Countering Anti-Forensics of Lateral Chromatic Aberration

Owen Mayer
Drexel University
Department of Electrical and Computer Engineering
Philadelphia, PA, USA
om82@drexel.edu

Matthew C. Stamm
Drexel University
Department of Electrical and Computer Engineering
Philadelphia, PA, USA
MStamm@coe.drexel.edu

ABSTRACT

Research has shown that lateral chromatic aberrations (LCA), an imaging fingerprint, can be anti-forensically modified to hide evidence of cut-and-paste forgery. In this paper, we propose a new technique for securing digital images against anti-forensic manipulation of LCA. To do this, we exploit resizing differences between color channels, which are induced by LCA anti-forensics, and define a feature vector to quantitatively capture these differences. Furthermore, we propose a detection method that exposes anti-forensically manipulated image patches. The technique algorithm is validated through experimental procedure, showing dependence on forgery patch size as well as anti-forensic scaling factor.

KEYWORDS

Image Forgery Detection; Anti-Forensics; Lateral Chromatic Aberration; Image Splicing; Multimedia Forensics

1 INTRODUCTION

Tampered digital images have become increasingly prevalent in today's society. Often, image forgers will manipulate the content of an image to maliciously alter its meaning. Since many facets of society rely upon authentic digital information, such as courts of law and media outlets, it necessary to ensure that images are truthful and haven't undergone manipulation. Image authenticity is verified using forensic methods that operate by detecting imperceptible traces, or fingerprints, left behind by the tampering process [16].

In response to multimedia forensics, techniques that hide or obfuscate tampering fingerprints have become common. These methods, called anti-forensics, operate by masking the traces that are inherently left behind during a tampering process. This fools forensic techniques into perceiving that a tampered image is authentic. For example, anti-forensic methods have been developed to hide traces of, median filtering [20], resampling [4, 8], JPEG compression [15], sensor noise [4], and lateral chromatic aberrations [11].

Anti-forensics, however, threaten societal confidence in both digital multimedia content and in forensic authentication algorithms. They do this by preventing multimedia content from being accurately authenticated. Therefore, it is crucial to also be able to secure images against anti-forensic methods. One way to do this is to detect traces that are left behind by the anti-forensic processes themselves. Research has shown that many anti-forensic techniques leave behind their own traces that can be detected, such as with anti-forensic tampering of median filtering [23], resampling [13], JPEG compression [1, 10, 18], and sensor noise [5].

Research has shown that localized inconsistencies in lateral chromatic aberrations (LCA) can be used to detect cut-and-paste image forgeries [6, 12, 21], where content from one image is inserted into another image to change its meaning. LCA is an imaging trace present in optical imaging systems. It is introduced by the inability of lenses to focus all wavelengths from a single point source in a scene to a single focal point on the sensor. This manifests as imperceptible color fringes about object edges in an image. LCA patterning is also used to identify source camera model [19] and source imaging lens [22].

Work in anti-forensics, however, has shown that the chromatic aberrations in cut-and-paste forgeries can be anti-forensically altered to hide traces of manipulation [11]. Mayer and Stamm proposed an anti-forensic technique that independently scales and shifts the forged content's color channels to induce specific spatial relationships of focal points across color channels. The induced focal point relationships alters the forged LCA trace to be consistent with an authentic image. As a result, evidence of cut-and-paste manipulation are anti-forensically hidden.

In this paper, we propose a new forensic fingerprint to expose anti-forensic manipulations of lateral chromatic aberrations. Currently, there are no known forensic traces that can detect anti-forensics of LCA. Our proposed fingerprint exploits differences in resizing between color channels, which are introduced during the anti-forensic manipulation of LCA. To do this, we extract spectral properties of resampling artifacts. Then, we examine amplitude and phase angle differences across color channels at frequencies related to JPEG blocking discontinuities in precompressed images. We use these amplitude and phase angle differences to define a feature vector that captures the fingerprint of anti-forensic tampering of LCA. Furthermore, we propose a detection method to expose image regions containing anti-forensically manipulated lateral chromatic aberrations. To do this, we calculate our proposed fingerprint-feature vector in an image region, and then conduct a statistical test to determine whether the fingerprint is indicative of an anti-forensically forged region.

2 BACKGROUND

When capturing an image, light from a scene is focused onto an optical sensor using a lens. However, the refractive index of glass is dependent on wavelength of light passing through it. This causes the different wavelengths of a light ray, originating from the same point source in a scene, to be focused onto laterally offset locations

IH&MMSec '17, June 20–22, 2017, Philadelphia, PA, USA

ACM ISBN 978-1-4503-5032-7/17/06…$15.00
DOI: http://dx.doi.org/10.1145/3082031.3083242

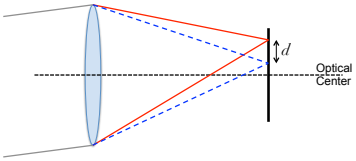


Figure 1: Ray tracing diagram of lateral chromatic aberration. The vector d shows the displacement of focal points between color channels.

on the sensor. This effect is called lateral chromatic aberration (LCA), which manifests as color fringes around object edges in an image. Fig. 1 shows a ray tracing diagram depicting LCA, which shows the red and blue components of an incoming ray of light being focused onto offset sensor locations.

