Detecting Video Forgeries Based on Noise Characteristics

Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato

Institute of Industrial Science, The University of Tokyo
{michi,takahiro,ysato}@iis.u-tokyo.ac.jp

Abstract. The recent development of video editing techniques enables us to create realistic synthesized videos. Therefore using video data as evidence in places such as a court of law requires a method to detect forged videos. In this paper we propose an approach to detect suspicious regions in video recorded from a static scene by using noise characteristics. The image signal contains irradiance-dependent noise where the relation between irradiance and noise depends on some parameters; they include inherent parameters of a camera such as quantum efficiency and a response function, and recording parameters such as exposure and electric gain. Forged regions from another video camera taken under different conditions can be differentiated when the noise characteristics of the regions are inconsistent with the rest of the video.

1 Introduction

In the last decade digital cameras have become so popular that enormous numbers of photographs and videos are taken by amateur photographers. On the other hand, the recent development of digital editing techniques can be used to synthesize realistic images and videos that could also be used in courts of law. Unfortunately, photographs taken by amateur photographers are not protected from tampering. So if these photographs are used as testimony in courts of law, how is it possible to distinguish true evidence from false one?

In the early days of the Internet, *digital watermarking* was the main countermeasure against illegal use of digital contents [6]. However, most images and videos do not have an embedded digital watermark. Once images or videos without watermarks are uploaded to the Internet, digital watermarks are ineffective even if they are embedded afterwards because the contents may have already been tampered with by someone. Therefore digital watermarking is found to be limited in its ability to assure authenticity.

Recently a number of forgery detecting techniques for images without watermarking have been studied [14]. These techniques exploit inconsistencies or unnaturally high coherence observed in an image. Jonson and Farid used inconsistencies in lighting [4] and chromatic aberration [5]. Lin et al. estimated camera response function and verified its uniformity across an image [7]. Lukáš et al. extracted fixed pattern noise from an image and compared it with a reference pattern [10]. Fridrich et al. computed correlation between segments in an image

T. Wada, F. Huang, and S. Lin (Eds.): PSIVT 2009, LNCS 5414, pp. 306–317, 2009.

and detected cloned regions [2]. Ye et al. used an estimated JPEG quantization table and evaluated its consistency [17]. The different digital image forensic methods mentioned above help us to aggressively estimate the authenticity of digital images. In contrast, research for digital video forensics is just getting started, and the development of forgery detecting techniques for video is in high demand.

One of the most frequent digital evidence declared invalid in a court of law is a video recorded by a fixed surveillance camera. Tampering methods for a scene that contains a static background can be classified into two approaches. One is replacing regions or frames with duplicates from the same video sequence: forgers can hide unfavorable objects in a scene by overwriting these with the background. The other is clipping objects from other images or video segments and superimposing them on the desired regions in the video. This type of forgery aims to show objects that are advantageous for false evidence.

The method for detecting replacement or duplication has been studied by Wang and Farid [16]. Duplication yields high correlation between original frames or regions and cloned ones. Detecting unnaturally high coherence is useful for discovering copy-paste tampering. It has been demonstrated in the research that we can find substitutions from another frame in the same video sequence. However, their proposed method has a serious limitation in that it can only detect copy-paste tampering from the same video sequence. It cannot be used to detect superimposition, i.e., inserting objects from other video segments. In contrast, our aim is to propose a method that can detect superimposition.

The basic idea of our proposed method is to use noise inconsistencies between the original video and superimposed segments to detect forgeries. We exploit the *photon shot noise* in a digital camera as a clue to tampering. Photon shot noise results from the quantum nature of photons and follows a Poisson distribution, where the variance of the number of photons equals the mean. This dependency on the irradiance of photon shot noise gives us a clue to inconsistencies in the video. A CCD camera converts photons into electrons and finally into bits; therefore, the relation between the variance and the mean of the number of photons is converted into that between the variance and the mean of the observed value. This relation is formulated as the *noise level function* (NLF) by Liu et al [8]. The NLF depends on such parameters as inherent parameters of the camera and recording parameters. Consequently, by comparing the relation of the variance and the mean in a video clip, we can detect forged regions clipped from another video.

