**M ABDULLAH NAWAZ**

**I21-1393**

**Dip Literature Review  
  
  
  
15. Literature Review: Image Forgery Detection Techniques**

Image forgery detection has become increasingly important in today's digital age as the manipulation of images is becoming more sophisticated and widespread. The article presents a comprehensive overview of image forgery detection techniques, focusing on Copy-Move and spliced images. The author has divided the main techniques into two main categories: Copy-Move Forgery Detection (CMFD) and Spliced Image Detection.

**Copy-Move Forgery Detection (CMFD) Techniques**

CMFD techniques aim to identify images where regions have been copied and pasted from other parts of the same image. These techniques typically involve dividing the image into blocks, extracting features from these blocks, and comparing the features to detect duplicates. The article reviews various CMFD techniques including extraction of feature with transformation and extraction of feature without transformation.

**Spliced Image Detection (SID) Techniques**

SID techniques detect images where regions have been spliced from different images. These techniques often focus on inconsistencies in image features or camera characteristics between the spliced regions and the rest of the image. The writer mentioned two of its types as Image Features-based Techniques and Camera Characteristics-based Techniques.

**Key Findings**

1. Both CMFD and SID techniques have made significant advancements in recent years.
2. CMFD techniques have become more robust against various image processing operations, such as JPEG compression and noise addition.
3. SID techniques have improved in their ability to detect spliced images with varying degrees of success.
4. A combination of CMFD and SID techniques may be necessary to detect complex forgeries.
5. The article identifies future research directions including reducing computational complexity, increasing detection rates and developing faster algorithms.

**Future Methodologies**

Researchers should continue to develop more efficient and accurate algorithms for both CMFD and SID. Reducing computational complexity is essential for real-time applications. Addressing the challenges posed by advanced image manipulation techniques is crucial.

**Conclusion**

Image forgery detection is a rapidly evolving field with significant implications for various applications, including law enforcement, journalism, and digital forensics. By understanding the strengths and limitations of different techniques, researchers can develop more effective tools to combat image forgery and protect the integrity of digital information. And authors should done research on future research directions, reducing computational complexity and increasing detection rates.

**16. Literature Review: Estimating Light Source Direction from a Single Image**

This research explores a method to determine the direction of a light source from a single image. This information can be useful in detecting digital tampering, as changes in lighting can be a sign of manipulation. The authors extend previous work in the field of computer vision to make the problem more tractable and applicable to forensic applications.

**CONCEPT**

The technique that estimates the light source direction from a single image by analyzing the intensity and surface normal along an occluding boundary. The technique assumes that the surface is Lambertian and has a constant reflectance value, and is illuminated by a point light source infinitely far away.

**Key Contributions**

1. The authors relax the assumption of constant reflectance along the entire surface by estimating the source directions for each surface patch considering local light sources.
2. Another technique mention in this article is about: The technique can be extended to handle multiple light sources by estimating a "virtual" light source, which is the vector sum of the individual light sources.

**Conclusion**

This research offers a valuable tool for analyzing images and detecting potential tampering. By estimating light source direction, it provides insights into the image's creation and can help identify inconsistencies that may indicate manipulation

**Bibliography**

[1] R. Brunelli. Estimation of pose and illuminant direction for face processing. Image and Vision Computing, 15(10):741–748, 1997.

[2] W. Chojnacki and M. J. Brooks. Revisiting Pentland’s estimator of light source direction. Journal of the Optical Society of America, 11(1):118–124, 1994.

[3] J. D. Foley, A. van Dam, S. K. Feiner, and J. F. Hughes. Computer Graphics: Principles and Practice. Addison-Wesley Publishing Company, Inc., 2nd edition, 1993.

[4] J. Fridrich, D. Soukal, and J. Luk´aˇs. Detection of copy-move forgery in digital images. In Proceedings of DFRWS, 2003.

[5] J. Luk´aˇs, J. Fridrich, and M. Goljan. Determining digital image origin using sensor imperfections. In Proceedings of the SPIE, volume 5685, pages 249–260, 2005.

[6] P. Nillius and J.-O. Eklundh. Automatic estimation of the projected light source direction. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001.

