Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.336 – 343

VIDEO CAMERA FEATURE EXTRACTION USING SENSOR PATTERN NOISE ON GRAY SCALE IMAGES

Jagbeer Kaur*[1], Deep Kamal Kaur Randhawa[2]
ECE Department, GNDU RC Jalandhar, INDIA*[1],[2]
Department of Electronics & Communication Engineering, GNDU, Amritsar, INDIA[3]
Kaurjagbeer29@gmail.com *[1], randhawadk@gmail.com [2]

Abstract: This paper proposed sensor pattern noise based method that exploits the inherent fingerprint of the camera sensor and is universally applicable and can be easily used to authenticate a video camera. The central idea of the paper is that correlated signal is compressible and predictable but uncorrelated noise is not. So, far work proposed uses three different color channels for noise estimation. We propose to work on grayscale images. The result shows when working on grayscale images gives same result in less time.

Keywords: Discrete Wavelet Transform, Gray Scale Image, Sensor Pattern Noise, Wiener Filter.

I. Introduction

Video Source identification method can be classified in two categories. The first category is device class identification which is used to tell the manufacturer or model of the device. The second category is specific device identification which deals with identification of identify the individual device that has produced the data. The first category identification is easier as image source identification methods can be easily adopted directly for video source identification to distinguish different models. It is bit easier to distinguish different models but difficult when identifying specific device. Some methods like watermarking technique helps to find specific device but have special limits on videos. Now, with advancement of technology, the world enters in wireless communication. The use of wireless camera has increased. The wireless cameras are generally used in a special security region. These cameras have no local storage. The video is captured and wirelessly streamed to a sink. Due to transmission delay in wireless streaming, some packets are lost causing blocking and blurring that appear in the received frames. Thus, when working on wireless networks the concern is to authenticate source of video. There is need to exploits the inherent fingerprint of camera sensor which must be universally applicable.

Video Source identification is widely used for validating video evidence in court as it necessary to prove that the video was truly recorded by the suspected camera [1]. It also, helps in tracking down video piracy crimes [2] [3] and help to regulate individual video sources on internet where videos are shared at large scale [4].

Modern digital cameras use tag such as date and time, camera settings, or the serial number of the camera when producing the image. Currently, there is no standard metadata pattern for video files. Also, when this metadata is present, it can be easily removed or manipulated. This can lead us to doubt about the source of image. Another method is Defective Pixels identification in which the defective pixels can act as a digital finger print which are present in sensor [5]. Defective pixels can be corrected by modern camera with additional features. This will give us false result and our motive to authenticate the suspect camera will

be not accomplished. Researcher moves to new techniques which focus on individual pixels that may report slightly lower or higher values than their neighbors. The Method based on PRNU (Photo Response Non-Uniformity) which is the output signals from pixels produced when the illumination incident on a number of pixels is exactly same for all pixels. To a certain extent, this pattern will be present in all images captured by a certain sensor like CCD or CMOS active pixel sensors cannot be easily removed by layman. But PRNU method suffers from performance degradation when the video is captured by wireless camera and contain blocking and blurring during transmission. Besides, most of these sensor methods are computationally expensive and are not suitable for fast identification. There will be need of making large data base. Recent work focus on fixed pattern extraction. Sensor pattern noise has been reported with best performance so far. It is based on idea that correlated signal is compressible and predictable but uncorrelated noise is not. This means each sensor has its own unique noise pattern. Sensor pattern noise which is extracted from a frame of video will be tested and compared with the suspected patterns from the trained database of cameras. When the two patterns are highly similar, almost having negligible difference than this indicates source might be same. Thus, it helps in source identification. Now another important aspect of wireless cameras is spoofing attack. Spoofing attack means that an attacker had send another video to the sink using the victim's identity. Sensor Pattern Noise also deals with this issue easily.