Johnson and Farid developed a model to characterize the effect of LCA [6], which maps a focal point location $\mathbf{r} = [r_x, r_y]^\mathsf{T}$ in a reference channel to its corresponding focal point location $\mathbf{c} = [c_x, c_y]^\mathsf{T}$ in a comparison color channel. This mapping by the function $f(\mathbf{r}, \boldsymbol{\theta})$ is parameterized by the tuple $\boldsymbol{\theta} = [\alpha, \boldsymbol{\zeta}]^\mathsf{T}$. Johnson and Farid model LCA as a first order scaling by an expansion coefficient α, about the image's optical center $\boldsymbol{\zeta} = [\zeta_x, \zeta_y]^\mathsf{T}$, where

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

The comparison color channel is viewed as an expanded or contracted version of the reference color channel, with the expansion coefficient α determining the expansion/contraction scaling factor. Note that the optical center $\boldsymbol{\zeta}$ need not be the image geometric center. Specification of which channels are used as reference and comparison are typically left out of notation to maintain generality, but are made explicit in the text where necessary.

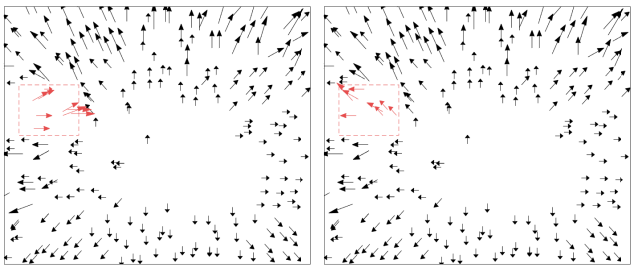
The displacement vector between reference focal point $\mathbf{r}$ and its corresponding focal point in the comparison channel $\mathbf{c}$ is useful for characterizing LCA. Gloe et al. developed a method to estimate localized LCA displacement vectors in a digital image, as well as a method to estimate the LCA model tuple $\boldsymbol{\theta}$ from these local displacement estimates [3]. Research has shown that localized inconsistencies of LCA displacement from the global model of displacement can be used to expose cut-and-paste image forgeries [6, 12], since the LCA displacement in the forged content is not consistent with the original image.

2.1 LCA Anti-Forensics

Work in [11] showed that the lateral chromatic aberration in a forged image region can be modified to hide traces of cut-and-paste tampering. This is accomplished by changing the LCA within the forged region to be consistent with the rest of the image. To change the LCA within the forged regions, the color channels of the forged image region are scaled and shifted, which changes the spatial relationships of focal points across color channels.

The specific scaling and shifting to be applied to the forged image region was determined so that its LCA displacements are consistent with the rest of the image. To do this, a transformation was introduced that relates the desired anti-forensicly modified focal point location in a comparison color channel $\mathbf{c}'$ to its current location $\mathbf{c}$, such that

$$\mathbf{c}' = \alpha_D \left(\frac{1}{\alpha_S} (\mathbf{c} - \boldsymbol{\zeta}_S) + \boldsymbol{\zeta}_S - \boldsymbol{\zeta}_V \right) + \boldsymbol{\zeta}_V. \tag{2}$$



(a) LCA Displacement in a Naive Forgery **(b) LCA Displacement in an Anti-Forensic Forgery**

Figure 2: LCA displacement vectors in naively forged (left), and anti-forensically forged (right) images. The LCA displacements in the forged region are highlighted in red. Vectors are scaled by a factor of 200 for display purposes.

The transformation first removes the inherent LCA parameterized by the source expansion coefficient α_S and source optical center $\boldsymbol{\zeta}_S$. Then, new focal point relationships are artificially induced by a resampling operation, parameterized by the destination image expansion coefficient α_D and virtual optical center $\boldsymbol{\zeta}_V$, a constant determined by the relationship of the forged image region to the destination optical center. The anti-forensic transformation equation can be rewritten to show that

$$\mathbf{c}' = \frac{\alpha_D}{\alpha_S}\mathbf{c} + K. \tag{3}$$

where K is a constant related to the scaled differences between the source and destination optical centers.

That is, the transformation that relates the comparison channel coordinates in source content $\mathbf{c}$, to it's anti-forensically modified version $\mathbf{c}'$, is simply a geometric scaling and shift. The scaling is determined by the ratio of the in the source image expansion coefficient α_S, and destination image expansion coefficient α_D. We call this ratio the anti-forensic scaling factor.

