Anti-Forensics of Chromatic Aberration

Owen Mayer and Matthew C. Stamm

Dept. of Electrical and Computer Engineering, Drexel University, Philadelphia, PA, USA

ABSTRACT

Over the past decade, a number of information forensic techniques have been developed to identify digital image manipulation and falsifications. However, recent research has shown that an intelligent forger can use anti-forensic countermeasures to disguise their forgeries. In this paper, an anti-forensic technique is proposed to falsify the lateral chromatic aberration present in a digital image. Lateral chromatic aberration corresponds to the relative contraction or expansion between an images color layers that occurs due to a lenss inability to focus all wavelengths of light on the same point. Previous work has used localized inconsistencies in an images chromatic aberration to expose cut-and-paste image forgeries. The anti-forensic technique presented in this paper operates by estimating the expected lateral chromatic aberration at an image location, then removing deviations from this estimate caused by tampering or falsification. Experimental results are presented that demonstrate that this anti-forensic technique can be used to effectively disguise evidence of an image forgery.

Keywords: Information Forensics, Anti-Forensics, Copy-and-Move Forgery, Lateral Chromatic Aberration

1. INTRODUCTION

In order to determine the authenticity, processing history, and source of digital images, researchers have developed a variety of information forensic techniques.[1] Recent research has shown, however, that an intelligent forger can create anti-forensic countermeasures capable of fooling several forensic algorithms. These anti-forensic attacks operate by removing or falsifying traces used by forensic techniques to identify image processing and falsification.

Anti-forensic attacks have been proposed to falsify an image's compression history,[2] and hide evidence of common editing operations such as resampling caused by image resizing or rotation,[3] median filtering,[4] contrast enhancement,[5] and "copy-move" forgeries.[6] General approaches have been developed to fool histogram-based forensic algorithms,[5,7] along with methods of falsifying camera-specific traces such as sensor noise[8] and both color-filter array patterns and demosaicking artifacts.[9] Additionally, anti-forensic attacks have been developed to hide evidence of frame deletion in digital videos.[10]

One important forensic trace that has not yet been anti-forensically attacked is an image's lateral chromatic aberration. Lateral chromatic aberration is specific form of color distortion that occurs because a camera's lens is unable to achieve the same focal point for all wavelengths of light. This results in a slight misalignment between an image's color channels corresponding to a relative contraction or expansion about the image's optical center. In previous work, Johnson and Farid showed that copying an object from an image then pasting it elsewhere within the same or a different image will introduce localized inconsistencies in an image's chromatic aberration.[11] Using this information, they developed a technique to detect "copy-and-move" forgeries by first fitting an image's global lateral chromatic aberration pattern to a model, then searching for image subregions where the localized lateral chromatic aberration significantly deviates from the global model.

In this paper, we present a technique to disguise copy-and-paste forgeries by falsifying the lateral chromatic aberration within the inauthentic region of an image. Our anti-forensic attack works by using a model to determine the expected lateral chromatic aberration of pixels in the image region where a copied object is to be pasted. Next, the image that the object is copied from is modified so that its lateral chromatic aberration within the object region matches the expected lateral chromatic aberration of the region of the image to where it will be pasted. This is done by first establishing a reference color channel, then mapping the pixel locations of the two remaining color channels to new spatial locations that will match the desired lateral chromatic aberration. Finally, the modified image is resampled along the pixel grid, and the object is copied and pasted into the target

The authors can be reached by email at om82@drexel.edu and mcstamm@coe.drexel.edu.

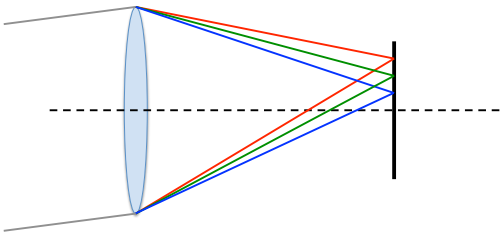


Figure 1. Lateral chromatic aberration through a lens.

image. We experimentally validate the performance of our anti-forensic attack by creating a set of anti-forensically modified copy-and-paste forgeries, then examining each image for lateral chromatic aberration inconsistencies indicative of a falsified image. Our results demonstrate that our proposed anti-forensic attack can successfully disguise inconsistencies in an image's lateral chromatic aberration caused by copy-and-paste forgeries.