II. Literature Survey

The research on video source identification is quite similar to image source identification, and often similar techniques are used for both identifications. A brief survey has been paragraphed below after reading the main outcomes of various journals on this topic. Kharrazi et al. [7] had proposed a simple method to identify the camera model which was used to obtain an image by distinguishing between images captured by a two and five different camera models. They proposed color image features like average pixel values and RGB correlation factor with SVM to identify device which have captured the image. Result shows acceptable accuracy even when the image is re-compressed. Similarly, Celiktutan et al. [8] focused on problem to identify a source cell-phone in blind manner. The idea was to differentiate the color characteristic which gives footprints in form of correlation factor across the adjacent pixel of the images. For this purpose, they explored various classifier which deals with similar image quality measures and high order wavelet statistics. They had used SVM and KNN classifiers to detect the cell-phone. They provide identification results among nine different brand cell-phone cameras and had used a large known image data set and direct research to increase classification accuracy. Choi et al. [9] further included lens radial distortions as part of the features extraction. They demonstrated that by taking the intrinsic lens radial distortion of each camera one can identify suspected camera with a high rate of accuracy. By using lenses with spherical surface having inherent radial distortion gives unique fingerprints of the images and also help in reducing manufacturing cost. They have conducted experiment using five cameras to show statistical the improvement. The results also show that the error rates also change in image datasets when captured using various optical zoom levels and finds that method is not much efficient as zooming makes difficult to work with radial distortion. Popescu et. al. [10] deals to authenticate an image by finding digital tampering in absence of digital signature or water marking. They have developed a detection tool for forensics using the Expectation/Maximization algorithm to identify the camera patterns, based on which different image sources are classified. A large database of 200 gray scale images was built and pattern was searched using Fourier transform from the original unadulterated images. The periodic patterns obtained during re-sampling using Fourier domain can help in telling the model or the manufacturer of the device, instead of identifying the individual camera that produced the image for forensic applications. Geradts et al. [5] proposed to utilize sensor dead pixels or hot pixels in identification of specific image source. They focus that many modern cameras are not having defective pixels, and now cameras are available which can eliminate these defective pixels easily during on board post-processing. They examined and conclude that noise levels should be used for investigation because the camera of suspect can help to give a fixed pattern noise even if we have nothing in it. Lukas et al. [6] also proposed to examine a suspected camera using sensor pattern noise. The first need is to determine reference pattern noise. This will give a unique fingerprint of each camera for identification. They have considered the reference pattern noise as a spread spectrum watermark established using a correlation detector. The Experiments were implemented on approximately 320 images captured from nine consumer digital cameras. Also, have worked on images having JPEG Compression or gamma correction. They concluded that sensor pattern noise estimation using wavelet decomposition can distinguish between two cameras of same brand also. Li et. al. [11] proposed source identification using sensor pattern noise method. The forensics investigator generally has large data set from various cameras and can utilize it in making number of classes. When situation arises that, there was no knowledge of the original device and even not the image from original source of image to be tested. It leads us to digital wavelet transform domain to enhance even the weak component of the pattern noise. Kurosawa et al. [12] propose that source identification can be achieved by measuring the dark current noise of the sensor which is used to give the device fingerprint. It is effective for dark current noise extracted from 100 dark frames. Chen et al. [2] inherited the idea proposed in [13] and applied it to videos. They also investigate the problem of determining whether two video clips came from the same camcorder and the problem of whether two differently transcoded versions of one movie came from the same camcorder. The source identification technique is based on estimating the Maximum Likelihood factor and deals with blocking and blurring using PRNU normalized cross-correlation. With decrease in video quality, there was need to increase video length that means will always require large data set and accuracy decreases with video quality. This is a

