IMPROVED FORGERY DETECTION WITH LATERAL CHROMATIC ABERRATION

Owen Mayer and Matthew Stamm

Department of Electrical and Computer Engineering
Drexel University, Philadelphia, PA 19103

ABSTRACT

In this paper we propose a technique to improve the accuracy of lateral chromatic aberration (LCA) based detection of copy-paste image forgeries. We propose a statistical model of the error between local estimates of LCA displacement vectors and those predicted by a global model. Using this statistical model, we formulate forgery detection as a hypothesis testing problem, and derive the optimal detection statistic for performing LCA-based forgery detection. Through a series of experiments, we demonstrate that our proposed technique outperforms existing approaches for conducting LCA-based forgery detection.

Index Terms— Digital Forensics, Copy Paste Forgery Detection, Lateral Chromatic Aberration

1. INTRODUCTION

Many facets of human society, such as courts of law and news agencies, rely upon authentic information and increasingly so upon authentic digital images. With the growing ability of digital image forgeries to deceive human perception, computational methods to determine if an image has been altered are becoming important. As a result, researchers have developed a variety of multimedia forensic techniques [1].

Two types of forgeries which are particularly important to detect are copy-paste forgeries, where image content is cut from one image and pasted into another, and copy-move forgeries, where image content is pasted to another location within the same image. Previous research has developed techniques to detect copy-paste forgeries by finding localized evidence of manipulation, such as traces of resampling [2, 3], JPEG compression [4–6], contrast enhancement [7], and sensor noise [8]. Techniques to detect copy-move forgeries have also been developed, which work by finding duplicate image blocks [9, 10], and by matching SIFT features [11, 12].

Johnson and Farid introduced the idea of using lateral chromatic aberration (LCA) as a feature of digital images to expose both copy-paste and copy-move forgeries [13]. LCA is a phenomenon of optical imaging systems that arises from a lens's inability to focus all wavelengths of light to a common focal point. The effect of LCA can be described by a vector of displacement between the focus locations of two color components of light that share a common source. Various techniques have been developed to measure and characterize the effects of LCA in digital images [13–15]. Johnson and Farid's proposed detection method works by searching for inconsistency in the angles of LCA displacement vectors, which is evident in forged images. Other work has shown that LCA can be used to detect forgeries in digital images [16], as well as for camera model identification [17]. Additionally, research has shown that artificial LCA can be induced in an image to avoid forgery detection [18].

While the heuristic forgery detection method proposed by Johnson and Farid has been shown capable of detecting image forgeries [13], it has several shortcomings. First, in a scenario where image content is copy-moved radially outwards from the image optical center, LCA displacement in the forged region will be inconsistent in magnitude only, but not angle. Such a scenario will not be detected by an angle based detection metric. Second, angle-based metrics can not be determined in forged regions cut from or near an image optical center. As a result, no decision can be rendered by an angle-based detector. This is because measurements of LCA displacement near the optical center have zero-magnitude, and thus an undefined angle.

In this paper, we propose a new LCA-based forgery detection technique to address the above shortcomings. To accomplish this, we first develop a new stochastic model that describes inconsistency between local observations and global predictions of LCA in both forged and unaltered images. Using this model, we frame forgery detection as a hypothesis test from which we derive the optimal decision metric. We perform a series of experiments to test the efficacy of this proposed decision metric, and compare to the method suggested by Johnson and Farid. The results of these experiments demonstrate that our proposed metric addresses the shortcomings outlined above, and outperforms existing techniques in all tested scenarios.

2. BACKGROUND

As light passes through a lens, it is focused onto a camera's optical sensor through refraction. The refractive index of glass, however, is dependent upon the wavelength of the incident light. This causes different color components of light originating from the same source to be focused onto different locations on the sensor. A diagram of this phenomenon, known as lateral chromatic aberration (LCA), is shown in Fig. 1.