2. BACKGROUND

In this section, we provide a brief overview of lateral chromatic aberration, how it is estimated, and how it is used in information forensic to detect copy-and-paste image forgeries.

When a digital camera captures an image, light is focused onto the camera's imaging sensor using a photographic lens. Ideally, the lens accomplishes this by refracting all rays of light originating from a single point in the scene onto a common focal point on the sensor. In reality, however, the refractive index of the lens is dependent on the wavelength of the light that passes through it. This will cause a specific type of color distortion known as lateral chromatic aberration. Lateral chromatic aberration occurs when different wavelengths of light originating from the same source point are focused onto slightly different points on the camera's sensor, as is shown in Fig. 1.

Since the amount of refraction is also dependent upon a light ray's angle of incidence with the lens, the distance between the focal points of two different wavelengths tends to increase with the radial distance from the optical axis. Because of this, lateral chromatic aberration can be viewed as a slight misalignment between an image's color channels corresponding to a relative contraction or expansion about the image's optical center. This visually manifests itself as color fringing around edges and corners within an image.

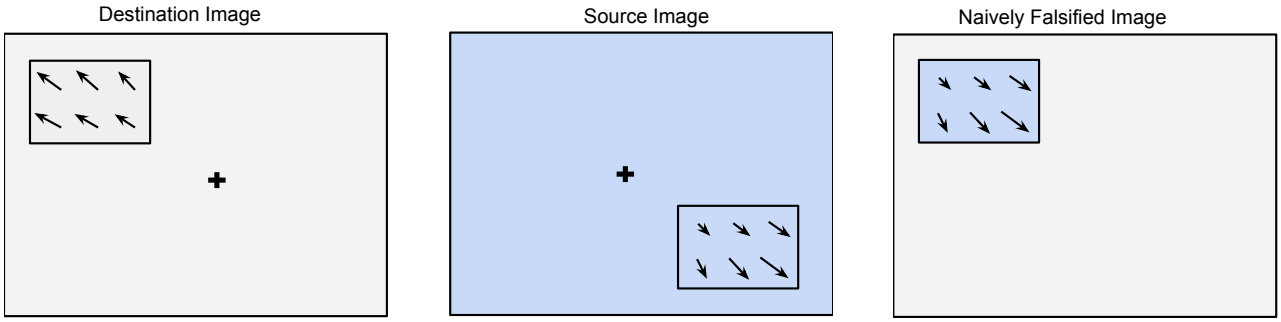
2.1 Forgery Detection Using Lateral Chromatic Aberration

The misalignment between two color channels due to lateral chromatic aberration can be characterized by a mapping relating the spatial location (x^r, y^r) of a point in a reference color channel to its location (x^c, y^c) in a comparison color channel. This mapping can be modeled as a parametric function f with parameter set θ, i.e. $(x^c, y^c) = f\big((x^r, y^r), \theta\big)$. By adopting this approach, the global lateral chromatic aberration pattern between two color channels can be determined entirely by estimating the values of the parameter set θ.

Johnson and Farid showed that significant localized deviations of the lateral chromatic aberration pattern from a global model can be used to expose copy-and-paste forgeries.[11] Copy-and-paste forgeries are created by copying an object from a source image, then pasting it into a destination image. When this is done, the lateral chromatic aberration pattern within the pasted region will correspond to the lateral chromatic aberration at the location it was copied from in the source image. This is unlikely to match the lateral chromatic aberration pattern at its pasted location in the destination image as predicted by a global model. An example of this is shown in Fig. 2.

