-domain statistic. Though different algorithms of motion estimation also introduce variation in the P-frame prediction error sequence, this variation is too little to change the position of the maximum prediction error in each GOP. Therefore, our countering anti-forensics is stable even when diamond search is used. The experimental results support that our counter anti-forensic method is more robust than the method in [19].

Table 2 Accuracy and AUC results of counter anti-forensics in different motion search algorithms

Items	Exhaustive search	With diamond search, method in [19]	With diamond search, proposed method
<i>Acc</i>	100 %	90.1 %	100 %
<i>AUC</i>	100 %	96.3 %	100 %

5.3 Game theoretic evaluation

Now the aforementioned game theoretic model is used to find out the optimal strategies of both the investigator and the forger. The control of the anti-forensic strength is accomplished as follows [19]:

$$\tilde{e}_k(n) = k \times \tilde{e}(n) + (1-k) \times e(n) \quad (25)$$

where $\tilde{e}(n)$ denotes the fingerprint-free target prediction error sequence as mentioned in Section 2. Typically, k is set from 0 to 1 with step 0.1, and as a result the video forger has 11 different anti-forensic strengths. We use these 11 strengths to anti-forensically modify the 352 videos that suffered from frame deletion. The diamond search is adopted for motion estimation in the initial compression.

For the forensic investigator, we consider two sets of forensic and counter anti-forensic methods, which are defined as follows.

- M₁** Our improved frame deletion detection algorithm is adopted for detecting video frame deletion and our proposed counter anti-forensics is adopted for detecting anti-forensics.
- M₂** The frame deletion detection algorithm in [12] is used for detecting video frame deletion and the counter anti-forensics in [19] is used for detecting anti-forensics.

For each set of forensic methods and each anti-forensic strength, the two-phase test is performed and the payoff matrix is generated. Figure 6 shows an example of the payoff matrix under the total false alarm rate constraint $P_{fa}^d=12.5\%$. The x-axis represents the strategy for player 1, i.e., the investigator's chosen false alarm rate P_{fa}^d for detecting video frame deletion. The y-axis represents the strategy for player 2, i.e., the forger's anti-forensic strength. The z-axis represents the total detection rate P_d given both players' strategies. In Fig. 6, the matrix in red is the total detection rate of **M₁** and the matrix in blue is the total detection rate of **M₂**. For all the combinations of P_{fa}^d and k , the red matrix is always above the blue matrix, and for some points, the red matrix is much higher than the blue matrix, which demonstrates that the performance of **M₁** is better than the performance of **M₂** in the two-phase test. Because we

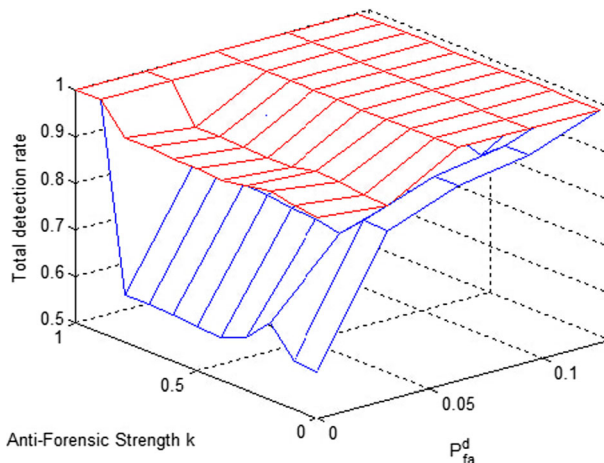


Fig. 6 The detection performances of **M₁** and **M₂** when $P_{fa}^d=12.5\%$

improve the frame deletion detection algorithm and propose a more robust counter anti-forensics, the total detection rate is improved.