The effects of LCA are characterized by the mapping of a point $\mathbf{r} = (r_x, r_y)^\mathsf{T}$ in a reference color channel of an image to the location of the corresponding point $\mathbf{c} = (c_x, c_y)^\mathsf{T}$ in a comparison color channel. Johnson and Farid proposed the following parametric model of this mapping

$$\mathbf{c} = \alpha(\mathbf{r} - \boldsymbol{\zeta}) + \boldsymbol{\zeta} \tag{1}$$

where α is a first order expansion coefficient, and $\boldsymbol{\zeta} = (\zeta_x, \zeta_y)^\mathsf{T}$ is the location of the image's optical center. While others have shown higher order LCA models to be useful [15], we have found a first order model to be sufficient for forgery detection.

The effect of LCA at location $\mathbf{r}$ is also described by a displacement vector $\mathbf{d}$. The LCA displacement vector is defined as the difference between $\mathbf{r}$ and $\mathbf{c}$, i.e. $\mathbf{d} = \mathbf{c} - \mathbf{r}$. By using the model (1) to determine $\mathbf{c}$, the LCA displacement vector is given by the equation

$$\mathbf{d} = \mathbf{c} - \mathbf{r} = \alpha(\mathbf{r} - \boldsymbol{\zeta}) + \boldsymbol{\zeta} - \mathbf{r}. \tag{2}$$

An example of an image's LCA displacement vector field is shown in the left of Fig. 2. For the model (1), LCA displacements point radially outward (inward) from the optical center for expansion coefficients greater (less) than 1.

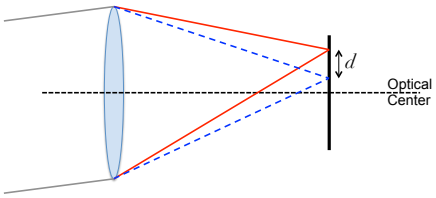

Fig. 1. Lateral chromatic aberration (LCA). The symbol d denotes LCA displacement.

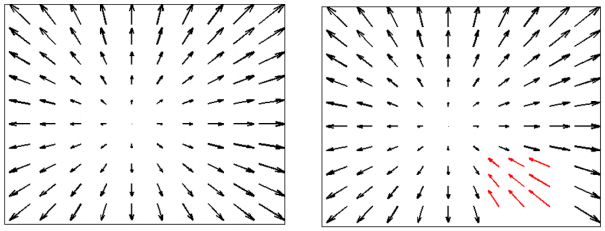

Fig. 2. **Left:** Lateral chromatic aberration (LCA) displacement vector field for an authentic image. **Right:** LCA displacement vector field for a copy-paste forgery, with pasted LCA in red. Displacement vectors are scaled 200X.

2.1. Lateral Chromatic Aberration Estimation

In practice, the LCA model parameters α and $\boldsymbol{\zeta}$ are typically unknown and must be estimated. Gloe et al. provide a technique to estimate the model parameters [14]. Their method operates by obtaining *local* estimates of the LCA displacement vector $\hat{\mathbf{d}}$ at several corner points located throughout an image. The *global* LCA model parameters are then identified by performing a least-squares fit of the estimated displacement vectors to the model (2) using an iterative Gauss-Newton method. Local estimates of the LCA displacement vector $\hat{\mathbf{d}}$ are obtained by searching for a $W \times W$ block $\mathbf{C}$ in the comparison channel that maximizes similarity with an equivalently sized block $\mathbf{R}$ in the reference channel, such that

$$\hat{\mathbf{d}} = \underset{(m,n)\in\{-\Delta,\ldots,\Delta\}}{\arg\max} S(\mathbf{R}(x,y), \mathbf{C}(x+m, y+n)) \qquad (3)$$

where the similarity $S(\cdot)$ is measured using the correlation coefficient, and (x, y) denote the horizontal and vertical location of a corner point, about which the blocks are centered. To enable a search over fractional pixel displacements, both blocks are upsampled by a factor of u. This search is performed exhaustively over a set of displacements (m, n) between $-\Delta$ and Δ.

2.2. Forgery Detection

In a copy-paste forgery, a forger moves image content from one location to another. Often, the local LCA of the copied region does not resemble the LCA original to the paste location. This causes a mismatch between the local LCA in the forged region and the global LCA model of the image. When looking at the LCA displacement field of a copy-paste forgery, the falsified region becomes readily apparent as shown on the right side of Fig. 2.