Specifically, given input video, we first analyze the noise characteristics at each pixel. Fig.1 shows a diagram of the noise characteristics. The solid line is the NLF of this distribution. Points in the figure represent the noise characteristic computed from each pixel. Once we obtain the per-pixel noise characteristics, NLF is fitted to the points using the least squares method. In this paper, we assume a linear *camera response function* (CRF). Since it is known that the linear CRF yields a linear NLF [13], the problem of estimating the NLF of the original video results in the problem of fitting a linear function to the data. We adopt

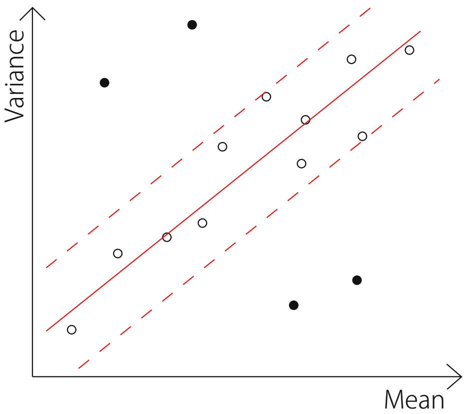

Fig. 1. Diagram of noise characteristics. Solid line is the estimated noise level function. Points inside the dashed lines (open circles) are regarded to be authentic. Closed circles are regarded to be from forged pixels.

the simplest metrics for the forgery measure, i.e., a point whose distance from the estimated function is greater than a threshold is from a forged pixel. The dashed lines in Fig.1 are the thresholds that separate the noise characteristic points into authentic (open circle) pixels and forged (closed circle) pixels. By evaluated every pixel in this way, we can detect per-pixel forgery in the given video.

We recorded some real videos for experiments and demonstrated that different recording parameters resulted in different noise characteristics. Then we applied the proposed method to the tampered video, we found that our method could properly detect the forged region.

2 Related Work

2.1 Forgery Detection Methods for Images and Video

The area of digital image forensics has progressed so markedly in the last few years that several approaches have been developed to detect forgeries in a digital image. Image tampering methods can be classified into two approaches. One is replacing regions with others in the same image and the other is superimposing regions clipped from other images.

The first attempt of forgery detection was proposed by Fridrich et al [2]. This method targets the copy-move method of attack, which yields unnaturally high correlation between duplicated regions. The researchers introduced a detection method based on robust block matching, which was carried out by using Discrete Cosine Transform (DCT) coefficients in order to deal with lossy JPEG compression.

Subsequent approaches target the superimposition-based forgeries, which verify the uniformity of characteristics in an image; therefore objects clipped from other images could be detected. Jonson and Farid proposed methods based on optical clues. They estimated the light source directions from some contours in an image and checked the consistency of estimated light source directions [4]. This technique showed so accurate estimation of light source directions for outdoor scenes that it could differentiate tampered objects in the image. Jonson and Farid also developed a method for detecting forgeries based on lateral chromatic aberration [5]: a spatial shift of light passing through the optical system due to the difference of refraction between wavelengths. Global model parameters that determine the displacement vector at each pixel in an image were estimated, and the degree of tampering was evaluated by calculating the average angular error between the displacement vector determined by global parameters and the actual local vector.

Lin et al. checked for the consistency of the camera response function estimated by analyzing the edges [7]. The irradiance on an edge should be a linear combination of those from objects at both sides of the edge, but a nonlinear camera response skews the linearity of signal processing. This approach estimates the nonlinear inverse response functions that convert a nonlinear relation of observed pixel values on the edge into a linear relation. If the function estimated from an edge does not conform to the rest of the image, the edge is marked as a sign of tampering.