[7] Y. Ostrovsky, P. Cavanagh, and P. Sinha. Perceiving illumination inconsistencies in scenes. Technical Report AI Memo 2001-029, Massachusetts Institute of Technology, 2001.

[8] A. Pentland. Finding the illuminant direction. Journal of the Optical Society of America, 72(4):448–455, 1982.

[9] J.-M. Pinel, H. Nicolas, and C. L. Bris. Estimation of 2D illuminant direction and shadow segmentation in natural video sequences. In Proceedings of VLBV, pages 197–202, 2001.

[10] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on Signal Processing, 53(2):758–767, 2005.

[11] A. C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, (in press), 2005.

[12] J. R. Shewchuck. An introduction to the conjugate gradient method without the agonizing pain. Technical Report CMU-CS-94-125, Carnegie Mellon University, 1994.

[13] P. Sinha. Perceiving illumination inconsistencies. In Investigative Ophthalmology

**17.** **Literature Review: Exposing Digital Forgeries Through Chromatic Aberration**

This research explores a method to detect digital tampering by analyzing chromatic aberration, a type of optical distortion that causes different colors of light to focus at slightly different points. Method for automatically estimating lateral chromatic aberration and show its efficacy in detecting digital tampering in synthetic and real images.

**Methodology**

The authors propose a technique that estimates lateral chromatic aberration by analyzing the intensity and surface normal along an occluding boundary. The technique assumes that the surface is Lambertian, has a constant reflectance value, and is illuminated by a point light source infinitely far away.

**Key Contributions**

1. The authors developed a mathematical model to describe how chromatic aberration affects images.
2. They created a method to estimate the amount of chromatic aberration present in an image. Using a brute-force iterative search that maximizes the mutual information between color channels.
3. By identifying inconsistencies in chromatic aberration, the technique can detect signs of tampering. Inconsistencies in lateral chromatic aberration can be used to detect tampering in visually plausible forgeries.

**Conclusion**

This research offers a valuable tool for forensic analysis. By examining chromatic aberration, it can help identify images that may have been digitally altered. This has implications for fields like law enforcement, journalism, and digital media verification. The technique is shown to be effective in various scenarios, including synthetic and real images. There was also discussion about future work, including incorporating longitudinal chromatic aberrations and other forms of optical distortions.

**Bibliography**

[1] T. E. Boult and G. Wolberg. Correcting chromatic aberrations using image warping. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 684–687, 1992.

[2] H. Farid and E. Simoncelli. Differentiation of multi-dimensional signals. IEEE Transactions on Image Processing, 13(4):496–508, 2004.

[3] J. Fridrich, D. Soukal, and J. Luk´aˇs. Detection of copy-move forgery in digital images. In Proceedings of DFRWS, 2003.

[4] E. Hecht. Optics. Addison-Wesley Publishing Company, Inc., 4th edition, 2002.

[5] M. K. Johnson and H. Farid. Exposing digital forgeries by detecting inconsistencies in lighting. In ACM Multimedia and Security Workshop, New York, NY, 2005.

[6] J. Luk´aˇs, J. Fridrich, and M. Goljan. Detecting digital image forgeries using sensor pattern noise. In Proceedings of the SPIE, volume 6072, 2006.

[7] T. Ng and S. Chang. A model for image splicing. In IEEE International Conference on Image Processing, Singapore, 2004.

[8] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[9] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on Signal Processing, 53(2):758–767, 2005.

[10] A. C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, 53(10):3948–3959, 2005.

[11] P. Viola and W. M. Wells, III. Alignment by maximization of mutual information. International Journal of Computer Vision, 24(2):137–154, 1997.

[12] R. G. Willson and S. A. Shafer. What is the center of the image? Journal of the Optical Society of America A, 11(11):2946–2955, November 1994.

18. **Literature Review: Noiseprint: A CNN-Based Camera Model Fingerprint**

This research explores a method to identify the camera used to take a photo. This information can be valuable in forensic investigations, especially when determining if images have been tampered with. They also propose a deep learning method based on a Siamese network, which is trained with pairs of image patches coming from the same or different cameras.

**Background**

Digital image forensics has become increasingly important in recent years, with the rise of social media and the ease of image transforming software. Image forgery detection is gone to be critical tasks in this field, and various methods have been proposed to address these challenges.