To detect copy-and-paste forgeries, Johnson and Farid proposed examining an image using the following forensic algorithm. First, a global estimate of the image's lateral chromatic aberration mapping between two color channels is estimated using the model

$$\begin{pmatrix} x^c \\ y^c \end{pmatrix} = f\left(\begin{pmatrix} x^r \\ y^r \end{pmatrix}, \alpha, x^0, y^0\right) = \begin{pmatrix} \alpha(x^r - x^0) + x^0 \\ \alpha(y^r - y^0) + y^0 \end{pmatrix}, \tag{1}$$



(a) (b) (c)

Figure 2. Diagram of a copy-and-paste forgery. (a) Destination image with lateral chromatic aberration displacement vectors highlighted in the paste region. (b) Source image with lateral chromatic aberration displacement vectors highlighted in the copy region. (c) Naively created copy-and-paste forgery with lateral chromatic aberration displacement vectors highlighted in the paste region. Note that the displacement vectors in the paste region of the naively falsified image are inconsistent with those in the unaltered destination image.

where the parameters x^0 and y^0 correspond to the spatial location of the image's optical center in the reference color channel, and α is a scaling parameter that characterizes the degree of expansion or contraction. The estimated parameter set $\theta = (\alpha, x^0, y^0)$ is used to calculate the lateral chromatic aberration displacement vector field, defined as the difference between (x^c, y^c) and (x^r, y^r). Next, the image is divided into blocks, and a local estimate of the lateral chromatic aberration and its corresponding displacement vector field is computed for each block. A block is classified as inauthentic if the angular error between the global and local lateral chromatic aberration displacement vectors exceeds a detection threshold.

2.2 Lateral Chromatic Aberration Estimation

Fitting the lateral chromatic aberration to the model in (1) is a critical step in Johnson and Farid's forgery detection algorithm. To accomplish this, Johnson and Farid observe that given the true values of the parameter set $\theta = (\alpha, x^0, y^0)$, the lateral chromatic aberration distortion in the comparison channel can be compensated for by applying the inverse mapping $f^{-1}(\cdot\,, \theta)$ of (1). As a result, they estimate the model parameters by finding the values θ^* that maximize the similarity, as measured by the mutual information $I(\cdot\,;\,\cdot)$, between a corrected version of the comparison color channel $\mathcal{C}$ and the reference color channel $\mathcal{R}$, i.e.

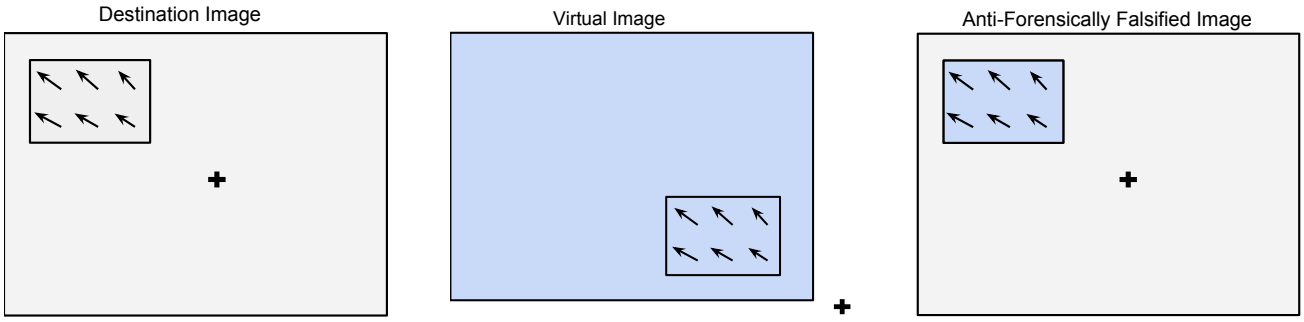
$$\theta^* = \arg\max_{\theta} I\big(f^{-1}(\mathcal{C}, \theta); \mathcal{R}\big). \tag{2}$$

Because the mutual information between the corrected comparison channel and the reference channel is nonconvex in the parameter space, the optimal parameter values θ^* are found through a brute-force search.