JPEG is a compression technique for images; different manufacturers design different quantization tables used in a compression process. Ye et al. proposed a method to detect inconsistencies in an image based on the blocking artifact measure [17]. If blocks compressed with different quantization tables are combined in an image, the blocking artifact measure of forged blocks is much larger than that of an authentic block. They estimated the quantization table from the histogram of DCT coefficients and evaluated the blocking artifact measure of each block.

Compared to the image forensic techniques mentioned above, only a few techniques have been developed for video. Wang and Farid proposed forgery detecting methods based on video duplication and a deinterlacing algorithm [15,16]. The first approach that detect duplication is similar to the correlation-based detection proposed by Fridrich et al., extended so that it could detect duplicated regions across frames. They combined spatial and temporal correlation for detecting duplicated frames as well. On the other hand, the deinterlacing algorithm is a technique of converting interlaced video into a non-interlaced form. Due to the half resolution of interlaced video, the deinterlacing algorithm makes full use of insertion, duplication, and interpolation of frames to create full-resolution video. Parameters in the interpolation and the posterior probability of forgery are estimated by using the Expectation Maximization (EM) algorithm. Wang and Farid referred to forgery detection for interlaced videos in the same paper. They suggested that the motion between fields of a frame is closely related to that across fields in interlaced videos. Evaluating the interference to this relation by tampering, they detect the forgeries in the given interlaced video.

The methods proposed by Wang and Farid are interesting attempts for digital video forensics. It should be pointed out, however, that these methods have limitations for forgery detection. The first forensic technique based on correlation assumes that forged regions are duplicated from the same video sequence. As a result, this method has the same limitation for forgery detection as the method proposed by Fridrich et al., that it cannot detect superimposed regions from other videos. The second method targeting deinterlaced and interlaced videos can detect superimposing from other video sequences, but it limits the form of the video to deinterlaced or interlaced form.

Our proposed method is based on the inconsistencies of the noise characteristics in the given video. Forged regions brought from other video clips can be effectively detected by our method. In addition, our method exploits the characteristic of camera noise. Noise is a stable clue for forensics because it is an inevitable phenomenon in signal processing. Therefore our method is applicable to a wide range of videos.

2.2 Effective Use of Noise in Digital Data

Since the early period of digital camera, various reports have been given on the study of noise in signal processing. The main purpose of this field of research is to remove noise in images. Many denoising techniques have been developed and systematically classified [12].

On the other hand, some researchers have recently introduced interesting attempts to make effective use of noise, rather than trying to remove it from images and videos. Matsushita and Lin exploited the distribution of noise intensity for each scene irradiance to estimate the *camera response functions* (CRFs) [11]. Noise distribution is by nature shown to be symmetric, but it is skewed by nonlinear CRFs. Conversely, the inverse CRF can be estimated by evaluating the degree of symmetry of back-projected irradiance distribution. Using the noise in an image, the detection ability of the method is not degraded by noise and thus the method can be used under conditions of high-level noise.

Liu et al. estimated the *noise level function* (NLF) from a single image, which relates the noise intensity with the image intensity [8]. The spatial variance in an image contains the variance resulted in object's texture as well as the intensity of the noise. Obtaining the component of the real noise from NLF, we can disassociate the component of texture from the variance of the observation. They utilized the function not only for denoising but also for adaptive bilateral filtering and edge detection.

Noise information is available for camera identification and forgery detection as well. Due to the sensor imperfections developed in a manufacturing process, the CCD camera contains pixels with different sensitivity to light. This spatial variation of sensitivity is temporally fixed and known as *fixed pattern noise*. Since this non-uniformity is inherent in a camera, we can exploit it as a fingerprint. Lukáš et al. determined the reference noise pattern of a camera by averaging the noise extracted from several images [9]. They extracted fixed pattern noise from a given image using a smoothing filter and identified the camera that took the image. The authors also proposed a method for detecting forgeries in an image using the same approach [10].