Johnson and Farid proposed using the absolute angular difference between a LCA displacement determined locally to a displacement determined by the global model (2) as a forgery detection feature [13]. This angular difference is averaged over observations in a region and compared to a threshold, where local observations that result in a mean angular error greater than a threshold are considered to be from a falsified region.

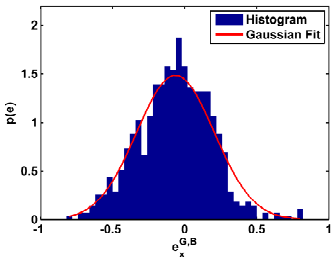

Fig. 3. Histogram of and Gaussian fit of n_x from 700 test points of an unaltered image taken by a Sony Cybershot DSCV1.

3. ERROR MODEL

While the use of an angular-difference metric between local and global LCA displacement has been shown capable of detecting image forgeries, we find this metric deficient in two regards. First, an angular-difference metric is unable to resolve magnitude differences between local and global LCA displacements. This limitation is highlighted in copy-move scenarios when image content is moved radially outward from the optical center; local displacement observations will differ from global in magnitude but not angle. Second, an angular-difference metric is not measurable in regions copied from near the image optical center. Since the LCA effect is small near the optical center, local displacement observations in that region will have no magnitude and thus no measurable angle.

To address the above concerns, we propose a new detection metric that is able to resolve magnitude differences and is measurable when local displacements are small. This metric is derived from a noise model that captures a scaled, Cartesian discrepancy between local and global LCA displacements.

Local estimates of LCA displacement $\hat{\mathbf{d}}$ are viewed as noisy observations of those determined by a global model $\mathbf{d}$. We model observational noise $\mathbf{n} = (n_x, n_y)^\mathsf{T}$ as an additive term upon a reference location in (1):

$$\hat{\mathbf{d}} = \alpha(\mathbf{r} + \mathbf{n} - \boldsymbol{\zeta}) + \boldsymbol{\zeta} - \mathbf{r} \qquad (4)$$

The noise term $\mathbf{n}$ captures the disagreement between local observations of LCA displacement and those predicted by the global model. Fig. 3 shows a histogram of the horizontal component of $\mathbf{n}$ in a single image. We model $\mathbf{n}$ as independent and identically distributed Gaussian.

In a forged region of an image, local observations will contain a constant offset in addition to observational noise. This offset is modeled as an additive term about a reference location in (1):

$$\hat{\mathbf{d}} = \alpha(\mathbf{r} + \mathbf{n} + \boldsymbol{\delta} - \boldsymbol{\zeta}) + \boldsymbol{\zeta} - \mathbf{r} \qquad (5)$$

The offset term $\boldsymbol{\delta} = (\delta_x, \delta_y)^\mathsf{T}$ is called the *forgery offset*, which is a result of the mismatch between LCA in the original and forged regions.

We define an error term that captures observational noise in an authentic region, as well as the forgery bias in a forged image region. This error term is called *model discrepancy*. We define model discrepancy $\mathbf{e} = (e_x, e_y)^\mathsf{T}$ as:

$$\mathbf{e} \triangleq \alpha^{-1}(\hat{\mathbf{d}} - \mathbf{d}) \qquad (6)$$

Solving for $\mathbf{e}$ in an authentic image region yields

$$\begin{aligned}\mathbf{e} &= \alpha^{-1}\left((\alpha(\mathbf{r} + \mathbf{n} - \boldsymbol{\zeta}) + \boldsymbol{\zeta}) - (\alpha(\mathbf{r} - \boldsymbol{\zeta}) + \boldsymbol{\zeta})\right) \\ &= \mathbf{n} \end{aligned} \qquad (7)$$

and in a forged region

$$\begin{aligned}\mathbf{e} &= \alpha^{-1}\left((\alpha(\mathbf{r}+\mathbf{n}+\boldsymbol{\delta}-\boldsymbol{\zeta})+\boldsymbol{\zeta})-(\alpha(\mathbf{r}-\boldsymbol{\zeta})+\boldsymbol{\zeta})\right)\\ &= \mathbf{n}+\boldsymbol{\delta}\end{aligned} \tag{8}$$

Observe that the model discrepancy (6) describes inconsistency in local and global displacement, much like angular error from Sec. 2.2. Unlike the angular error metric, this form is practical when the local displacement has a small magnitude. Additionally, the error model is able to discern differences between the magnitudes of local and global displacement.