This scaling and shift is performed via interpolated resampling [11]. The resulting anti-forensically modified forged region has LCA that matches its host image. This can be seen in Fig. 2b, which shows the LCA displacement vectors in an anti-forensically forged image region that are consistent with the destination image. Compare this with the LCA in the naively forged version, as shown in 2a, where the LCA displacement vectors in the forged region are inconsistent with the rest of the image.

3 THE LCA ANTI-FORENSICS FINGERPRINT

Anti-forensic tampering of lateral chromatic aberration poses a threat to the security of multimedia information, and therefore it is important to detect. However, no technique currently exists that is able to detect LCA anti-forensics. In this section, we propose a new fingerprint that exposes LCA anti-forensics tampering operations. Our proposed fingerprint exploits differences in resizing between color channels, which are introduced during the anti-forensic manipulation of lateral chromatic aberrations. In our model, we assume that the source image content has been compressed at some point prior to forgery and anti-forensic manipulation. Since images are commonly stored in JPEG format, it is likely that a forger will alter an image that has been compressed. We exploit distinct

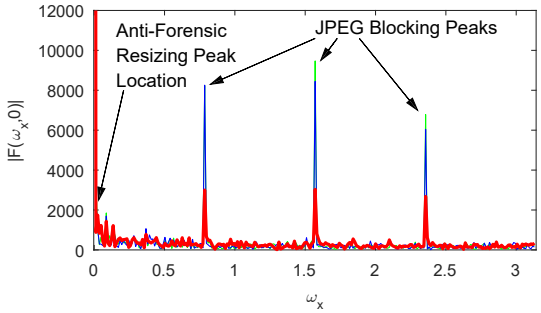


Figure 3: FFT magnitude of the resampling p-map, at $\omega_y = 0$, in an image patch where the red color channel has been anti-forensically modified.

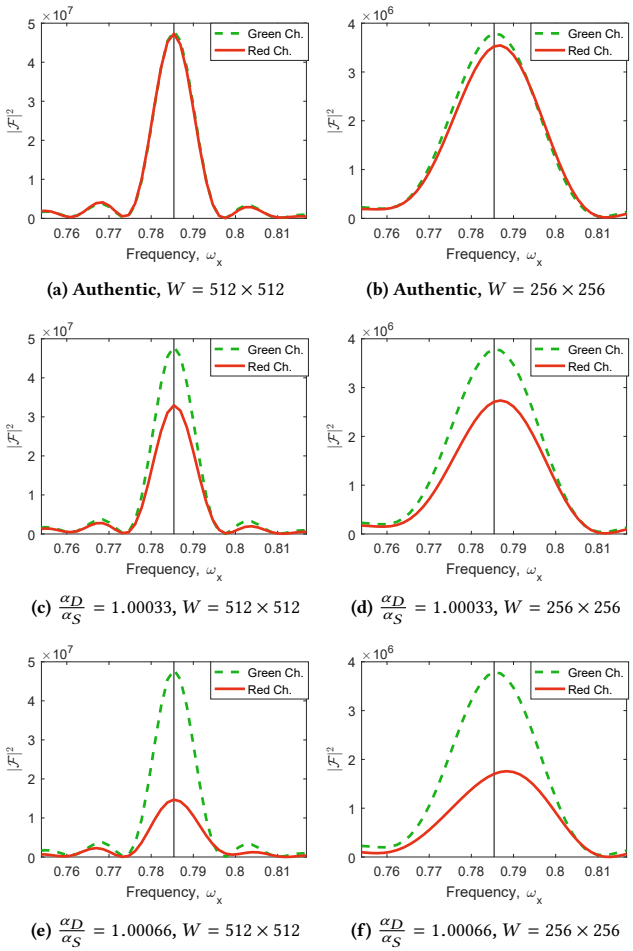
spectral peaks that are related to JPEG blocking discontinuities, by examining amplitude and phase angle differences across color channels at these spectral peaks. The amplitude and phase differences are used as evidence of anti-forensic LCA manipulation.

Since anti-forensic LCA tampering is performed by a scaling and resampling operation, it follows that resampling detection techniques are useful for detecting anti-forensically forged images. However, the scaling factor used in LCA anti-forensics is too small to be detected by typical resampling detection methods, such as those in [7, 14]. Typically, resizing is detected using a construct called a p-map, which describes the probability that a pixel is a linear combination of its neighbors. Resizing introduces periodicity into the p-map, and the corresponding spectral peaks in the p-map FFT are used to expose resizing operations [7, 14]. However, at these small anti-forensic scaling factors, the resizing spectral peak in the resampling p-map is indiscernible from the naturally occuring low frequency content. This is seen in Fig. 3, which shows the p-map FFT of an anti-forensically tampered image region. In this figure, the anti-forensic resizing peak in the anti-forensically modified red channel is indiscernible from low-frequency content and is undetectable by traditional peak detection methods.