disadvantage of using PRNU pattern noise. Houten et al. [14] and Hyun et al. [15] extended Chen's method to implement on low resolution videos. It is based on enhanced PRNU pattern noise method. All these solutions also suffer from performance degradation when the video is captured by wireless cameras because will contain blocking and blurring. These methods are not only computationally expensive but not also suitable for fast identification. In present time, use of wireless cameras has increased. They are widely used for security purpose. The security issues like spoofing attack are stemming in the wireless communication. This means need faster and most accurate method to be explored. Lawgaly A et. al. [18] has concentrate on different color channels for PRNU estimation. They have used Locally Adaptive DCT filtering and Weighted Averaging value of three color channels. The motivation of work was that images are acquired under different conditions giving rise to different residual noise. The weighted average value of the three channel helps to eliminate this residual noise for best match. It is complex technique which require high time value, not suitable in wireless network for fast detection. Also, require large dataset to train and test a query video. S. Chen et. al. [1] proposed sensor pattern noise method is efficient method. It works effectively for identifying wirelessly transmitted videos which have blocking and blurring due to packet loss during wireless transmissions. In addition, they proposed to incorporate selective frame processing and wireless channel signatures in source identification, which makes source identification faster. Extensive real-world experiments were conducted to validate the method. The results show that the accuracy of source identification based on the proposed method is far better than the existing methods in the presence of video blocking and blurring. The method identifies the video source in a real-time environment to detect spoofing attack. The paper has conclusion that number of existing studies are orthogonal to source identification. So, there is need to explore and incorporate it with the method to make it more accurate and less complex.

III. Sensor Pattern Noise Extraction

Sensor pattern noise has been evaluated for randomly selected camera frames. In first step, frames have been extracted from the video using VideoReader Mat lab command. VideoReader (filename) is used to create object v. The object v will read video data from the file named as filename. Five Frames are selected randomly from a video. Here instead of working on RGB channels, we are using gray scale image for sensor pattern noise generation to decrease complexity. Now there is only one channel for further processing.