**Methodology**

The authors propose a technique that estimates the noiseprint of an image by analyzing the intensity and surface normal along an occluding boundary. The technique assumes that the surface is Lambertian and has a constant reflectance value, and is illuminated by a point light source infinitely far away.

**Key Contributions**

1. A technique to extract a unique identifier, called a "noiseprint," from an image. This identifier is specific to the camera used to take the photo.
2. The authors use a Siamese network to train the noiseprint extractor, which is a deep learning architecture that is well-suited for this task.
3. The noiseprints can be used to identify forged regions in images, where parts from different photos have been combined.

**Conclusion**

This research offers a valuable tool for forensic analysis. By identifying the camera used to take a photo, it can help determine the image's origin and detect potential tampering. This has implications for law enforcement, journalism, and other fields where image authenticity is important. They also demonstrate the effectiveness of the noiseprint-based method and highlight its potential for future research in digital image forensics.

**Bibliography**

[1] H. Farid, Photo Forensics. Cambridge, MA, USA: MIT Press, 2016.

[2] A. Piva, “An overview on image forensics,” ISRN Signal Process., vol. 2013, Nov. 2012, Art. no. 496701.

[3] M. K. Johnson and H. Farid, “Exposing digital forgeries in complex lighting environments,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 450–461, Sep. 2007.

[4] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. Rocha, “Exposing digital image forgeries by illumination color classification,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1182–1194, Jul. 2013.

[5] M. K. Johnson and H. Farid, “Exposing digital forgeries through chromatic aberration,” in Proc. 8th Workshop Multimedia Secur., Sep. 2006, pp. 48–55.

[6] I. Yerushalmy and H. Hel-Or, “Digital image forgery detection based on lens and sensor aberration,” Int. J. Comput. Vis., vol. 92, no. 1, pp. 71–91, 2011.

[7] O. Mayer and M. C. Stamm, “Accurate and efficient image forgery detection using lateral chromatic aberration,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 7, pp. 1762–1777, Jul. 2018.

[8] Z. Lin, R. Wang, X. Tang, and H.-Y. Shum, “Detecting doctored images using camera response normality and consistency,” in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jun. 2005, pp. 1087–1092.

[9] Y.-F. Hsu and S.-F. Chang, “Detecting image splicing using geometry invariants and camera characteristics consistency,” in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2006, pp. 549–552.

[10] C. Chen, S. McCloskey, and J. Yu, “Image splicing detection via camera response function analysis,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jul. 2017, pp. 1876–1885.

[11] A. C. Popescu and H. Farid, “Exposing digital forgeries in color filter array interpolated images,” IEEE Trans. Signal Process., vol. 53, no.

19. **Literature Review: Unsupervised Multi-Modal Tampering Localization**

This research focuses on identifying tampered areas in digital images. The authors propose a method that combines the results from multiple forgery detection techniques to improve accuracy. The article also discusses the problem of unsupervised multi-modal tampering localization in digital image forensics.

**Background**

Digital image forensics is a critical area of research, and tampering localization is a key task in this field. Various methods have been proposed to address this challenge, but most of them rely on pixel-wise combination of the input tampering maps, which is suboptimal.

**Methodology**

The authors propose a CRF-based method that model’s dependencies between neighboring pixels and exploits the content of the tampered image. The method uses a content-dependent interaction potential to encourage nearby similar pixels to assume the same label.

**Key Contributions**

1. The method uses a conditional random field (CRF) model to combine the outputs of different detection techniques, considering the relationships between neighboring pixels. The method models the dependencies between neighboring pixels and exploits the content of the tampered image.
2. The CRF model takes into account the content of the image, focusing on areas with similar characteristics.
3. The approach effectively identifies the boundaries of tampered regions and can detect subtle manipulations.

**Conclusion**

This research offers a valuable tool for forensic analysis. By combining multiple detection techniques and considering image content, it can more accurately pinpoint tampered areas in digital images. The method is effective in tampering localization and can accurately delineate the shape of the forgery.

**Bibliography**

[1] M. Fontani et al., "A framework for decision fusion in image forensics based on Dempster-Shafer theory of evidence," IEEE Trans. Inf. Forensics Security, vol. 8, no. 4, 2013.