This paper introduces a video forensic method by checking for inconsistency of the noise characteristics, which has never been proposed among the forensic methods for videos. Since the proposed method aggressively exploits noise, it is effective also for a video contaminated by significant noise. Other approaches are not able to handle high levels of noise.

3 Proposal Method

In this section, we propose a forgery detecting method using a noise characteristics model. In this paper, we will consider the inconsistencies of the characteristics of the noise mixed in the signal to be a clue to tampering. We first introduce a noise characteristic model in Section 3.1. As stated before, we focus in particular on *photon shot noise* for detecting forgeries in the given video. This is because the variance of observed intensity caused by photon shot noise is closely related to its mean. The relationship between the variance and mean of observed intensity is formulated as the *noise level function* (NLF), which is the clue to tampering. In Section 3.2, we propose a method to estimate NLF and detect forgeries by using the estimated NLF.

3.1 Noise Level Function of Video

A CCD digital camera converts photons into electrons and finally into bits. This signal processing has been studied for a long time [3,13]. In the signal process of a digital camera, several noise sources corrupt the signal such as *photon shot noise*, *dark current noise*, *thermal noise*, *read-out noise* and *quantization noise*. We focus on photon shot noise among these noise sources because of the following two reasons: (1) photon shot noise is dominant noise in a scene except in an extremely dark environment, and (2) the relation between the brightness and the noise intensity is useful for forgery detection.

The number of photons that enters a CCD element has temporal fluctuation and thus this variation behaves as noise. Since this fluctuation follows a Poisson distribution, the noise intensity depends on its mean – the noiseless irradiance. Unfortunately, we cannot measure the distribution of photons directly because photons are converted into electrons, electric voltage, and finally bit chains. However, we can instead compute the relation between the mean and the variance of the observed pixel value. We consider their relation as a measure of tampering.

Let $\hat{O}$ be the noiseless observed intensity. Due to the effect of noise, the real observation has fluctuation and thus we obtain a random variable of observation O. Let $\mu_{\hat{O}}$ and $\sigma^2_{\hat{O}}$ be the mean and the variance of the observed pixel intensity O, respectively, when the noiseless observation is $\hat{O}$. Following the formulation described in [8], we introduce NLF $\tau(\mu_{\hat{O}})$ as

$$\tau(\mu_{\hat{O}}) = \mathrm{E}[(O - \mu_{\hat{O}})^2]. \qquad (1)$$

Unlike the equation in [8], we do NOT calculate the square root of Mean Square Error. This function represents how the variance changes with respect to the mean of the observed pixel value. When we obtain the mean observation $\mu_{\hat{O}}$, the variance is described by a function with respect to the mean as

$$\sigma^2_{\hat{O}} = \tau(\mu_{\hat{O}}). \tag{2}$$

NLF depends on such parameters as inherent parameters of the camera and recording circumstance; they include inherent parameters of a camera such as quantum efficiency and the response function, and recording parameters such as exposure and electric gain.

For the sake of simplicity, we make two assumptions regarding the input video. The first assumption is that the distribution of the noise is zero-mean, and therefore we can obtain noiseless observed intensity of each pixel by averaging. Since this assumption suggests that the mean of observed intensity equals the noiseless intensity, we rewrite $\mu_{\hat{O}}$ as simply μ. Second, we assume a linear camera response function (CRF). Former research on noise in a CCD camera [13] implies that a linear CRF yields a linear NLF. Therefore we simply apply linear least squares method to the calculated points.

3.2 Detection of Forged Pixels

Based on the theoretical background described in the previous section, we analyze the noise characteristics and detect forgeries of the given video by the following process. First, the mean and the variance of the pixel value are calculated at each pixel. Next, the NLF is estimated by fitting a function to the noise characteristic points. Finally, each pixel is evaluated based on its distance from the estimated NLF. We describe each step in detail in the following.