The effects of LCA anti-forensics, however, are apparent in the spectral peaks related to JPEG blocking discontinuities. Spectral peaks related to JPEG blocking occur in the p-map frequency domain because pixel values are not linearly predictable across JPEG blocks, and thus have a relatively low p-map value. These low p-map values occur every 8 pixels, and introduce distinct peaks in the p-map spectrum at $\omega = \frac{\pi}{4}, \frac{\pi}{2}$, and $\frac{3\pi}{4}$ [9], which can be seen in Fig. 3.

When an image channel is anti-forensically modified, the channel is slightly resized through an interpolation operation. This consequently introduces correlations, albeit slight, in pixel values across the JPEG blocking grid. As a result, the p-map deviations that are typically observed at JPEG blocking boundaries are decreased. Thus the spectral peaks related to JPEG blocking are reduced in anti-forensically modified color channels. This effect is seen in Fig. 3, which shows the p-map FFT in the x direction ($\omega_y = 0$) for three color channels, with the red channel anti-forensically modified. The JPEG spectral peaks in the anti-forensically modified red channel are small relative to the to unmodified green and blue channels.

In practice, an image is anti-forensically modified by keeping one color channel unmodified and applying the anti-forensic scaling and shifting to the remaining two color channels [11]. The unmodified



(a) **Authentic,** $W = 512 \times 512$ (b) **Authentic,** $W = 256 \times 256$

(c) $\frac{\alpha_D}{\alpha_S} = 1.00033$, $W = 512 \times 512$ (d) $\frac{\alpha_D}{\alpha_S} = 1.00033$, $W = 256 \times 256$

(e) $\frac{\alpha_D}{\alpha_S} = 1.00066$, $W = 512 \times 512$ (f) $\frac{\alpha_D}{\alpha_S} = 1.00066$, $W = 256 \times 256$

Figure 4: Magnitude of p-map FFT in red and green color channels showing the affect of LCA anti-forensics. The JPEG blocking peak at $(\omega_x, \omega_y) = (\frac{\pi}{4}, 0)$ is shown. The pre-compressed image taken by a Canon SX500-IS has an anti-forensically modified red channel using the green channel as the reference channel. Different window sizes W and anti-forensic scaling factors α_D/α_S are examined. The windowed p-maps are zero padded to 4096×4096 before taking their FFT.

color channel is called the reference channel and the modified color channels are called the comparison color channels. As a result, an anti-forensically tampered image region will have JPEG-blocking spectral peaks that are much smaller in the comparison color channels relative to the reference color channel.

The effect of LCA anti-forensics is detailed in Fig. 4, which shows the spectral p-map FFT magnitude with different anti-forensic scaling factors and different inspection window sizes. The figures show the first JPEG spectral peak in the x direction at $\omega_x = \frac{\pi}{4}$, $\omega_y = 0$ in both the red comparison channel and in the green reference channel. In authentic image regions, the spectral peak in the red (comparison) and green (reference) channels are nearly identical. The spectral peak in the comparison channel is reduced when LCA anti-forensics is applied with scaling factor 1.00033, and further reduced when the scaling factor is increased to 1.00066. Furthermore,

the peak differences are much more discernible at larger window sizes of 512×512 than 256×256.

The spatial shifting of color channels during LCA anti-forensic tampering also affects the phase of the JPEG blocking grid. This manifests as phase angle differences when comparing the phase angle of the reference channel to the phase angle of the anti-forensically modified comparison channel. Fig. 5 shows phase angles in an authentic image patch and in the same image patch that has been anti-forensically modified. In the anti-forensically modified patch, the phase angles of the red comparison channel deviate from the phase angles of the green comparison channel. In the authentic image patch, the phase angles are well matched.

4 PROPOSED FINGERPRINT FEATURE VECTOR OF LCA ANTI-FORENSICS

To quantitatively capture the effects of LCA anti-forensics we define a feature vector as follows. We measure the ratio of JPEG spectral peak magnitudes between the 1) red and green channels, 2) blue and green channels, and 3) red and blue channels. In authentic image regions, it is expected that these ratios are near unity whereas in anti-forensically tampered regions these ratios deviate significantly. Since the choice of reference channel is unknown to an investigator, ratios between all three possible color channel pairs are considered. Additionally, the difference in phase angle at the JPEG spectral peaks are measured for each of the three color channel pairings. In authentic image regions, it is expected that these phase angle differences are near zero whereas in anti-forensically modified image regions these phase angle differences deviate from zero.