Then we show the outcomes and optimal strategies for both players under the **VIF** game. The combination of our improved frame deletion algorithm and proposed counter anti-forensics. When $P_{fa}=12.5\%$, for any strategies adopted by player 2, player 1 can reach 100% detection rate with M_1 under *Mixed Strategy Nash Equilibrium*. The optimal strategy for player 1 is $P_{fa}^{d*}=[1/16, 3/32, 1/8]$ with any probability combination. That is, the **VIF** game has both pure strategy NE and mixed strategy NE. If player 1 adopts M_2 , no pure strategy NE exists in this case. The mixed strategy NE is that player 1 chooses $P_{fa}^{d*}=[1/32, 1/8]$ with the probability combination of [0.663, 0.337] and that player 2 chooses $k^*=[0.2, 0.9, 1.0]$ with the probability combination of [0.620, 0.190, 0.190]. The total detection rate under NE is 87.5%.

We determine the total detection rates under NE and the optimal strategies for both players under a set of total probability of false alarm rate between 0 and 50%. The investigator and the forger can choose their optimal strategies depend on their requirements. For each total false alarm rate, both M_1 and M_2 are adopted as the forensic methods for player 1. The NE ROC curves are shown in Fig. 7, where the x-axis is the total false alarm rate, and the y-axis is the payoff(total detection rate under *Mix Strategy Nash Equilibrium*). The blue NE ROC curve shows the performance when player 1 use M_2 as his forensic methods, yielding $Acc=87.9\%$ and $AUC=95.8\%$. The red NE ROC curve shows the performance when player adopt M_1 , giving $Acc=96.8\%$ and $AUC=99.6\%$.

The optimal strategies for the forger with M_1 at different total false alarm rate are shown in Table 3. Each row in Table 3 is the optimal strategy for the forger under a given total false alarm rate, and each column is probability distribution for a certain anti-forensic strength. For example, when the total false alarm rate is 0.0%, the optimal strategy for the forger is $k^*=0.4$ with 100% probability. Table 3 suggests that medium anti-forensic strength should be optimized for a forger. We just show the strategies for the forger at a total false alarm rate ($\leq 3.1\%$) for the reason that the

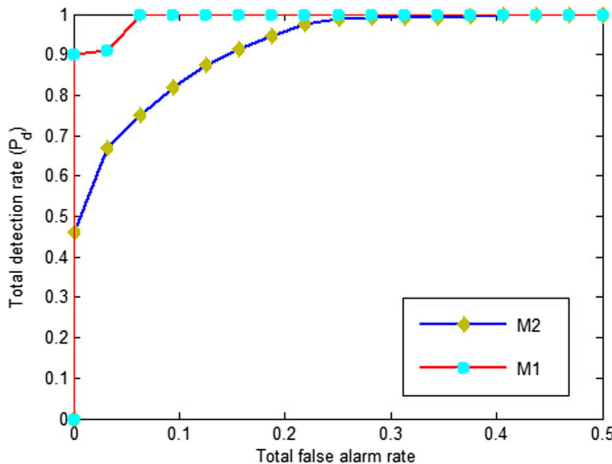


Fig. 7 Nash equilibrium ROC curves when the investigator uses M_1 or M_2 as the forensic method

Table 3 Nash equilibrium strategies k^* obtained for the forger at different total false alarm rates

k	P_{fa}	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	100 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %
3.1 %	0.0 %	20.8 %	0.0 %	0.0 %	53.2 %	26.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %

total detection rate will reach 100 % when the false alarm rate is larger than 6.3 %. The optimal strategies for the investigator with M_1 and the total detection rate under NE at different total false alarm rate are shown in Table 4. Each row in Table 4 is the optimal strategy for the investigator and total detection rate under a given total false alarm rate, and each column is the probability distribution for a certain false alarm rate which is allocated in detecting video inter-frame forgery. For example, when the total false alarm rate is 9.4 %, the optimal strategy for the investigator is $P_{fa}^{d*} = [6.3\%, 9.4\%]$ with a probability combination of $[0.5, 0.5]$, and the total detection rate is 100 %. With the increase of the total false alarm rate, the investigator should allot a larger false alarm rate for the first phase detector.

