ISSN:0975-9646

Naveen Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016, 363-366

Video Source Identification

Naveen Sharma, Anwer Reyaz J, Balan C

Resource Centre for Cyber Forensics
Centre for Development of Advanced Computing
Thiruvananthapuram, India

***Abstract*— Whenever there comes a cybercrime case related to multimedia, the first question which comes in a mind is what the source of this suspect multimedia is? Cases related to illegal copying and re-distribution of the media is growing innumerably. Digital photograph and video footage are an important or even crucial part of the incriminating evidence. In almost all past studies they have either focused on traditional cameras or traditional mobile cameras. To compete with the latest technology where sensors qualities have improved a lot it is very difficult to identify the proper source of a suspect video file. This compels further an area of study. We are using wavelet based technique to identify the source. To check the correlation performance we have used Peak-to-Correlation Energy (PCE) criteria. We have tested more than 250 videos/images taken from digital cameras /mobile cameras, using different permutation and combinations i.e. same make and models, same make and different models and different make and models, with accuracy rate of around 98%.**

Keywords*— *Digital forensics; Identification; photo-response non-uniformity; PCE

I. Introduction

Modern era is rapidly shifting from analog to digital world. Reliable identification of the source device used to acquire the digital files i.e. image or video, would especially prove useful in the court for establishing the origin of images presented as evidence. To determine the origin of a given digital image, several techniques have been developed. For instance, the aspect ratio of the photograph, color quantization tables and effects caused by color interpolation schemes [1] can be used to determine the camera model. These methods, however, only discriminate between camera models and thus cannot distinguish between the suspected source camera and a different camera of the exact same model. In the work of Jan Lukáš, Jessica Fridrich, and Miroslav Goljan[2], they proposed digital camera identification from its images based on the sensor's pattern noise. Erwin J,Geradts and Veenman [3] used the same PRNU patterns but to deal with the low quality compressed image material they did extensive experiments for both the closed and open set source camera identification problem. Kai, Edmund and Wong [4] present identification by noting the intrinsic lens radial distortion of each camera. To reduce manufacturing cost, the majority of digital cameras are equipped with lenses having rather spherical surfaces, whose inherent radial distortions serve as unique fingerprints in the images. Yuting Su,Junyu Xu and Bo Dong [5], proposed based on the motion vector information in the encoded stream; it takes full advantage of the various characteristics in the motion estimation algorithm in different video compression systems, and combines a k-nearest neighbor (k-NN) classifier to build a complete video system identification scheme. Xuemei Zhang and Brainard [6], to handle pixel saturation (Pixel where the incident light at a pixel causes one of the color channels of the camera sensor to respond at its maximum value) which sometimes produce undesirable artifacts in digital color images used Bayesian algorithm that estimates what the saturated channel's value would have been in the absence of saturation. Another approach to identify the source device is analysis of pixel defects. In [7], the authors show that hot pixels or dead pixels (defective pixels in general), could be used for reliable camera identification even from lossy JPEG compressed images. However, there are cameras that do not contain any defective pixels or cameras that eliminate defective pixels by post-processing their images on-board. For such cameras or sensors, this method cannot be applied.

Using the method described in [11], one can compute a prediction for the green channel, and subsequently predictions for the red and blue channel. These three predictions can then be used as features. The algorithm divides the image into blocks and lets each block cast one vote on which of the types of Bayer patterns that is the most likely. The algorithm concludes that the configuration that is the most likely one for the most blocks is the true configuration. An algorithm for clustering of noise patterns was proposed by Caldelli . [12] that begins by calculating a comparison matrix, where each noise pattern is correlated with all other noise patterns. The noise patterns used in the paper are modified by a method that is supposed to enhance the noise

The source identification method based on PRNU noise proposed in this paper gives more reliable results than the previous approaches. Use of peak-to-correlation energy to evaluate the correlation performance for the classification make it a good candidate for the equivalent of biometrics for sensors suitable for forensic applications.

II. Methodology

Here we will use two terms frequently i.e. reference and suspect. The term 'reference' refers to the file used for training while 'suspect' refers to the file under forensics analysis. Our methodology is divided into the following parts.