At a given peak location defined by frequencies ω_x and ω_y six fingerprint values are measured: three magnitude ratios and three phase angle differences. These six values are represented by the vector $\mathbf{x}\left(\omega_x, \omega_y\right)$ as follows,

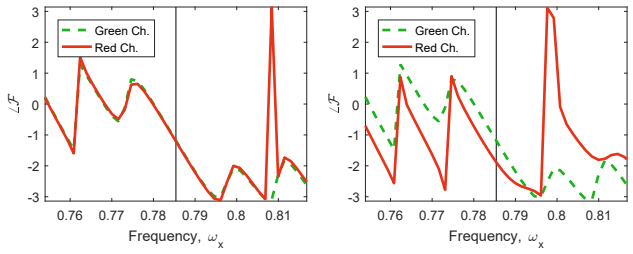
$$\mathbf{x}\left(\omega_x,\omega_y\right) = \begin{bmatrix} \left|\mathcal{F}_{\mathcal{R}}\left(\omega_x,\omega_y\right)\right| / \left|\mathcal{F}_{\mathcal{G}}\left(\omega_x,\omega_y\right)\right| \\ \left|\mathcal{F}_{\mathcal{B}}\left(\omega_x,\omega_y\right)\right| / \left|\mathcal{F}_{\mathcal{G}}\left(\omega_x,\omega_y\right)\right| \\ \left|\mathcal{F}_{\mathcal{R}}\left(\omega_x,\omega_y\right)\right| / \left|\mathcal{F}_{\mathcal{B}}\left(\omega_x,\omega_y\right)\right| \\ \angle\mathcal{F}_{\mathcal{R}}\left(\omega_x,\omega_y\right) - \angle\mathcal{F}_{\mathcal{G}}\left(\omega_x,\omega_y\right) \\ \angle\mathcal{F}_{\mathcal{B}}\left(\omega_x,\omega_y\right) - \angle\mathcal{F}_{\mathcal{G}}\left(\omega_x,\omega_y\right) \\ \angle\mathcal{F}_{\mathcal{R}}\left(\omega_x,\omega_y\right) - \angle\mathcal{F}_{\mathcal{B}}\left(\omega_x,\omega_y\right) \end{bmatrix}^{\mathsf{T}}. \tag{4}$$

Here, $\left|\mathcal{F}\left(\omega_x,\omega_y\right)\right|$ is the p-map FFT magnitude at frequency (ω_x,ω_y), and $\angle\mathcal{F}\left(\omega_x,\omega_y\right)$ is the p-map FFT phase angle at frequency (ω_x,ω_y). The subscripts $\mathcal{R}$, $\mathcal{G}$ and $\mathcal{B}$ denote the red, green, and blue color channels respectively.

The fingerprint values are measured at six JPEG spectral peak frequencies $(\omega_x,\omega_y) = \left(\frac{\pi}{4},0\right), \left(\frac{\pi}{2},0\right), \left(\frac{3\pi}{4},0\right), \left(0,\frac{\pi}{4}\right), \left(0,\frac{\pi}{2}\right)$, and $\left(0,\frac{3\pi}{4}\right)$. This yields six vectors that are then concatenate to form the full, proposed feature vector

$$\mathbf{X} = \left[\mathbf{x}\left(\tfrac{\pi}{4},0\right)\ \mathbf{x}\left(\tfrac{\pi}{2},0\right)\ \mathbf{x}\left(\tfrac{3\pi}{4},0\right)\ \mathbf{x}\left(0,\tfrac{\pi}{4}\right)\ \mathbf{x}\left(0,\tfrac{\pi}{2}\right)\ \mathbf{x}\left(0,\tfrac{3\pi}{4}\right)\right]^{\mathsf{T}}. \tag{5}$$

The full LCA anti-forensics feature vector $\mathbf{X}$ contains 36 values, comprised of 18 spectral peak magnitude ratios and 18 phase angle differences.



(a) Authentic, $W = 512 \times 512$ **(b) $\frac{\alpha_D}{\alpha_S} = 1.00033$, $W = 512 \times 512$**

Figure 5: Phase angle of p-map FFT in red (comparison) and green (reference) color channels showing the affect of LCA anti-forensics on the JPEG blocking peak at $\omega_x = \frac{\pi}{4}, \omega_y = 0$.

Examples of the fingerprint $\mathbf{X}$ are shown in Fig. 6 for authentic and anti-forensically modified image patches. Fig. 6a shows histograms of $\mathbf{X}_1 = \left|\mathcal{F}_{\mathcal{R}}\left(\frac{\pi}{4},0\right)\right| / \left|\mathcal{F}_{\mathcal{G}}\left(\frac{\pi}{4},0\right)\right|$, the first fingerprint dimension. The authentic values are distributed near unity whereas values from anti-forensic patches are typically smaller, and are easily discriminated. Fig. 6b shows a scatter plot of dimensions $\mathbf{X}_1 = \left|\mathcal{F}_{\mathcal{R}}\left(\frac{\pi}{4},0\right)\right| / \left|\mathcal{F}_{\mathcal{G}}\left(\frac{\pi}{4},0\right)\right|$ and $\mathbf{X}_{19} = \left|\mathcal{F}_{\mathcal{R}}\left(0,\frac{\pi}{4}\right)\right| / \left|\mathcal{F}_{\mathcal{G}}\left(0,\frac{\pi}{4}\right)\right|$. The use of two (and more) dimensions increases discrimination.