[2] M. Barni and A. Costanzo, "Dealing with uncertainty in image forensics: a fuzzy approach," in Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing, 2012.

[3] L. Gaborini et al., "Multi-clue image tampering localization," in Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2014.

[4] D. Cozzolino et al., "Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques," in Proc. of IEEE Int. Conf. on Image Processing, 2014.

[5] D. Cozzolino et al., "Multiple classifier systems for image forgery detection," in Image Analysis and Processing, vol. 8157 of LNCS. 2013.

[6] P. Ferrara et al., "Unsupervised fusion for forgery localization exploiting background information," in Proc. of IEEE Int. Conf. on Multimedia & Expo Workshops, 2015.

[7] P. Ferrara et al., "Image forgery localization via fine-grained analysis of cfa artifacts.," IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, 2012.

[8] M. Chen et al., "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, 2008.

[9] M. Barni et al., "Identification of cut & paste tampering by means of double-jpeg detection and image segmentation," in Proc. of IEEE Int. Symposium on Circuits and Systems, 2010.

[10] G. Chierchia et al., "PRNU-based detection of small-size image forgeries," in Proc. of Int. Conf. on Digital Signal Processing, 2011.

[11] G. Chierchia et al., "Guided filtering for PRNU-based localization of small-size image forgeries," in Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing, 2014.

[12] M.-M. Cheng et al., "DenseCut: Densely connected CRFs for real-time GrabCut," Computer Graphics Forum, vol. 34, no. 7, 2015.

[13] P. Korus and J. Huang, "Multi-scale analysis strategies in PRNU-based tampering localization," IEEE Trans. Inf. Forensics Security, To appear.

[14] S. Z. Li, Markov Random Field Modeling in Image Analysis, Springer-Verlang, 2001.

[15] G.

20. **Literature Review: ImageNet Classification with Deep Convolutional Neural Networks**

This research explores the use of deep convolutional neural networks (CNNs) for image classification. The goal is to accurately categorize images into different categories. The authors propose a novel architecture that uses a combination of techniques such as rectified linear units (ReLUs), local response normalization, and dropout to improve the performance of the network.

The ImageNet dataset is a large-scale image classification dataset that consists of over 15 million labeled high-resolution images in over 22,000 categories. The ILSVRC competition is a benchmark for evaluating the performance of image classification algorithms on this dataset.

**Methodology**

The authors propose a deep CNN architecture that consists of five convolutional layers and three fully connected layers. The network layer uses ReLUs as the activation function, which are faster to train than traditional nonlinearities. The authors also use local response normalization to normalize the responses of the neurons in each layer.

**Key Contributions**

1. The authors designed a new CNN architecture that incorporates techniques like rectified linear units (ReLUs) and local response normalization. The authors propose the use of ReLUs as a activation function, which are faster to train than traditional saturating nonlinearities.
2. The use of dropout to prevent overfitting in the fully connected layers.
3. The use of data augmentation to artificially enlarge the dataset and reduce overfitting.

The network achieved excellent results on the ImageNet dataset, a benchmark for image classification.

**Conclusion**

This research demonstrates the power of deep CNNs for image classification tasks. The techniques developed in this study have been influential and have contributed to advancements in computer vision.

**Bibliography**

[1] Bell, R., Koren, Y. Lessons from the Netflix prize challenge. ACM SIGKDD Explor. Newsl. 9, 2 (2007), 75–79.

[2] Berg, A., Deng, J., Fei-Fei, L. Large scale visual recognition challenge 2010. www.image-net.org/challenges. 2010.

[3] Breiman, L. Random forests. Mach. Learn. 45, 1 (2001), 5–32.

[4] Cires¸an, D., Meier, U., Masci, J., Gambardella, L., Schmidhuber, J. High-performance neural networks for visual object classification. Arxiv preprint arXiv:1102.0183, 2011.

[5] Cires¸an, D., Meier, U., Schmidhuber, J. Multi-column deep neural networks for image classification. Arxiv preprint arXiv:1202.2745, 2012.

[6] Deng, J., Berg, A., Satheesh, S., Su, H., Khosla, A., Fei-Fei, L. In ILSVRC-2012 (2012).

[7] Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., Fei-Fei, L. ImageNet: A large-scale hierarchical image database. In CVPR09 (2009).