A. Preprocessing

Frames are taken from the video files. Following are few points which need to be taken care while using our methods.

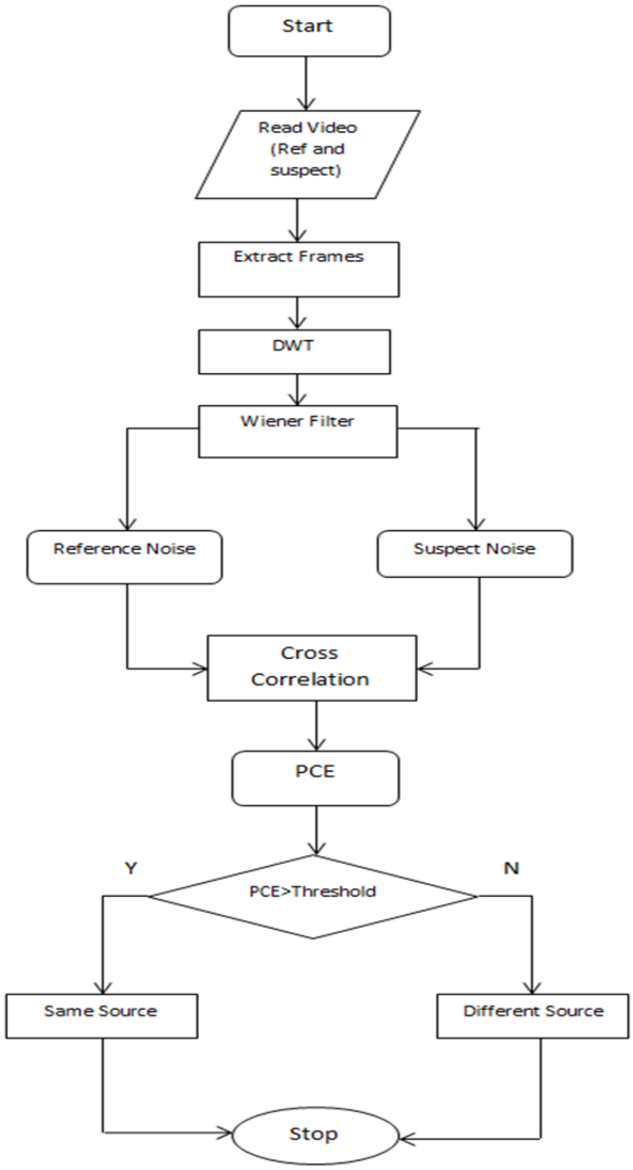
1. Resolution should be same for both the video files i.e. suspect as well reference file.
2. For reference noise pattern, take at least 150-200 frames/images if ,uniformly lit scenes known as flat fielding ,images/frames are used, otherwise take 300 images/frames of natural scenes.
3. For suspect noise pattern, take at least 50 images/ frames.

B. Sensor noise

There are various source of imperfection and noise that enter into different stages of media acquisition process. Even if it is taken in an absolutely evenly lit scene, still there will be small variation in intensity between individual pixels. This is because of two different noise known as short noise (Which is a random component) and pattern noise (a deterministic component that stays approximately the same if multiple pictures of the exact same scene are taken). Pattern noise is of two type. 1) Fixed pattern noise which is caused by dark current and is primarily refer to pixel-to-pixel differences when the sensor array is not exposed to light. Since FPN is an additive noise, high end cameras suppress this noise automatically by subtracting a dark frame from every image they take. FPN also depends on exposure and temperature. On the other hand 2) Photo-response non-uniformity noise (PRNU), define as different sensitivity of pixels to light caused by the inhomogeneity of silicon wafers and imperfections during the sensor manufacturing process. This noise is not affected by affected by ambient temperature or humidity. So PRNU can be taken as intrinsic characteristic of the sensor.