4. FORGERY DETECTION

From (7) and (8), we formulate a hypothesis test to differentiate between authentic and forged image regions. For a particular region of interest within an image, we define H_0 as the hypothesis that the image region is unaltered and H_1 as the hypothesis that the region has been falsified through copy-paste forgery.

$$\begin{aligned} H_0 &: \quad \mathbf{e} \sim \mathcal{N}(\boldsymbol{\mu}_0, \boldsymbol{\Sigma}) \\ H_1 &: \quad \mathbf{e} \sim \mathcal{N}(\boldsymbol{\mu}_0 + \boldsymbol{\delta}, \boldsymbol{\Sigma}) \end{aligned} \tag{9}$$

Here $\boldsymbol{\mu}_0$ and $\boldsymbol{\Sigma}$ are the mean and covariance of observational noise in the image. The following equation specifies the probability density of a sequence $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_N\}$ of N independent and identically distributed observations of m dimensional model discrepancy.

$$\begin{aligned} &p(\mathbf{e}_1, \ldots, \mathbf{e}_N | \boldsymbol{\mu}, \boldsymbol{\Sigma}) \\ &\quad = \frac{|\boldsymbol{\Sigma}|^{-N/2}}{2\pi^{Nm/2}} \exp\left\{-\frac{1}{2}\sum_{i=1}^{N}(\mathbf{e}_i - \boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1}(\mathbf{e}_i - \boldsymbol{\mu})\right\} \end{aligned} \tag{10}$$

From the hypotheses in (9) and density in (10), we construct a log-likelihood ratio test to determine whether a sequence of error observations is inauthentic.

$$\begin{aligned} &\log\left(\frac{p(\mathbf{e}_1, \ldots, \mathbf{e}_N | \boldsymbol{\mu}_0 + \boldsymbol{\delta}, \boldsymbol{\Sigma})}{p(\mathbf{e}_1, \ldots, \mathbf{e}_N | \boldsymbol{\mu}_0, \boldsymbol{\Sigma})}\right) \\ &\quad = -\frac{1}{2}\sum_{i=1}^{N}(\mathbf{e}_i - \boldsymbol{\mu}_0 - \boldsymbol{\delta})^{\mathsf{T}} \boldsymbol{\Sigma}^{-1}(\mathbf{e}_i - \boldsymbol{\mu}_0 - \boldsymbol{\delta}) \\ &\qquad + \frac{1}{2}\sum_{i=1}^{N}(\mathbf{e}_i - \boldsymbol{\mu}_0)^{\mathsf{T}} \boldsymbol{\Sigma}^{-1}(\mathbf{e}_i - \boldsymbol{\mu}_0) \end{aligned} \tag{11}$$

Observe that the terms within the summations on the second and third lines of (11) are Euclidean-squared distances of $\mathbf{e}_i$ to $\boldsymbol{\mu}_0 + \boldsymbol{\delta}$ and $\boldsymbol{\mu}_0$, respectively, projected onto the error-space defined by $\boldsymbol{\Sigma}^{-1}$. Thus, the likelihood ratio test can be thought of as comparing the aggregate distances of error observations to the two distribution means.

Further algebraic reduction of (11) yields a simplified form of the optimal detector:

$$(\bar{\mathbf{e}} - \boldsymbol{\mu}_0)^{\mathsf{T}} \boldsymbol{\Sigma}^{-1} \boldsymbol{\delta} \underset{H_1}{\overset{H_0}{\lessgtr}} \tau \tag{12}$$

where $\bar{\mathbf{e}}$ is the sample average of $\mathbf{e}_i$, and τ is a decision threshold.