5 PROPOSED DETECTION METHOD

To expose image regions that have undergone LCA anti-forensic manipulation, we propose a new detection method using the fingerprint described in Sec. 4. To do this, we define a hypothesis testing problem where under the null hypothesis $\mathcal{H}_0$ the image patch has not undergone LCA anti-forensics, and under the alternative hypothesis, $\mathcal{H}_1$, the LCA in the image patch has anti-forensically modified.

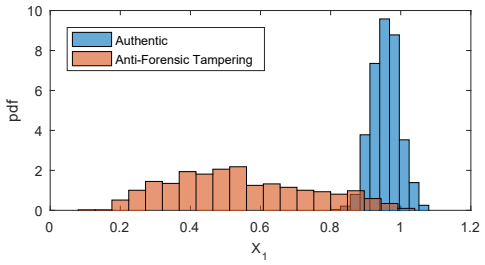
$$\mathcal{H}_0 : \text{No LCA anti-forensics}$$
$$\mathcal{H}_1 : \text{LCA anti-forensics}$$

To describe patches under the null hypothesis, we build a statistical model of the LCA anti-forensic fingerprint in unmodified image regions. Fig 6a shows a histogram of $\mathbf{X}_1$, the first dimension of the fingerprint feature vector, in authentic and anti-forensically modified image patches. We observe from this histogram that $\mathbf{X}_1$ is distributed approximately Gaussian in authentic patches, with a mean near one. We model the entire fingerprint vector as a 36 dimensional random variable that is distributed Gaussian, with a mean vector $\boldsymbol{\mu}$, and covariance Σ. The probability density function $p(\mathbf{X}|\mathcal{H}_0)$ of $\mathbf{X}$ in authentic patches is as follows:

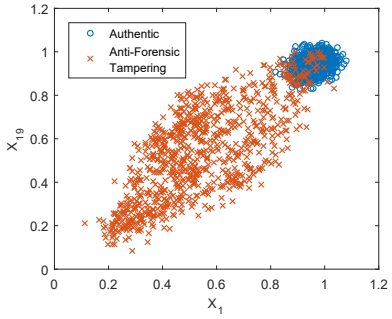
$$p(\mathbf{X}|\mathcal{H}_0) = \frac{1}{\sqrt{(2\pi)^{36}\,|\Sigma|}} \exp\left(-\tfrac{1}{2}\left(\mathbf{X}-\boldsymbol{\mu}\right)\Sigma^{-1}\left(\mathbf{X}-\boldsymbol{\mu}\right)\right). \tag{6}$$

The authentic distribution parameters mean, $\boldsymbol{\mu}$, and covariance, Σ, are estimated from image patches extracted from many JPEG compressed images that are known to have not been modified. Since the patch size effects the fingerprint values, as seen in Fig. 6, the authentic distribution parameters must be estimated separately for each patch/window size that is used.

The fingerprint feature vector under the alternative hypothesis depends upon the anti-forensically scaling factor. This is shown in Fig. 4. Without knowing the anti-forensic scaling factor, which



(a) Histogram of X_1



(b) Features X_1 and X_{19}

Figure 6: Histogram (top) and scatterplot (bottom) of fingerprint features X in authentic (blue) and anti-forensically modified patches (red).

requires knowledge of the source image, it is impractical to model the fingerprint feature in anti-forensically manipulated patches. As a result, we are left only to compare with authentic model. In anti-forensically forged image patches, the fingerprint feature vector deviates significantly from $\boldsymbol{\mu}$. This effect is seen in Fig. 6b, where a scatter plot of features $\mathbf{X}_1$ and $\mathbf{X}_{19}$ shows that the fingerprint in anti-forensically modified patches deviates significantly from the fingerprint in authentic patches.

To quantify the deviations of $\mathbf{X}$ from the authentic model of the fingerprint feature, we use the Mahalanobis distance [17], which is as follows:

$$m = \left((\mathbf{X} - \boldsymbol{\mu})^{\mathsf{T}} \Sigma^{-1} (\mathbf{X} - \boldsymbol{\mu})\right)^{\frac{1}{2}}. \tag{7}$$

The distance m describes deviations of the fingerprint vector $\mathbf{X}$ from the authentic distribution mean $\boldsymbol{\mu}$. Importantly, the Mahalanobis distance accounts for differences in the variances of each of the fingerprint dimensions. That is, a deviation in a dimension with a small variance is more indicative of manipulation than an equivalent deviation in a dimension with a large variance. The differences in variances are normalized by the Σ^{-1} term in (7). Additionally, the Mahalanobis distance accounts for any correlations that may exist among the authentic fingerprint dimensions.