C. Media Source Identification Algorithm

To extract reference noise pattern flat fielding images are used. Firstly we calculate 4-Level wavelet decomposition with daubechies wavelet. At every level, for each subband (vertical, horizontal, and diagonal) local variance is calculated. To denoise the wavelet coefficients, Wiener filter is used. Getting the denoising coefficient once subtracting from the original image we get reference pattern. Similar process is followed for getting suspect noise pattern. Using the pattern from both sources, correlation is calculated. To evaluate the correlation performance, Peak-to-Correlation Energy (PCE) is used.



III. EXPERIMENTS AND RESULTS

To measure the effectiveness of the algorithm, different combination of are taken. We have tested different set of mobiles as well as digital cameras.

1. Same make and model e.g. Make: Nikon CoolPix P340 & Model: Nikon CoolPix P340
2. Same make and different model e.g. Make: Nikon CoolPix P340 & Model: Nikon CoolPix S9900
3. Different make and different model e.g. Make: Nikon CoolPix P340 & Model: SonyH20

The combination of the used dataset is taken in such a way where almost all the lightening conditions are taken care i.e. indoor, outdoor, low light, high light, and variation in resolutions. We have tested almost 250 videos. Classification threshold is consider as if PCE>50 the suspect and reference source is same else different. For combination of the testing we took one video from the reference camera and tested it with other videos of the same reference camera as well as videos taken from other camera (suspect).

RESULTS

1. Noise pattern in the case of reference and suspect camera match

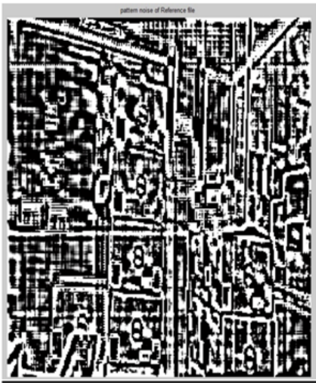


Figure 2. Pattern noise of Reference file

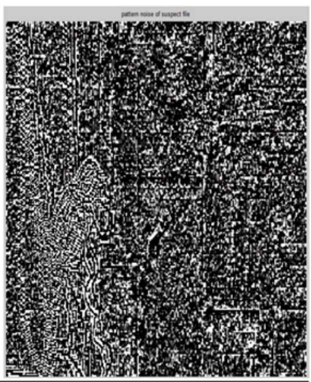


Figure 3. Pattern noise of Suspect file

2. Noise pattern in the case of reference and suspect camera mismatch

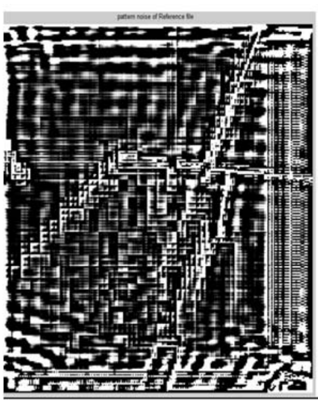


Figure 4. Pattern noise of Reference file

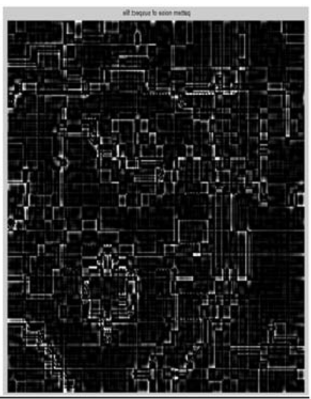


Figure 5. Pattern noise of Suspect file

Table 1. Same make and model. (100% accuracy)

Reference /Suspect	CoolPixL28-Black	CoolPixL28-White
	251610	28.64
CoolPixL28-Black	**144.15**	24.06
	818.075	20.738
	993.24	13.147

Table 2. Same make and different model. (95% accuracy)

Reference /Suspect	Samsung S7562	Samsung I9070	Samsung S2	Samsung GTI8162
	73923	-0.3176	2.5361	0.9455
	33.973	1.29	0.0003	1.7873
Samsung S7562	**99.677**	-0.2621	4.87	2.5598
	833.867	0.414	3.8773	15.884
	243.89	-0.0646	0.2329	0.8771

Table 3. Different make and different model. (100% accuracy)