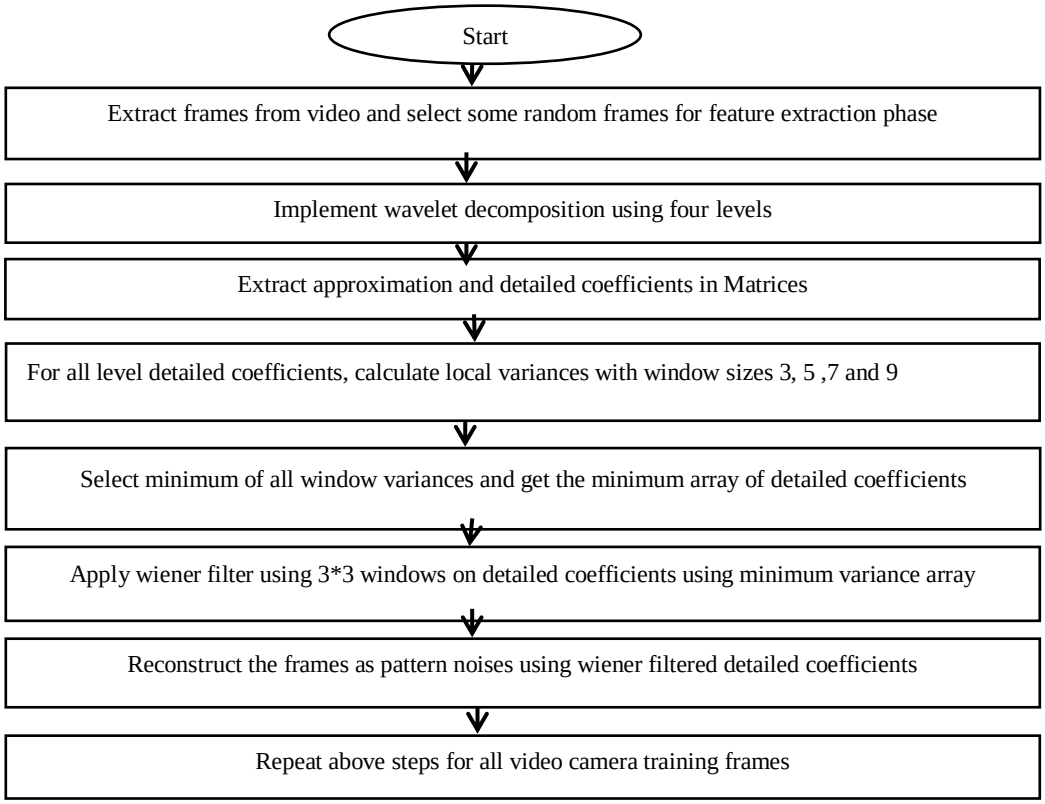


Figure 3.1 Flowchart for pattern noise generation

For this rgb2gray Mat lab function has been used. Otherwise first we have to perform wavelet implementation on each channel then combine the three channels data to have denoised image. The combination of three color channel will include interpolation noise when color location vary with luminance light[16]. Wavelet implementation is described further in flowchart.

The main effect that has been produced in detailed coefficients has been caused by wiener filter. Wiener filter[17] uses the first order statistics such as the mean and the variance of the neighborhood.

This filter follows the following equation.

$$f_{x,y} = \bar{g} + k_{x,y}(g_{x,y} - \bar{g}) \tag{3.1}$$

Here $f_{x,y}$ is the estimated noise-free pixel value, $g_{x,y}$ is the noisy pixel value in the moving window, $\bar{g}$ is local mean value of an $N_1 * N_2$ region surrounding $g_{x,y}$, $k_{x,y}$ is a weighting factor with $k \epsilon [0..1]$ and x, y are the pixel coordinates. The factor $k_{x,y}$ is the function of the local statistics in a moving window.

$$k_{x,y} = \frac{\sigma^2 - \sigma_n^2}{\sigma^2} \tag{3.2}$$

The values σ^2 and σ_n^2 represent the variance in moving window and variance of the noise in the whole image respectively [18], [19].

IV. Experimental Setup

Videos have been collected for eight digital cameras used in wireless transmission. Table below shows the video cameras chosen in this work. To implement the algorithm formed we will use MATLAB tool. MATLAB software is widely used in various research work. MATLAB stands for MATRIX LABORATORY. The Software was developed by Math works honor (www.mathworks.com) in USA. MATLAB is beneficial for mathematics equations (linear algebra) moreover numerical integration equations are also solved by MATLAB. It is also a simple programming language for writing mathematical program. It has various types of tool boxes that are very beneficial for optimization.

Table 4.1 A list of video cameras selected for testing

AXIS M1011
D-Link DCS-942L
Foscam FI8910W
Smiledrive Panoramic 360
TP-Link NC220
TRENDnet TV-IP672W
WVC80N Camera test
ZVision AHD 1.3 MP

V. Result Analysis

The results found at every step have been visualized and explained as under of Axis M1011 camera frame in detail.

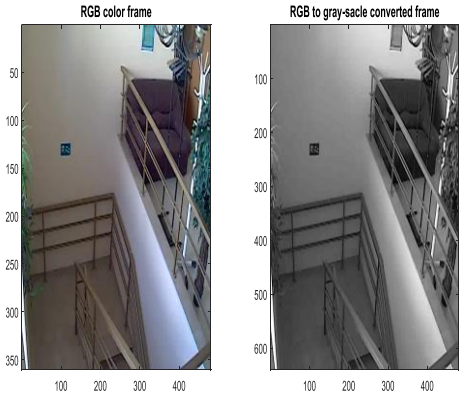
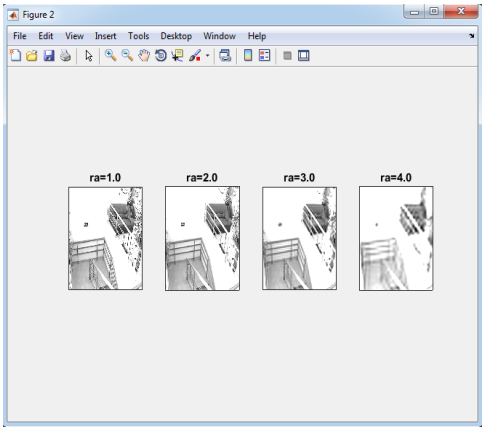