In most practical forensic scenarios the forgery offset $\boldsymbol{\delta}$ is unknown, since information regarding the source forgery content is not available. In these scenarios the optimal decision feature (12) cannot be computed explicitly. Instead, we form a maximum-likelihood estimate of the forgery offset $\hat{\boldsymbol{\delta}}$. Since error in a forged region is distributed Gaussian with mean $\boldsymbol{\mu}_0 + \boldsymbol{\delta}$, the forgery offset is estimated by

$$\hat{\boldsymbol{\delta}} = \frac{1}{N}\sum_{i=1}^{N}\mathbf{e}_i - \boldsymbol{\mu}_0 = \bar{\mathbf{e}} - \boldsymbol{\mu}_0 \tag{13}$$

Substituting $\hat{\boldsymbol{\delta}}$ for $\boldsymbol{\delta}$ in (12) yields:

$$(\bar{\mathbf{e}} - \boldsymbol{\mu}_0)^{\mathsf{T}} \boldsymbol{\Sigma}^{-1} (\bar{\mathbf{e}} - \boldsymbol{\mu}_0) \underset{H_1}{\overset{H_0}{\lessgtr}} \tau \tag{14}$$

Since $\boldsymbol{\Sigma}$ and $\boldsymbol{\mu}_0$ are often unknown apriori, they must also be estimated. We follow the convention set by Johnson and Farid, and assume the forgery be sufficiently small such that it does not introduce bias to global estimates [13]. Thus we estimate $\boldsymbol{\Sigma}$ and $\boldsymbol{\mu}_0$ from all model discrepancy observations within an image.

5. EXPERIMENTAL RESULTS

We conducted three experiments to test the efficacy of the proposed detection technique. Test forgery images were created by splicing a 512x512 block of image content from one image and inserting into another. For the cameras whose abbreviated names are listed in Table 1, a 512x512 block is 1.7%, 2.2% and 3.3% of a CPS, SAN and CER image, respectively.

Local LCA measurements were obtained at corner points identified using the Harris corner point detector [20]. We used the green channel as a reference channel with red and blue as comparison channels, forming four dimensional displacement vectors. For local LCA estimation we used an upsample factor of $u = 5$, maximum displacement of $\Delta = 3$, and window size of $W = 64$ (see Sec. 2.1).

The detection metric (14) was then calculated in regions of interest in forged and authentic images. We defined a region of interest in each forged image to be the location of the pasted block. In an authentic image we defined multiple regions of interest the same size as the forgery block, which span the image with 50% overlap. This methodology was adopted to test the ability of the detection metric to distinguish between a completely forged image block and unaltered image blocks.

The average angular error was also calculated in each region of interest. For both detection metrics, we required $N \geq 10$ corner points in the region of interest in order to make a decision. This ensures that homogenous regions (i.e. sky) are not included, as they are generally not suitable for this method of forgery detection.

5.1. Copy-Paste Forgery Detection

In our first experiment, we cut image content from one image, which we refer to as the source image, and pasted it into a different image called the destination image. We chose one of the three camera models listed in Table 1 as a source camera model and another as the destination camera model. To make a forged image, we chose a source image uniformly at random among the authentic images belonging to the source camera model, and a destination image uniformly at random from those images belonging to the destination camera model. A 512x512 block was then cut from the source image and pasted into the destination image, with the cut and paste locations both chosen uniformly at random. In all, 9 test groups were formed from the possible permutations of source and destination models, with 1000 forged images in each.

Fig. 4 shows the receiver operating characteristics (ROC) of the proposed and angular-error detectors for the 9 test groups. We see from these ROC curves that the proposed detector method outperforms the angular error method. While the ROC curves appear comparable in the case when the destination image is from the CPS camera, at low false alarm rates there is noticeable disparity between detection methods, as highlighted in Table 2.