Our improved detector and the proposed counter anti-forensic methods not only outperform the existing methods in detecting frame deletion and anti-forensics, but also perform better in the VIF game. In the VIF game, the forger can vary the anti-forensic strength, which increases the detection difficulty. The total detection rate with the existing forensic methods (M_2) drops in this case. In contrast, our methods (M_1) can yield a high detection rate, where the total detection rate under NE reaches 100 % at a total false alarm rate 6.3 %. The superiority is attributed to the following reasons. Firstly, we take the magnitude of the prediction error caused by frame deletion into consideration, which improves the performance of the frame deletion detection algorithm in [12]. Secondly, our proposed counter anti-forensics is based on the analysis of the variation of the P-frame prediction error sequence and is more robust than the counter anti-forensics in [19]. Thirdly, the combination of our video frame deletion forensics and counter anti-forensics can effectively capture the fingerprints left by frame deletion or anti-forensics. The effectiveness of frame deletion detection algorithm degrades when strong anti-forensics is adopted, as indicated by the decrease of I'_t . However, strong anti-forensics will introduce obvious changes in I''_t and I'_t , which can be detected by our counter anti-forensics. Therefore our forensics and counter anti-forensics of video frame deletion yield a desired complementary effect.

Table 4 Nash equilibrium strategies P_{fa}^{d*} obtained for the investigator and total detection rate at different total false alarm rates

P_{fa}^d	P_{fa}	0.0 %	3.1 %	6.3 %	9.4 %	Total detection rate
0.0 %		100 %	–	–	–	90.0 %
3.1 %		0.0 %	100 %	–	–	90.1 %
6.3 %		0.0 %	0.0 %	100 %	–	100 %
9.4 %		0.0 %	0.0 %	50.0 %	50.0 %	100 %
...	

6 Conclusions

In this paper, we focus on video inter-frame forgery. Firstly, the frame deletion detection algorithm in [12] is improved. We analyze the shortcoming of the algorithm [12] and combine the magnitude together with the periodicity of the predicted error resulted from video frame deletion to improve the algorithm. Secondly, we propose a counter anti-forensic method to defeat a typical anti-forensics. By analyzing the anti-forensics in [19], we demonstrate that the periodic characteristics introduced by frame deletion still remain in the anti-forensically modified videos. By estimating the true prediction error and comparing it with the prediction error stored in the video, we can detect the anti-forensics. Thirdly, we define a **VIF** (Video Inter-frame Forgery) game to analyze the interplay between the forensic investigator and the forger. Compared with the game in [19], we do not assume that the investigator moves first to reflect the practical scenarios. The **VIF** game is a zero-sum, simultaneous-move game, and the *Mixed Strategy Nash Equilibrium* is adopted to solve this game.

Video experiments are implemented to evaluate the performances of our improved detection algorithm and the proposed counter anti-forensics. Additionally, we also show that this improved detection algorithm is also useful for detecting video frame insertion. We test the performance of the proposed counter anti-forensics under different motion search algorithms. Experimental results demonstrate that our counter anti-forensics can successfully detect the typical anti-forensics and is more robust to different motion search algorithms.

In the **VIF** game, for the investigator, our improved frame deletion algorithm and the proposed counter anti-forensics are used as forensic methods (\mathbf{M}_1). The existing frame deletion algorithm [12] and the counter anti-forensics [19] are set as the compared set (\mathbf{M}_2). We analyze the optimal strategies for both the investigator and the forger under the **VIF** game. For the forger, he/she should adopt a medium anti-forensic strength. While for the investigator, he/she should allot a larger false alarm rate for detecting video frame deletion as the total false alarm rate increases. Our methods not only outperform the existing methods in detecting frame deletion and anti-forensics, but also perform better in the **VIF** game. Since the combination of our deletion algorithm and the proposed counter anti-forensics operates effectively, in our experiments, the total detection rate can reach 100 % at the 6.3 % total false alarm rate regardless of the strategies adopted by the forger.