Reference /Suspect	MotoXt1033	Nokia520	Sony H20	Nikon CoolPIX21	IPhone 4	Panasonic HC-V160	Xiaomi Redmi 2
	143610	-0.8863	3.946	-0.507	-6.1897	6.7973	16.5766
MotoXt1033	**1030.4**	1.7239	5.8306	0.4591	5.7341	6.4622	9.2501
	6387.8	-0.0747	-0.1259	2.4755	-0.6692	0.0031	2.96
	199.466	3.532	-0.162	18.4874	-1.334	1.1528	9.0563

Overall looking at the above result it clearly identify the source, irrespective of the condition. Our method has been tested for the videos taken from digital camera, smart phone and camcorder. In all the previous research regarding source camera identification they have mostly restricted their methods to a particular type of source i.e. either a traditional cameras or mobile phone but our method has been successfully tested for images(jpeg) as well as videos taken from digital camera ,mobile phones and HD Camcorders with a accuracy of around 98%.

IV. CONCLUSION

A novel methodology for source camera identification has been developed from a continuous research conducted by analyzing a number of videos and image file. The advantage of the method described here is that it works for almost all type of digital camera as well as mobiles phone cameras with high accuracy. Certainly, this could be extremely useful to cyber forensics investigators as a lots of crime is happening related to multimedia forensics like video footage and images etc. Today, media forensics is highly recommended for a cybercrime investigation, especially for incident responding, and thus more research is recommended in this area to bring out highly efficient algorithm.

ACKNOWLEDGMENT

This research is supported by Resource Center for Cyber Forensics (RCCF) Department, Centre for Development of Advanced Computing (CDAC), Thiruvananthapuram, India.

REFERENCES

[1] S. Bayram, H. Sencar, N. Memon, and I. Avcibas. “Source camera identification based on cfa interpolation” IEEE International Conference on Image Processing, volume 3, pages 69–72, 2005.

[2] Jan Lukáš, Jessica Fridrich, and Miroslav Goljan, “Digital Camera Identification from Sensor Pattern Noise,” Information Forensics and Security, IEEE Transactions on, pp. 205-214, June 2006.

[3] Erwin J,Geradts and Veenman “Source Camera Identification for Low Resolution Heavily Compressed Images”, ICCSA , pp. 557-567,2008.

[4] Kai,Edmund and Wong, “Automatic source camera identification using the intrinsic lens radial distortion,” Optical Society of America, vol., pp. 11551-11565,2006.

[5] Yuting Su,Junyu Xu and Bo Dong, “A source video identification algorithm based on motion vectors,” WCSE '09. Second International Workshop on Vol:2,pp. 312 – 316,2009.

[6] Xuemei Zhang and Brainard, “Estimation of saturated pixel values in digital color imaging” Optical Society of America, 2004.

[7] Geradts, Z., Bijhold, J., Kieft, M., Kurosawa, K., Kuroki, K., and Saitoh,N.: “Methods for Identification of Images Acquired with Digital Cameras,” Proc. of SPIE, Enabling Technologies for Law Enforcement and Security, vol. 4232, pp. 505–512, February 2001.

[8] Razzazi, F ,Seyedabadi, A. “A robust feature for single image camera identification using local binary patterns” Pp 462 - 467 ,IEEE -2014

[9] Shaxun Chen, Amit Pande, Kai Zeng, and Prasant Mohapatra,"Live Video Forensics: Source Identification in Lossy Wireless Networks" Pp 28 - 39,IEEE Transactions ,October 2014`

[10] Fatma H, Mohamed I and Salah Deyab, “Comparison between Haar and Daubechies Wavelet transformation on FPGA Technology, Vol-2 World Academy of Science, Engineering and Technology 2008.

[11] M. Kirchner, "Efficient Estimation of CFA Pattern Configuration in Digital Camera Images," Proceedings of SPIE Electronic Imaging, vol. 7541, January 2010.

[12] R. Caldelli, I. Amerini, F. Picchioni, and M. Innocenti, "Fast image clustering of unknown source images," IEEE International Workshop on Information Forensics and Security, pp. 1-5, December 2010