Figure 5.1 (a) RGB color frame gray-scale frame



(b) Figure 5.2 Approximation DWT coefficients at four level

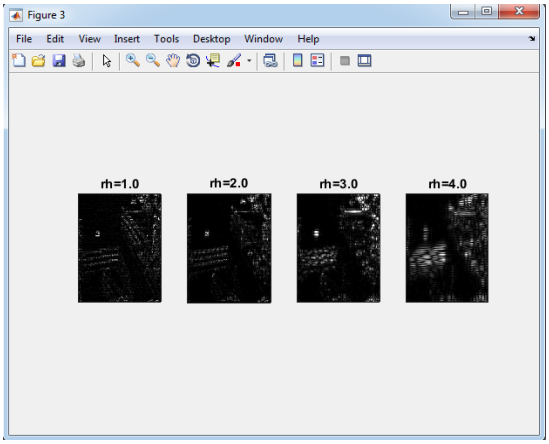


Figure 5.3 Detailed Horizontal DWT coefficients at four levels

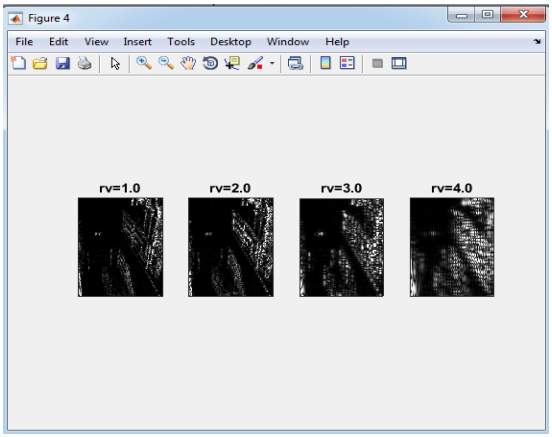


Figure 5.4 Detailed Vertical DWT coefficients at four levels

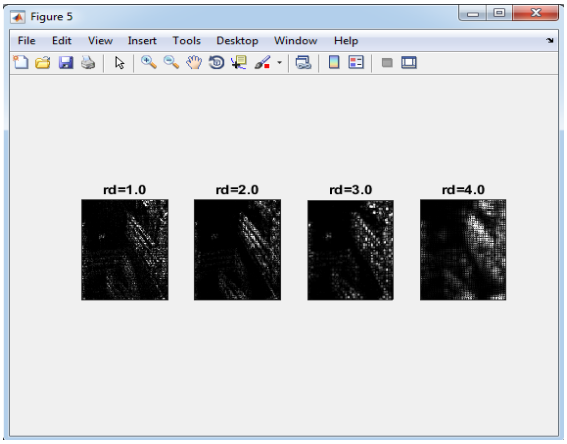


Figure 5.5 Detailed diagonal DWT coefficients at four levels

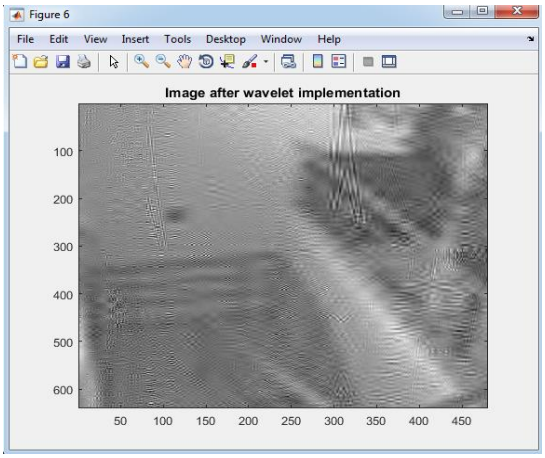


Figure 5.6 Image after wavelet reconstruction

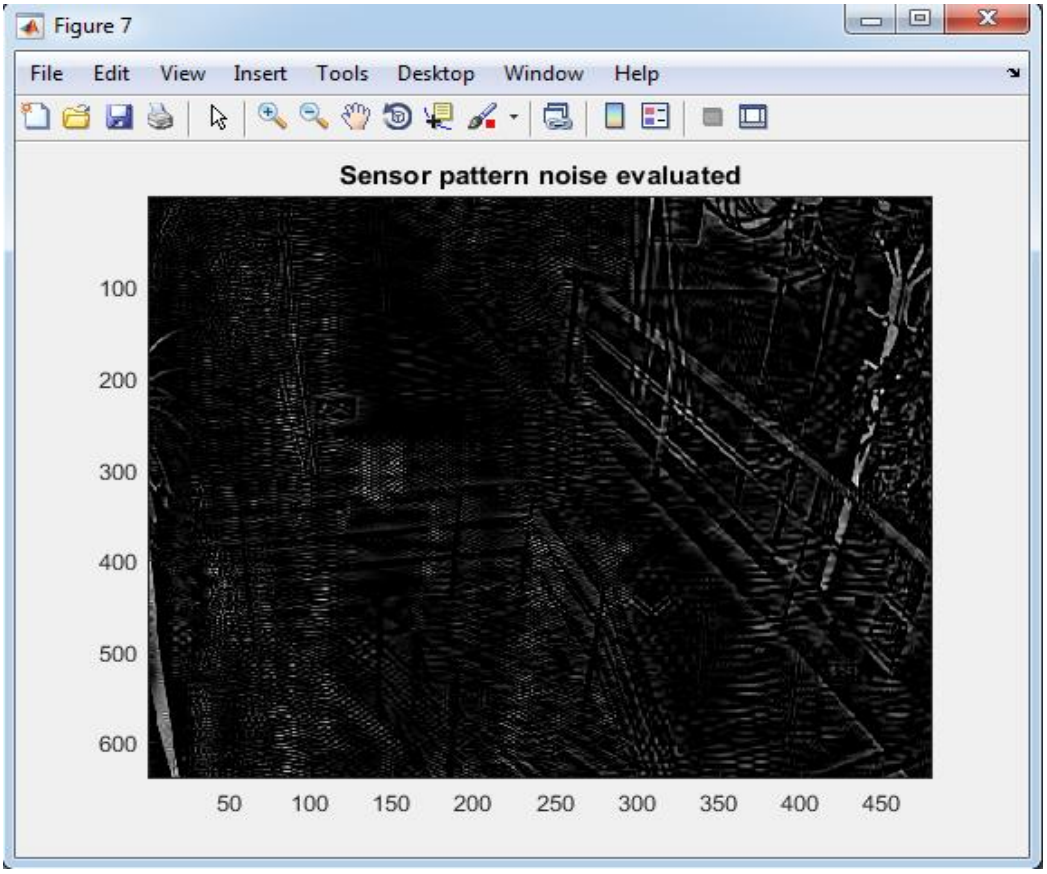


Figure 5.7 Sensor pattern noise as difference of original frame and reconstructed frame after wavelet implementation

Table 5.1 Time Performance Analysis

Camera No	Camera Name	Time taken for SPN of a Frame(seconds)		
		RGB	Grayscale	Difference
1	AXIS M1011	579.95	77.21	502.74
2	D-Link DCS-942L	847.34	54.77	792.57
3	Foscam FI8910W	865.25	153.53	711.72
4	Smiledrive Panoramic 360	941.02	132.76	808.26
5	TP-Link NC220	817.26	172.36	644.9
6	TRENDnet TV-IP672W	781.51	81.33	700.18
7	WVC80N Camera test	889.91	131.21	758.7
8	ZVision AHD 1.3 MP	1250.51	234.42	1016.09
Average		871.59	129.69	1071.59

Time Performance has been evaluated on the intel core i5 processor of 8 different wireless transmitted videos of different cameras. It shows working on grayscale in spite of three channel will save time of approximately 5-6 minutes on average.