Acknowledgments This work was supported by the NSFC (Grant nos. 61379155, U1405254 and 61232016), the 973 Program (Grant no. 2011CB302204), the Research Fund for the Doctoral Program of Higher Education of China (Grant no. 20110171110042) and the NSF of Guangdong province (Grant no. S2013020012788).

Appendix

The complete list of the video sequences investigated in our experiments is listed here: *Akiyo, Bowling, Bridge-Close, Bridge-Far, Carphone, Claire, Coastguard, Contianer, Deadline, Football, Foreman, Galleon, Grandma, Hall, Highway* (The longest sequence is divided into six portions), *Husky, Mobile, Mother-Daughter, News, Pamphlet, Paris, Salesman, Sign-Irene, Silent, Stefan, Table, Tmpete*.

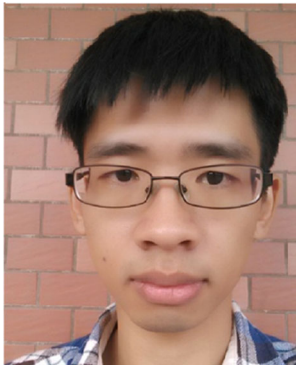
These video sequences can be downloaded from [<http://trace.eas.asu.edu/yuv/>, <http://media.xiph.org/video/derf/>].

References

1. Barni M (2012) A Game theoretic approach to source identification with known statistics. Proc. of ICASSP 1745–1748
2. Bestagini P, et al (2012) Video codec identification. Proc. of ICASSP 2257–2260
3. Chao J, Jiang XH, Sun TF (2012) A novel video inter-frame model deletion scheme based on optical flow consistency. Proc. of IWDW 267–281
4. Gironi A, Fontani M, Bianchi T, Piva A, Barni M (2014) A video forensic technique for detecting frame deletion and insertion. Proc. of ICASSP 6226–6230
5. Grant M, Boyd S (2008) Graph implementations for non-smooth convex programs. recent Advances in learning and control, lecture notes in control and information sciences, Springer 95–110
6. Hespanha J (2011) An introductory course in non-cooperative game theory. Published online, available at <http://www.ece.ucsb.edu/~hespanha/>
7. ISO (2008) Information technology - generic coding of moving pictures and associated audio information - part 2: Video. International Organization for Standardization. ISO/IEC IS 13818–2
8. ISO (2009) Information technology - coding of audio-visual objects-part 2: Visual. International Organization for Standardization, ISO/IEC IS 14496–2. Geneva
9. ISO (2010) Information technology - coding of audio-visual objects-part 10: Advanced video coding (avc). International Organization for Standardization, ISO/IEC IS 14496–10
10. Jiang X, Wang W, Sun T, Shi YQ, Wang S (2013) Detection of double compression in MPEG-4 videos based on Markov statistics. IEEE Signal Process Lett 20(5):447–450
11. Liu L, Cohen R, Sun H, Vetro A, Zhuang S (2010) New techniques for next generation video coding. Proc. of BMSB: p 1–6
12. Liu H, Li S, Bian S (2013) Detecting frame deletion in H.264 video. Proc. of ISPEC 262–270
13. Luo W, Wu M, Huang J (2008) MPEG recompression detection based on block artifacts. Proc. of SPIE 68190X 1–12
14. Milani S, Bestagini P, Tagliasacchi M, Tubaro S (2012) Mul-tiple compression detection for video sequences. Proc. of MMSP 112–117
15. Milani S et al (2012) An overview on video forensics. In APSIPA trans. Signal Inf Process 1:1–18
16. Osborne MJ, Rubinstein A (1994) A course in game theory. MIT Press
17. Pan Z, Zhang Y, Kwong S (2015) Efficient motion and disparity estimation optimization for low complexity multiview video coding. IEEE Trans Broad., 61(2):166–176.
18. Rocha A, Scheirer W, Boulton T et al (2011) Vision of the unseen: current trends and challenges in digital image and video forensics. ACM Comput Surv 43(5):1–42
19. Stamm MC, Lin WS, Liu KJR (2012) Temporal forensics and anti-forensics for motion compensated video. IEEE Trans Inf Forensics Sec 7(4):1315–1329
20. Stamm MC, Lin WS, Liu KJR (2012) Forensics vs. anti-forensics: a decision and game theoretic framework. Proc. of ICASSP 1749–1752
21. Stamm MC, Liu KJR (2011) Anti-forensics for frame deletion/addition in MPEG video. Proc. of ICASSP 1876–1879
22. Vazquez-Padin D, Fontani M, Bianchi T, Comesana P, Piva A, Barni M (2012) Detection of video double encoding with GOP size estimation. in Proc. of WIFS 151–156
23. Wang W, Farid H (2006) Exposing digital forgeries in video by detecting double MPEG compression. Proc. of ACM Multimedia Secur Workshop 37–47
24. Wu Y, Jiang X, Sun T, Wang W (2014) Exposing video inter-frame forgery based on velocity field consistency. Proc. of ICASSP 2674–2678
25. Xu J, Su Y, Liu Q (2013) Detection of double MPEG-2 compression based on distributions of DCT coefficients. Int J Pattern Recognit Artif Intell 27(1):1354001
26. Zeng H, Kang X (2013) Camera source identification game with incomplete information. in Proc. of international workshop of digital-dorensics and watermarking. Aucland, New zealand, 2013
27. Zeng H, Kang X, Huang J (2013) Mixed-strategy Nash equilibrium in the camera source identification game. Proc. of IEEE Int. Conf. Image Process 4472–4476