[8] Fei-Fei, L., Fergus, R., Perona, P. Learning generative visual models from few training examples: An incremental Bayesian approach tested on 101 object categories. Comput. Vision Image Understanding 106, 1 (2007), 59–70.

[9] Fukushima, K. Neocognitron: A self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position. Biol. Cybern. 36, 4 (1980), 193–202.

[10] Griffin, G., Holub, A., Perona, P. Caltech-256 object category dataset. Technical Report 7694, California Institute of Technology, 2007.

[11] He, K., Zhang, X., Ren, S., Sun, J

**21.** **Literature Review: Can People Detect Photo Forgeries?**

This research explores whether people can effectively identify manipulated photos. With the increasing sophistication of image editing tools, it's important to understand the public's ability to detect fakes. They conducted two experiments to investigate people's ability to detect and locate manipulations in real world photos.

The creation of visually compelling photographic fakes is growing at an incredible speed, and the prevalence of manipulated photos in everyday life invites an important question: Can people detect photo forgeries? With the rise of digital technology, even amateurs can use sophisticated image editing software to create detailed and compelling fake images.

**Key Findings**

1. People struggle to accurately identify manipulated photos, even when the changes are significant.
2. Even when they correctly identify a photo as fake, people often have trouble pinpointing the exact location of the manipulation as many people are unaware from the latest image editing software’s and AI creations.
3. The more the manipulation disrupts the underlying structure of the image, the more likely people are to detect it.

**Experiment**

They conduct a small experiment among people to detect the manipulated images. The results showed that people have a limited ability to detect and locate manipulations in real world photos. The participants correctly classified 66% of the photos as original or manipulated, and they were able to locate the manipulation in 45% of the manipulated photos.

**Conclusion**

This research suggests that people are not well equipped to spot fake photos, and even when they correctly detect a manipulation, they often fail to locate it. This has implications for various fields, highlighting the need for guidelines and regulations regarding the use of images to ensure authenticity and prevent the spread of misinformation.

**Bibliography**

Amsler, M. (1953). Earliest symptoms of diseases of the macula. British Journal of Ophthalmology, 37, 521-537.

Barlow, H. B. (1961). Possible principles underlying the transformation of sensory messages. In W. A. Rosenblith (Ed.), Sensory communication (pp. 217-234). Cambridge, MA: MIT Press.

Bex, P. J. (2010). (In) sensitivity to spatial distortion in natural scenes. Journal of Vision, 10, 1-15. doi:10.1167/10.2.23.

Bex, P. J., Solomon, S. G., & Dakin, S. C. (2009). Contrast sensitivity in natural scenes depends on edge as well as spatial frequency structure. Journal of Vision, 9, 1-19. doi:10.1167/9.10.1.

Bonfiglioli, C., Pavani, F., & Castiello, U. (2004). Differential effects of cast shadows on perception and action. Perception, 33, 1291-1304. doi:10.1068/p5325.

Bouwens, M. D., & Meurs, J. C. (2003). Sine Amsler Charts: A new method for the follow-up of metamorphopsia in patients undergoing macular pucker surgery. Graefes Archive for Clinical and Experimental Ophthalmology, 241, 89-93. doi:10.1007/s00417-002-0613-5.

Braun, K. A., Ellis, R., & Loftus, E. F. (2002). Make my memory: How advertising can change our memories of the past. Psychology and Marketing, 19, 1-23. doi:10.1002/mar.1000.

Cavanagh, P. (2005). The artist as neuroscientist. Nature, 434, 301-307. doi:10.1038/434301a.

Craik, K. (1943). The nature of exploration. Cambridge, England: Cambridge University Press.

Cumming, G. (2012). Understanding the new statistics: Effect sizes, confidence intervals, and meta-analysis. New York: Routledge.

Ehinger, K. A., Allen, K., & Wolfe, J. M. (2016). Change blindness for cast shadows in natural scenes: Even informative shadow changes are missed. Attention, Perception, & Psychophysics, 78, 978-987. doi:10.3758/s13414-015-1054-7.

Farid, H. (2006). Digital doctoring: how to tell the real from the fake. Significance, 3, 162-166. doi:10.1111/j.1740-9713.2006.00197.x.

Farid, H. (2009). Image forgery