Figure 5.8 and 5.9 visualize the SPN when working on rgb and gray scale image respectively and finds grayscale effective when working on minute details as weighting averaging value of three channel eliminate residual noise that is not effective

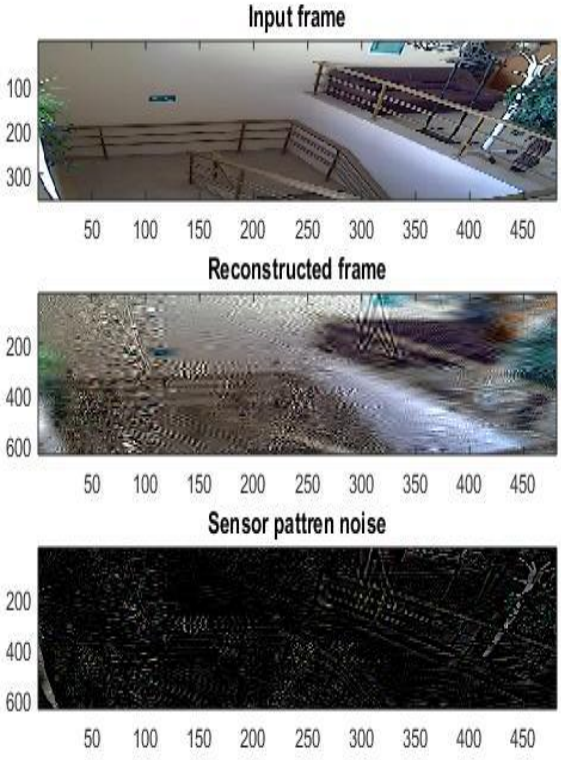


Figure 5.8 Sensor pattern noise for RGB Image

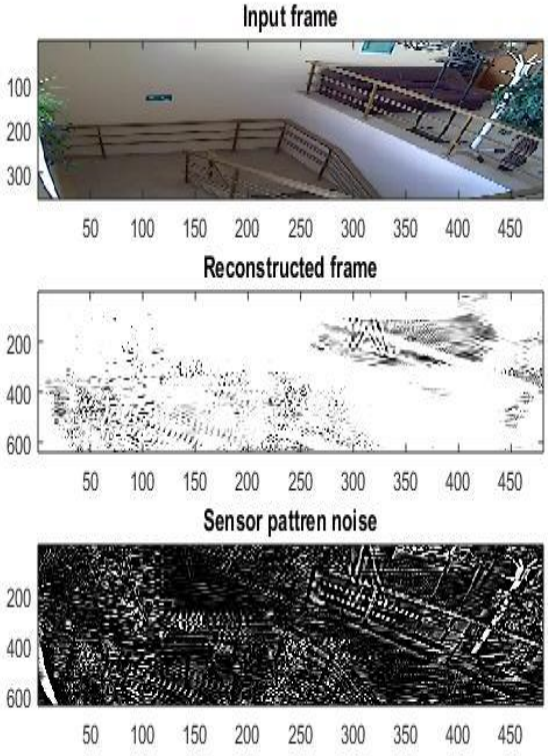


Figure 5.9 Sensor pattern noise for Grayscale Image

VI. Conclusion

The sensor pattern noise method exploits the inherent fingerprint of camera sensor and is universally applicable. This method has the best performance reported so far among the existing methods and only method effective in lossy wireless network. It is applicable on different size video. It leads us to conclusion that it is more reliable, accurate and less complex. It gives a direction to work on grayscale images instead of three channels to reduce time complexity. The future scope for this method is that algorithm can be made more effective when dealing with illumination factor and heavy packet loss. Active research work with advanced security attacks in wireless network to make it further effective in real time environment.

References

[1] S. Chen, A. Pande, K. Zeng, and P. Mohapatra, January 2015, " Live Video Forensics: Source Identification in Lossy Wireless Networks," IEEE Transactions on Information Forensics and Security, vol.10, NO.1, pp. 28 - 39.

[2] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, February 2007, "Source digital camcorder identification using sensor photo response non-uniformity," Proceeding SPIE, Security, Steganogr., Watermarking Multimedia Contents IX, vol. 6505, no. 1, pp. 65051G.