The distance m is small in authentic image patches, and large in anti-forensically tampered image patches. We use this to define a decision rule $\delta(\cdot)$ to determine if an image patch authentic or anti-forensically modified. The decision rule employs a threshold test, where distances m greater than or equal to the threshold τ reject the null hypothesis in favor of the alternative hypothesis.

$$\delta(m) = \begin{cases} \mathcal{H}_0, & m < \tau \\ \mathcal{H}_1, & m \geq \tau \end{cases} \tag{8}$$

The decision threshold τ can be varied to set the false alarm rate.

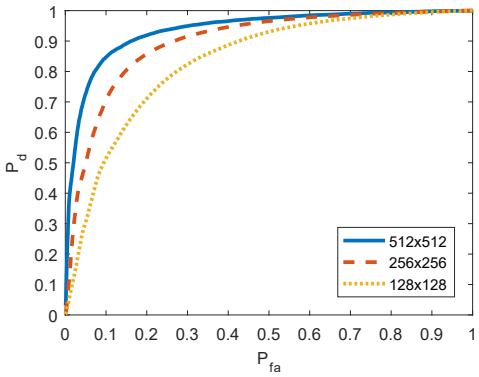


Figure 7: ROC curves of the proposed detection method on different block sizes. Forgeries were made by copying and pasting image blocks from database images, and anti-forensically modifying their LCA to hide forgery traces.

6 EXPERIMENTAL RESULTS

We conducted a series of experiments in order to evaluate the efficacy of our proposed fingerprint and proposed detection method at exposing image patches that have been manipulated by LCA anti-forensics. To do this, we started with a database of images 16961 unaltered, JPEG compressed images from the Dresden Image Database [2]. We used all images from the "Natural images" set, which were captured by 27 unique camera models and representing a diverse set of LCA expansion coefficients. We produced 20000 cut-and-paste forged images and anti-forensically tampered the forged regions to hide traces of LCA inconsistency. To make the cut-and-paste forgeries, we randomly chose a source image to cut from, and randomly chose a destination image to paste into. The source (cut) and destination (paste) locations were chosen at random, as well.

To make each forgery, a 512×512 block was cut from the source location in the source image, and pasted at the destination location in the destination image. The LCA model parameters for the destination and source images were estimated using Gloe et al.'s efficient method [3]. Finally, LCA anti-forensics was applied using Mayer and Stamm's method [11], using the green channel as the reference channel and the red and blue channels as the comparison channel.

The LCA anti-forensics fingerprint was calculated in each of the 512×512 forged image regions. Furthermore, to evaluate the effect of inspection window size, the forged image regions were segmented into 4 non-overlapping 256×256 patches, as well as 16 non-overlapping 128×128 patches and the anti-forensic fingerprint was determined for each patch. To measure the anti-forensic fingerprint, we first determined the resampling p-map FFT for each color plane in the image region, using the method described in [7]. Finally, the anti-forensics fingerprint $\mathbf{X}$ was determined, its distance m to the authentic model was calculated according to 7, and classification decision $\delta(m)$ rendered according to (8).

To estimate the authentic model parameters, 100000 unmodified image patches of size 512×512, 256×256, and 128×128 were chosen. The LCA anti-forensics fingerprint was measured in each of the 300000 authentic patches (100000 patches for each of 3 window sizes). At each size, 10000 patches were randomly chosen to estimate the authentic fingerprint distribution parameters mean

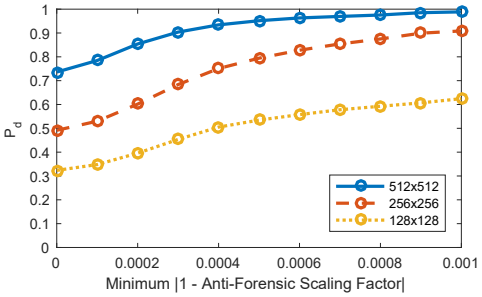


Figure 8: Probability of detection versus LCA anti-forensic scaling at a 5% false alarm rate.

$\boldsymbol{\mu}$, and covariance $\boldsymbol{\Sigma}$. The remaining 90000 patches were used to determine false alarm rates at varied decision thresholds.

Fig. 7 shows the receiver operator characteristic for our proposed detection method. At a 10% false alarm rate, our method achieved a 85% positive detection rate when using a 512×512 inspection window, demonstrating that our proposed fingerprint feature vector and detection method are able to successfully expose image patches as having been manipulated with LCA anti-forensics. At a smaller window size of 256×256, our detection method achieved a 71% positive detection rate, and a 52% positive detection rate with the smallest 128×128 window. At a 5% false alarm rate, our method achieved a 73%, 50%, and 31% positive detection rate at window sizes of 512×512, 256×256, and 128×128 respectively.