Calculation of noise characteristics. If we have an image or a single frame of video sequence, NLF can be obtained by calculating spatial mean and variance. This approach, however, requires an assumption of the local uniformity of the object's reflectance and shading. If there is a textured object in a scene, we cannot obtain the noise component independently from the total variance because the spatial variation is mixed in the signal. The proposed method proves its merits in this case. As mentioned in the introduction, we deal with a static scene where the camera and the objects are fixed during recording. Therefore a conclusion is drawn that the temporal variation of each pixel value results entirely from noise. Operating statistical analysis along a time-line to the given video, we obtain the relation between μ and $\sigma^2_{\hat{O}}$ at each pixel.

NLF estimation. Analyzing observed intensity along a time-line, we obtain a dense set of points, as many as the resolution of the video. Then we fit a linear NLF $\tau(\mu)$ to the points using linear least squares method as

$$\tau(\mu) = \alpha\mu + \beta, \tag{3}$$

where α and β are the estimated parameters. In order to eliminate the effect of the scale factor between the mean and the variance, they are normalized before estimation.

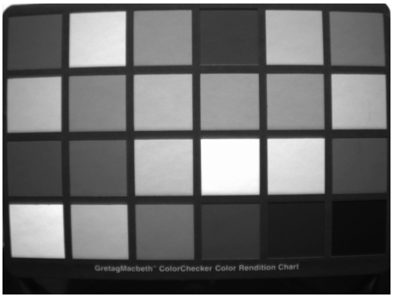

Fig. 2. Example of the recorded video

Table 1. Recording parameters

No.	Shutter time[ms]	Gain[dB]
(a)	19.79	0.00
(b)	11.22	4.99
(c)	6.60	9.90
(d)	3.85	15.08
(e)	2.29	20.04
(f)	1.25	24.96

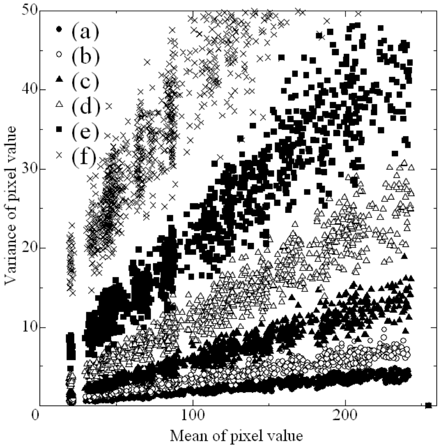

Fig. 3. Noise characteristics with different gain. Data points are thinned out for display. Shutter times and gain of data sets are shown in Table 1.

Because the noise intensity of the video created from an authentic process is uniquely determined by the estimated NLF, every pixel value converted from the same irradiance should yield the same noise intensity. Consequently, inconsistencies of the relation between the mean and the variance can be a clue to the forgery. Therefore we can claim pixels whose noise characteristic is far from NLF to be from a tampering process.

In this paper we use RANSAC [1] so that the NLF is estimated robust to the outliers calculated from the forged regions. The closed circles in Fig.1 are the outliers. Although we need to set a threshold manually, RANSAC is relatively robust to outliers, considering its ease of implementation.

Evaluation of pixels. Once we obtain the NLF $\tau(\mu)$, the authenticity of each pixel in the video is evaluated based on the distance from the estimated NLF according to (2). The evaluation of the pixel N located at the position $\boldsymbol{r}$ is determined as follows.

$$N(\boldsymbol{r}) = \begin{cases} \text{forged} & \text{if } \left|\sigma_O^2(\boldsymbol{r}) - \tau(\mu(\boldsymbol{r}))\right| > \varepsilon \\ \text{authentic} & \text{otherwise,} \end{cases} \tag{4}$$

where ε is the constant threshold.

Note that near the maximum pixel value (Here we consider 8-bit depth, hence the maximum is 255), the observed values are saturated and their apparent variances are smaller than real ones, which causes degradation of the detection quality. Therefore we set an upper limit T for the mean value to omit evaluation of the pixels with the mean larger than T.