[3] F. Lefebvre, B. Chupeau, A. Massoudi, and E. Diehl, February 2009, "Image and video fingerprinting: Forensic applications," Proceeding SPIE, Media Forensics Security, vol. 7254, pp. 1–9, Art. ID 725405.

[4] Y. Su, J. Xu, and B. Dong, October 2009, "A source video identification algorithm based on motion vectors" in Proceeding 2nd International Workshop Computer Science Engineering, Vol. 2., pp. 312–316.

[5] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, February 2001, "Methods for identification of images acquired with digital cameras," Proceeding SPIE, Enabling Technolology Law Enforcement Security, vol. 4232, pp. 505–512.

[6] J. Lukáš, J. Fridrich, and M. Goljan, June 2006, "Digital camera identification from sensor pattern noise" IEEE Transactions Information Forensics Security, vol. 1, no. 2, pp. 205–214.

[7] M. Kharrazi, H. T. Sencar, and N. Memon, "Blind source camera identification," in Proceedings IEEE International Conference Image Processing, Singapore, pp. 709–712, October 2004.

[8] O. Celiktutan, I. Avcibas, B. Sankur, and N. Memon, "Source cell-phone identification," in Proceesing International Conference Advance Computer Communication, Tamil Nadu, India, 2005.

[9] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Automatic source camera identification using the intrinsic lens radial distortion," Optics Express, vol. 14, no. 24, pp. 11551–11565, 2006.

[10] A. C. Popescu, 2004, "Statistical tools for digital image forensics," Ph.D. dissertation, Department of Computer Science., Dartmouth College, Hanover, NH, USA.

[11] C.-T. Li, June 2010, "Source camera identification using enhanced sensor pattern noise," IEEE Transactions Information Forensics Security, vol. 5, no. 2, pp. 280–287.

[12] K. Kurosawa, K. Kuroki, and N. Saitoh, 1999, "CCD fingerprint method—Identification of a video camera from videotaped images," in Proceeding IEEE International Conference of Image Processing, pp. 537–540.

[13] [10] Zeno J Geradts, Jurrien Bijhold, Martijn Kie, Kenro Kuroki, and Naoki Saitoh, 2001, " Methods for identification of images acquired with digital cameras,".

[14] W. van Houten and Z. Geradts, 2009, "Source video camera identification for multiply compressed videos originating from YouTube," Digital Investigation., vol. 6, nos. 1–2, pp. 48–60.

[15] D.-K. Hyun, C.-H.Choi, and H.-K. Lee, 2012, "Camcorder identification for heavily compressed low resolution videos " in Computer Science and Convergence, Amsterdam, The Netherlands: Springer-Verlag, vol. 114, pp. 695–701.

[16] Ashref Lawgaly, and Fouad Khelifi, 2016, "Sensor Pattern Noise Estimation Based on Improved Locally Adaptive DCT Filtering and Weighted Averaging for Source Camera Identification and Verification", IEEE Transactions On Information Forensics And Security.

[17] H. Zhang, A. Nosratinia and R. O. Wells, 2000,"Image denoising via wavelet-domain spatially adaptive FIR Wiener filtering," IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No.00CH37100), Istanbul, pp. 2179-2182 vol.4.

[18] C. Loizou, C. Christodoulou, C. Pattichis, R. Istepanian, M. Pantziaris, and A. Nicolaides, 2002, "Speckle Reduction in Ultrasound Images of Atherosclerotic Carotid Plaque," In Proceeding of IEEE conference on DSP, pp. 525-528.

[19] C. P. Loizou, C. S. Pattichis, C. I. Christodoulou, R. S. Istepanian, M. Pantziaris and A. Nicolaides, 2005, "Comparative evaluation of de-speckle filtering in ultrasound imaging of the carotid artery," IEEE Transactions on Ultrasonic, Ferroelectrics and Frequency Control, vol. 52, no. 10, pp. 1653-1669.