Xiangui Kang Received the B.S. degree from Peking University, Beijing, China, in 1990, the M.S. degree from Nanjing University, Nanjing, China, in 1993, and the Ph.D. degree from Sun Yat-Sen University, Guangzhou, China, in 2004. He was a visiting Professor with College of Computer and Software, Nanjing University of Information Science & Technology, and is currently a professor with the School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China. His research interests include information forensics, watermarking, and multimedia communications and security. Dr. Kang is a member of the IEEE ComSoc's Multimedia Communications Technical Committee, and a member of IMV Technical Committee of Asian-Pacific Signal and Information Processing Association. He has published more than 50 research papers in major international academic journals and peer-reviewed conference proceedings. He was a visiting scholar with University of Maryland-College Park during 2011–2012, and with New Jersey Institute of Technology during 2004–2005.



Jingxian Liu Received the B.S. degree from Sun Yat-Sen University, Guangzhou, China, in 2013. He is currently a postgraduate student in School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China. His research interests are information security and forensics, multimedia signal processing.



Hongmei Liu received the B.S. degree and M.S. degree in computer science from Tsinghua University, Beijing, China, in 1992 and 1996, respectively, and the Ph.D. degree in radio physics from Sun Yat-sen University in 2001. Since fall 1996, she has been on the faculty of the Electronics and communication Engineering Department at Sun Yat-sen University where she is now an Associate Professor. Dr. Liu's research interests include multimedia security and multimedia signal processing and communications. She holds several China patents on media security, and has a few more pending.



Z. Jane Wang received the B.Sc. degree from Tsinghua University, China, in 1996, and the M.Sc. and Ph.D. degrees from the University of Connecticut in 2000 and 2002, respectively, all in electrical engineering. She has been Research Associate of Electrical & Computer Engineering Department at the University of Maryland, College Park. Since Aug. 1, 2004, she has been with the Department Electrical and Computer Engineering at the University of British Columbia, Canada, and is currently a Professor. Her research interests are in the broad areas of statistical signal processing theory and applications. She has published over 80 journal papers and about 90 conference papers. She served as Associate Editor for several IEEE journals, including IEEE Trans. on Signal Processing, IEEE Trans. on Information Forensics & Security, IEEE Trans. on Biomedical Engineering, IEEE Signal Processing Letters and IEEE Trans. on Multimedia.