4 Experimental Results

All the experiments were done on video recorded on a PointGrey Flea digital camera. 128 grayscale frames are recorded at 30 fps for the 640 × 480-resolution compressed by Huffyuv, lossless compression Codec. We chose a Macbeth Color Checker Board under sunlight as the object. Fig. 2 shows an example of the recorded video.

4.1 Noise Characteristics with Various Parameters

We first showed how the noise characteristics change based on the recording parameters. Fig.3 shows the comparison of the noise characteristics with various electric gain. The shutter times and the gain of the data sets are shown in Table 1. Note that the horizontal and vertical axes indicate absolute, not normalized, values. The data points of each set distribute on a line that rises steeply corresponding to the gain. In the range of upper limit, the variances fall rapidly to zero, which results from the saturation in the quantization process.

4.2 Forgery Detection Using Noise Characteristics

We conducted another experiment of forgery detection. We created forged video clips as follows from 6 video sources analyzed above. At first a pair of videos taken under different parameters was chosen from the sources: they are a pair of the original and the replaced video clips. A forged region of 100×100-dimension was randomly located, and the position was kept as the ground truth. The pixel values in the located region over all frames in the original video were overwritten by those in the replaced video. An example of a frame in the forged video is shown in Fig.5 (Left). The white box in the image indicates the forged region.

The noise characteristics of the forged video were calculated as described in the previous section. Fig.4(A) shows the noise characteristics of the forged video created by replacing a part of the video of parameter (a) with that of parameter (c) in Table 1. Note that the means and the variances are normalized in this figure. Using RANSAC, we fitted a linear NLF to the calculated points. The threshold parameter of RANSAC was empirically set to 0.1 in the normalized noise characteristics space. There are two clusters: a dense cluster projected from the region of parameter (a) and a sparse cluster from the region of parameter (c). The solid line in the figure is the estimated NLF. Due to RANSAC, the linear NLF is properly estimated robust to the outliers.

Next, we assessed the pixels based on (4) and the estimated NLF. The boundary of forgery ε is set to 0.1, which is equal to the threshold of inliers on RANSAC. The upper limit of the mean value for evaluation T is empirically set to 0.9.

Fig.5 (Right) shows the detection result for the test data shown in Fig.5 (Left). The highlighted pixels in the figure represent the pixels determined to be forged. The proposed method detects most of the forged pixels in the color patches, while some pixels in the border are accepted. This is because the noise characteristic in the dark border is not sufficiently distinctive from that of the pixels in the authentic region to differentiate between them.

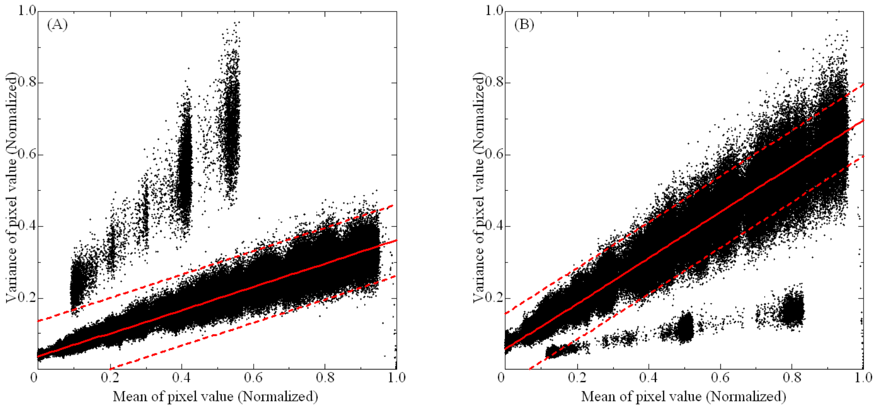

Fig. 4. Noise characteristics of a mixture video containing parameter (a) for the original and (c) for the replaced region (A) and vice versa (B). The solid line is the estimated NLF by using RANSAC and the dashed lines are the boundaries of forgery.