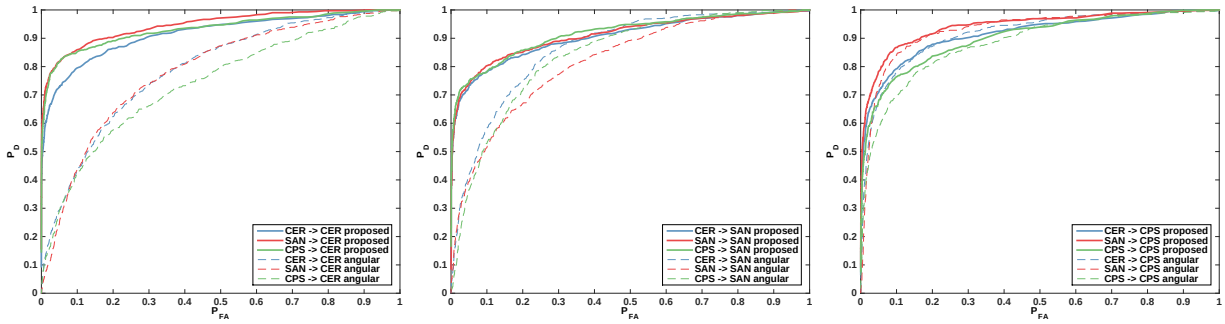

Fig. 4. From left to right are the receiver operating characteristic for forgery detection with CER, SAN and CPS cameras as the destination image. For each source camera two line-plots are shown; solid for the proposed detection ROC, and dashed for the angular-error ROC.

Table 1. Camera models used in experimental results

Camera model (ID)	Image size	No. images
Canon EOS Rebel T3i (CER)	3456x2304	199
Sony Alpha NEX5 (SAN)	4592x2576	239
Canon Powershot SX500IS (CPS)	4608x3456	206

Table 2. Differences in detection rates between proposed method and angular error method at $P_{FA} = 0.01$

		Destination		
		CER	**SAN**	**CPS**
Source	**CER**	0.41	0.31	0.21
	SAN	0.61	0.27	0.44
	CPS	0.51	0.45	0.20

Table 2 shows the difference in detection rates between the proposed and angular-difference metrics at a 1% false alarm rate. In all cases, our proposed detection method outperforms the angular-error metric (i.e. has a positive difference). At minimum, our proposed detector improves the positive detection rate by 20 percentage points in the CPS to CPS case. The proposed detector achieves highest benefit in the SAN to CER case, improving the positive detection rate by 61 percentage points.

5.2. Radial Forgery Experiment

In this experiment, we started with 199 unaltered images from CER. In each authentic image, 9 copy blocks are defined at a distance of 800 pixels from the image optical center. The first block is defined 800 pixels to the right of the optical center. Subsequent blocks are defined at increments of 22.5 degrees, clockwise, so that the 9th block is defined at 800 pixels to the left of the optical center. Each copy block is then moved 600 pixels inwards along the radius between the optical center and the copy block. After filtering out forgeries with less than 10 corner points in the copy region, 189 forgeries were created and used for analysis of detection performance.

Fig. 5 shows that the receiver operating characteristic for the proposed detection feature and angular error method. We observe that the angular error decision rule achieves little better than random chance in this scenario. At a false alarm rate of 0.05, the proposed technique achieves a positive detection rate of 30 percent, whereas the angular error method has 8 percent positive detection rate.

5.3. Undetectable Copy Area

It is important to note that in order for the angular error detection method to render a decision, it must have local estimates $\hat{\mathbf{d}}$ with non-zero magnitude. However, part of the image near the optical center will not have an inherent LCA displacement large enough to affect a non-zero estimate of $\hat{\mathbf{d}}$. Thus an image block copied from near the image optical center will fail to be detected in a forgery with the angular error method.

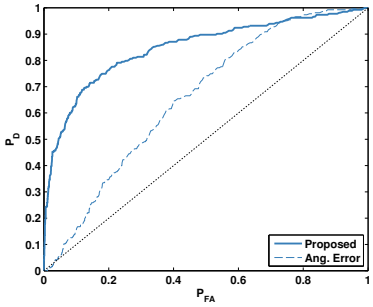

Fig. 5. The receiver operating characteristic for detection of copy-move forgeries created radially using images from the CER camera.

