Digital Image forensics using noise features

Abhijit Sharang, Pankaj Jindal

1 Motivation

Advances in digital image techniques has simplified the task of image manipulation. Traces of image tampering by software can be easily covered.This undermines the credibility of digital images. Establishing the authenticity of digital images is important as digital images are used in a wide number of applications related to military, law enforcement, surveillence, intelligence etc....
The field of digital image forensics is an emerging field that aims to determine the origin and potential authenticity of digital images. In general, two approaches are used for detecting image tampering. In the first approach, the aim is to identify a specific kind of image forgery, which may include image splicing, image composition or something as basic as image rotation. Though these methods work well in identifying a paticular kind of forgery, it would require an exhaustive search over all kinds of operations to establish the authenticity of an image. The second approach aims at blind image forensics which is more general and targets teh image without making any assumptions on the type of forgery. Generally, classifiers are used in this approach.

2 Methodology

A novel method for differentiating between camera generated and computer generated images has been proposed by Memon et al.[1]. As argued by them, the pattern noise introduced by cameras may have common statistical properties as the deployed image sensor technology remains same, and that this common characteristic would not be present in images generated by computer software. Similarly, computer generated images may exhibit common properties because of the similarity of the algorithms used by computer software. Various methods exist to obtain the noise in images. Examples include the use of quadrature mirror filters, wavelet statistics, neighbourhood prediction and autocorrelation.[2][3][4]

A classifier can be built using these features to distinguish between real and fake images. We intend to use a Support Vector Machine with a radial basis function as the classifier as it can construct a non-linear classification surface between the two classes of data viz. real and fake images.

3 Data Set

The database for computer generated images is abundant. Various websites can be referred to for obtaining these images. For camera generated images, we aim to use the Dresden image database.[5].

References

[1] S.Dehnie,H.T. Sencar,and N.Memon, "Digital image forensics for identifying computer generated and digital camera images", in Proc.*IEEE Int. Conf.Image Processing (ICIP)*, Atlanta, GA, 2006, pp. 2313-2316.

[2] S. Lyu and H. Farid,"How realistic is photorealistic?"*IEEE Trans. SignalProcessing*, vol. 53, no. 2, pp. 845850, 2005.

[3] Khanna, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp,"Forensic techniques for classifying scanner, computer generated and digital camera images,"*in Proc. IEEE ICASSP, Mar. 31Apr. 4, 2008*, pp. 16531656.

[4] Hongmei Gou; Swaminathan, A.; Min Wu; ,"Noise Features for Image Tampering Detection and Steganalysis,"*Image Processing, 2007. ICIP 2007. IEEE International Conference on*, vol.6, no., pp.VI-97-VI-100, Sept. 16 2007-Oct. 19 2007

[5] Gloe, T., Bhme, R. (2010). "The Dresden Image Database for benchmarking digital image forensics".*In Proceedings of the 25th Symposium on Applied Computing (ACM SAC 2010)* (Vol. 2, pp. 15851591).