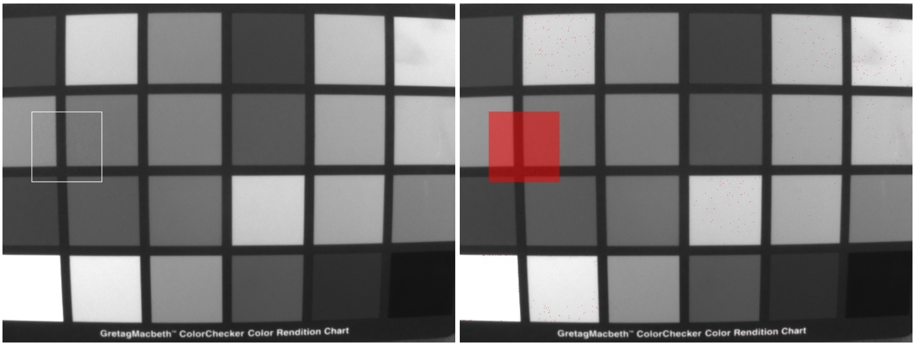
GretagMacbeth™ ColorChecker Color Rendition Chart
GretagMacbeth™ ColorChecker Color Rendition Chart

Fig. 5. Left: Example of the forged video. White box indicates the forged region. Right: Detection result for the video shown in the left figure. Highlighted pixels are determined to be forged.

To evaluate our method, we calculated the recall and the precision rates for every combination of the video clips. For one set of the recording parameters, we averaged over 30 random trials. The parameters in the fitting and the detection process were constant over this evaluation. The experimental result is shown in Table 2. We found that the proposed method can differentiate the forged pixels when the noise characteristics in the forged region are sufficiently isolated from the rest of the video.

However, the proposed method does not evaluate the authenticity of the pixels brighter than the upper limit T, which may cause degradation of detection. Even in the case that the noise characteristics are well separated, recall becomes worse if the forged region is located on a bright color patch. In addition, we should take notice of the low precision rate in the lower triangular portion of the table. The

Table 2. Evaluation result (Top: Recall [%], Bottom: Precision [%])

Original Video	Replaced Video					
	(a)	(b)	(c)	(d)	(e)	(f)
(a)	-	80.6	95.1	95.1	95.3	96.2
(b)	52.8	-	82.2	95.1	95.3	96.2
(c)	95.8	74.3	-	88.6	95.3	96.2
(d)	95.8	96.1	85.8	-	90.1	96.2
(e)	95.8	96.1	95.3	88.9	-	94.9
(f)	95.8	96.4	95.3	95.1	94.8	-

Original Video	Replaced Video					
	(a)	(b)	(c)	(d)	(e)	(f)
(a)	-	71.4	94.5	99.7	99.9	100.0
(b)	61.0	-	76.2	91.9	98.3	99.7
(c)	70.7	64.9	-	81.6	96.7	99.8
(d)	72.5	72.6	70.1	-	82.6	97.8
(e)	69.9	70.0	69.7	68.2	-	84.3
(f)	66.6	66.7	66.4	66.3	66.3	-

characteristic points of the original video in these conditions spread broad in spite of the constant boundary of forgery (See Fig.4(B) for an example). That is why there occurred many false-positives and the quality of the detection is degraded.

It should be noted that the threshold for outliers in RANSAC is empirically adjusted and constant with the gain. Nevertheless, the proposed method achieves robust fitting for all combinations of the recording parameters because of the benefit of robust fitting. It is interesting that the parameters can be fixed because we can easily detect forgeries properly without a probabilistic model or adaptive learning.

5 Conclusions and Future Work

In this paper we introduce a noise level function of a video clip and propose a digital video forensic technique based on the noise characteristics. The proposed method calculates the noise characteristic of each pixel by using temporal averaging, and achieves per-pixel evaluation of the authenticity with a high degree of accuracy by using a fitting method robust to outliers.