In order to estimate the area of the image where our proposed detector can be used but an angular-difference detector cannot, we conducted the following experiment. We started with an unaltered image database described in Table 1. We then divided the images into 3000 non-overlapping square blocks, and determined the strongest corner point in each box. Boxes lacking a sufficient corner point were discounted from this test. Local LCA displacements were estimated at each corner point with green as the reference channel, red and blue as the comparison channels, and upsample factor $u = 5$. The number of blocks where both green-to-red and green-to-blue local LCA displacement estimates were of zero magnitude were counted over all images of one camera model. This number was divided by the total number of blocks over all images of that camera model. This ratio represents the percentage of the image area that has insufficient LCA displacement magnitude to affect a non-zero local LCA displacement estimate. We found that 11%, 25%, and 6% of image area from the CER, CPS and SAN cameras had insufficient LCA displacement magnitude, respectively.

6. CONCLUSION

In this paper, we propose a technique to improve the accuracy of LCA-based forgery detection. The proposed technique is derived from a statistical model of the error between local estimates of LCA displacement vectors and those predicted by a global model. Using this statistical model, we formulate forgery detection as a hypothesis testing problem, and derive the optimal detection statistic for performing LCA-based forgery detection. Through a series of experiments, we demonstrate that our proposed technique outperforms existing approaches for conducting LCA-based forgery detection.

7. REFERENCES

[1] M. C. Stamm, M. Wu, and K. Liu, "Information forensics: An overview of the first decade," *Access, IEEE*, vol. 1, pp. 167–200, 2013.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *Signal Processing, IEEE Transactions on*, vol. 53, no. 2, pp. 758–767, 2005.

[3] M. Kirchner, "Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue," in *Proceedings of the 10th ACM workshop on Multimedia and security*. ACM, 2008, pp. 11–20.

[4] H. Farid, "Exposing digital forgeries from JPEG ghosts," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 1, pp. 154–160, 2009.

[5] S. Ye, Q. Sun, and E.-C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in *Multimedia and Expo, 2007 IEEE International Conference on*. IEEE, 2007, pp. 12–15.

[6] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of jpeg artifacts," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 3, pp. 1003–1017, 2012.

[7] M. C. Stamm and K. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 3, pp. 492–506, 2010.

[8] M. Chen, J. Fridrich, J. Lukáš, and M. Goljan, "Imaging sensor noise as digital x-ray for revealing forgeries," in *Information hiding*. Springer, 2007, pp. 342–358.

[9] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgery in digital images," in *in Proceedings of Digital Forensic Research Workshop*. Citeseer, 2003.

[10] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Information Hiding*. Springer, 2005, pp. 128–147.

[11] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 1099–1110, 2011.

[12] X. Pan and S. Lyu, "Detecting image region duplication using sift features," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1706–1709.

[13] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in *Proceedings of the 8th workshop on Multimedia and security*. ACM, 2006, pp. 48–55.

[14] T. Gloe, K. Borowka, and A. Winkler, "Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, 2010, pp. 7541–7547.

[15] J. Mallon and P. F. Whelan, "Calibration and removal of lateral chromatic aberration in images," *Pattern recognition letters*, vol. 28, no. 1, pp. 125–135, 2007.

[16] I. Yerushalmy and H. Hel-Or, "Digital image forgery detection based on lens and sensor aberration," *International journal of computer vision*, vol. 92, no. 1, pp. 71–91, 2011.

[17] L. T. Van, S. Emmanuel, and M. S. Kankanhalli, "Identifying source cell phone using chromatic aberration," in *Multimedia and Expo, 2007 IEEE International Conference on*. IEEE, 2007, pp. 883–886.

[18] O. Mayer and M. C. Stamm, "Anti-forensics of chromatic aberration," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, 2015.

[19] C. Harris and M. Stephens, "A combined corner and edge detector." in *Alvey vision conference*, vol. 15. Citeseer, 1988, p. 50.