Furthermore, we evaluated the effect of the scaling factor used in the LCA anti-forensic tampering process on detection performance. Fig. 8 shows the detection rates at a 5% false alarm rate as a function of anti-forensic scaling factor. For each forgery, we determined the anti-forensic scaling factor applied for each of the two comparison color channels and determined its absolute distance from 1 (no scaling). The x-axis of Fig. 8 includes all forgeries with at least one of the two anti-forensic scaling factors greater than the x axis value. This method gives a measure of "strength" of LCA anti-forensics. For example, a scaling factor value of 0.0005 indicates that at least one of the red or blue comparison channels were scaled by either greater than 1.0005, or less than 0.9995.

At a scaling factor value of 0.0005, anti-forensically tampered patches were correctly identified at a rate of 95% with a window size of 512×512, 79% with a window size of 256×256, and 53% with a window size of 128×128. At a scaling factor value of 0.001, anti-forensically tampered patches were correctly identified at a rate of 99% with a window size of 512×512, 91% with a window size of 256×256, and 62% with a window size of 128×128. This result demonstrates that the strength of the LCA anti-forensic tampering greatly effects its ability to be detected.

7 CONCLUSION

In this paper, we propose a new algorithm for securing digital images against anti-forensic manipulation of LCA. To do this, we exploit resizing differences between color channels, which are induced by LCA anti-forensics, and define a feature vector to quantitatively capture these differences. Furthermore, we propose a detection method that exposes anti-forensically manipulated image patches. The proposed algorithm is validated through experimental procedure, showing dependence on patch size as well as anti-forensic scaling factor.

8 ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 1553610. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Fontani, M., Bonchi, A., Piva, A., and Barni, M. Countering anti-forensics by means of data fusion. In *IS&T/SPIE Electronic Imaging* (2014), International Society for Optics and Photonics, pp. 90280Z–90280Z.

[2] Gloe, T., and Böhme, R. The dresden image database for benchmarking digital image forensics. *Journal of Digital Forensic Practice 3*, 2-4 (2010), 150–159.

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

[4] Gloe, T., Kirchner, M., Winkler, A., and Böhme, R. Can we trust digital image forensics? In *Proceedings of the 15th International Conference on Multimedia* (New York, NY, USA, 2007), MULTIMEDIA '07, ACM, pp. 78–86.

[5] Goljan, M., Fridrich, J., and Chen, M. Sensor noise camera identification: Countering counter-forensics. In *IS&T/SPIE Electronic Imaging* (2010), International Society for Optics and Photonics, pp. 75410S–75410S.

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

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

[8] Kirchner, M., and Böhme, R. Hiding traces of resampling in digital images. *IEEE Transactions on Information Forensics and Security 3*, 4 (2008), 582–592.

[9] Kirchner, M., and Gloe, T. On resampling detection in re-compressed images. In *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on* (2009), IEEE, pp. 21–25.

[10] Lai, S., and Böhme, R. Countering counter-forensics: The case of JPEG compression. In *Int. Workshop on Information Hiding* (2011), Springer, pp. 285–298.

[11] Mayer, O., and Stamm, M. C. Anti-forensics of chromatic aberration. In *IS&T/SPIE Electronic Imaging* (2015), Int. Society for Optics and Photonics.

[12] Mayer, O., and Stamm, M. C. Improved forgery detection with lateral chromatic aberration. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (2016), IEEE, pp. 2024–2028.

[13] Peng, A., Zeng, H., Lin, X., and Kang, X. Countering anti-forensics of image resampling. In *Image Processing (ICIP), 2015 IEEE International Conference on* (2015), IEEE, pp. 3595–3599.

[14] Popescu, A. C., and Farid, H. Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on signal processing 53*, 2 (2005), 758–767.

[15] Stamm, M. C., and Liu, K. J. R. Anti-forensics of digital image compression. *IEEE Trans. Information Forensics and Security 6*, 3 (Sep. 2011), 1050 –1065.

[16] Stamm, M. C., Wu, M., and Liu, K. J. R. Information forensics: An overview of the first decade. *Access, IEEE 1* (2013), 167–200.

[17] Theodoridis, S., and Koutroumbas, K. Pattern recognition (4th edition), 2009.

[18] Valenzise, G., Nobile, V., Tagliasacchi, M., and Tubaro, S. Countering JPEG anti-forensics. In *Image Processing (ICIP), 2011 18th IEEE International Conference on* (2011), IEEE, pp. 1949–1952.

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

[20] Wu, Z.-H., Stamm, M. C., and Liu, K. R. Anti-forensics of median filtering. In *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on* (2013), IEEE, pp. 3043–3047.

[21] Yerushalmy, I., and Hel-Or, H. Digital image forgery detection based on lens and sensor aberration. *International journal of computer vision 92*, 1 (2011), 71–91.

[22] Yu, J., Craver, S., and Li, E. Toward the identification of DSLR lenses by chromatic aberration. In *IS&T/SPIE Electronic Imaging* (2011), International Society for Optics and Photonics, pp. 788010–788010.

[23] Zeng, H., Qin, T., Kang, X., and Liu, L. Countering anti-forensics of median filtering. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on* (2014), IEEE, pp. 2704–2708.