The following considerations will provide work for the future. First, in this paper we deal only with the videos recorded from a static scene, but in the future we will definitely have to consider working with persons and moving objects. In addition, the spatial relation of pixels is not used in this paper, but it will be useful for locating objects to integrate information of neighboring pixels. Also, combined with image segmentation techniques, it is expected that the method will reveal suspicious regions in the given video. Second, nonlinear CRFs are not considered in this report. In order to apply our method to a variety of cameras, we should expand it to generalized NLFs.

References

1. Fischler, M.A., Bolles, R.C.: Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography 24(6), 381–395 (1981)
2. Fridrich, J., Soukal, D., Lukáš, J.: Detection of copy-move forgery in digital images. In: Proc. of Digital Forensic Research Workshop (2003)
3. Healey, G.E., Kondepudy, R.: Radiometric ccd camera calibration and noise estimation. IEEE Transactions on Pattern Analysis and Machine Intelligence 16(3), 267–276 (1994)
4. Johnson, M.K., Farid, H.: Exposing digital forgeries by detecting inconsistencies in lighting. In: Proc. of Workshop on Multimedia and security (2005)
5. Johnson, M.K., Farid, H.: Exposing digital forgeries through chromatic aberration. In: Proc. of International Multimedia Conference, pp. 48–55 (2006)
6. Lee, S.-J., Jung, S.-H.: A survey of watermarking techniques applied to multimedia. In: Proc. of IEEE International Symposium on Industrial Electronics, vol. 1, pp. 272–277 (2001)
7. Lin, Z., Wang, R., Tang, X., Shum, H.-Y.: Detecting doctored images using camera response normality and consistency. In: Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 1, pp. 1087–1092 (2005)
8. Liu, C., Szeliski, R., Kang, S.B., Lawrence Zitnick, C., Freeman, W.T.: Automatic estimation and removal of noise from a single image. Technical Report MSR-TR-2006-180, Microsoft Research (December 2006)
9. Lukáš, J., Fridrich, J., Goljan, M.: Determining digital image origin using sensor imperfections. In: Proc. of Society of Photo-Optical lnstrumentation Engineers Conference, vol. 5685, pp. 249–260 (2005)
10. Lukáš, J., Fridrich, J., Goljan, M.: Detecting digital image forgeries using sensor pattern noise. In: Proc. of Society of Photo-Optical Instrumentation Engineers Conference, vol. 6072, pp. 362–372 (2006)
11. Matsushita, Y., Lin, S.: Radiometric calibration from noise distributions. In: Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 1–8 (2007)
12. Motwani, M.C., Gadiya, M.C., Motwani, R.C., Harris Jr., F.C.: Survey of image denoising techniques. In: Proc. of Global Signal Processing Expo. and Conference (2004)
13. Tsin, Y., Ramesh, V., Kanade, T.: Statistical calibration of ccd imaging process. In: Proc. of IEEE International Conference on Computer Vision, vol. 1, pp. 480–487 (2001)
14. Van Lanh, T., Chong, K.-S., Emmanuel, S., Kankanhalli, M.S.: A survey on digital camera image forensic methods. In: Proc. of IEEE International Conference on Multimedia and Expo., pp. 16–19 (2007)
15. Wang, W., Farid, H.: Exposing digital forgeries in interlaced and deinterlaced video. IEEE Transactions on Information Forensics and Security 2(3), 438–449 (2007)
16. Wang, W., Farid, H.: Exposing digital forgeries in video by detecting duplication. In: Proc. of Workshop on Multimedia & security in International Multimedia Conference, pp. 35–42 (2007)
17. Ye, S., Sun, Q., Chang, E.-C.: Detecting digital image forgeries by measuring inconsistencies of blocking artifact. In: Proc. of IEEE International Conference on Multimedia and Expo., pp. 12–15 (2007)