While Johnson and Farid's approach yields strong results in terms of model fit for global estimates of the lateral chromatic aberration, it is very computationally expensive. For example, Gloe et al. reported that when conducting experiments with their run-time optimized implementation of this approach, it took approximately 38 minutes to calculate the model parameters for one pair of color channels in a 6 megapixel image.[12] Furthermore, this process must be performed on both pairs of color channels (i.e. (green-to-red) and (green-to-blueblue)), and repeated again for each image block that is examined for evidence of copy-and-past forgery.

To address this problem, a more computationally efficient method of estimating the model parameters was proposed by Gloe et al.[12] This method operates by locally estimating lateral chromatic aberration displacement vectors at several locations throughout the image, then fitting a global model to the local estimates.

Locations suitable for performing these local estimates are chosen by using the Harris corner detection algorithm to identify corner points throughout the reference channel.[13] Next, a search is performed in the comparison channel for the $W \times W$ pixel block $\mathbf{B}^c$ that maximizes the similarity with an equivalently sized block $\mathbf{B}^r$ in the reference channel centered at each corner point. To enable a search over fractional pixel displacements,



(a) (b) (c)

Figure 3. Diagram of an anti-forensically disguised copy-and-paste forgery. (a) Destination image with lateral chromatic aberration displacement vectors highlighted in the paste region. (b) "Virtual" image whose lateral chromatic aberration displacement vectors in the copy region have been modified to match those in the paste region of the destination image. (c) Anti-forensically disguised copy-and-paste forgery with lateral chromatic aberration displacement vectors highlighted in the paste region. Note that the displacement vectors in the paste region of the naively falsified image are consistent with those in the unaltered destination image.

the window is upsampled by a factor of u using bicubic interpolation. The search is limited to a maximum shift of Δ, and the local displacement vector is chosen to correspond to the shift that yields the maximum similarity between the blocks, i.e.

$$\hat{\mathbf{d}}(x,y) = \underset{(m,n)\in\{-\Delta,\ldots,\Delta\}}{\arg\max} s(\mathbf{B}^r(x,y), \mathbf{B}^c(x+m, y+n)) \tag{3}$$

where the similarity $s(\dot{})$ between the two blocks is measured using the correlation coefficient. Finally, the model parameters are found by using an interative Gauss-Newton method to performing a least squares fit of the model to the locally measured displacement vectors.

This approach to lateral chromatic aberration estimation yields significant gains in terms of run time without suffering in terms of accuracy. As a result, we use this approach when estimating the lateral chromatic aberration displacement vectors and model parameters in our experiments.

3. ANTI-FORENSIC ATTACK

In order for a copy-and-paste forgery to successfully avoid detection, local estimates of the lateral chromatic aberration obtained in the image region corresponding to the pasted object must not significantly deviate from the lateral chromatic aberration predicted by a global model. In this section, we propose an anti-forensic attack that to accomplish this by falsifying the lateral chromatic aberration within the pasted object.

When performing our anti-forensic attack, we refer to the image containing the object to be copied as the "source image", and the image into which the object will be pasted as the "destination image." Additionally, we construct an intermediate image referred to as the "virtual image." The virtual image is created so that it contains visual information from the source image, while having a chromatic aberration pattern that is consistent with the destination image. We then conduct an anti-forensic attack by copying information from the virtual and pasting into destination image. Figure 3 provides a diagram of the process.

We adopt the notation convention that coordinates in the source, destination, and virtual images are denoted by the subscripts S, D, and V respectively. For a particular image, coordinates in the reference and comparison color channels are indicated by the superscripts r and c. Furthermore, the coordinates of optical center of an image's comparison channel are indicated by the superscript 0.

We begin our attack by first identifying the location of each pixel in the reference channel of the source image that corresponds to the object to be copied, along with the corresponding location that it will be pasted in the reference channel of the destination image. After this, we choose a comparison channel, and estimate the lateral

chromatic aberration model parameters for both the source and destination images using Gloe et al.'s method described in Sec. 2.2.

Next, we begin to construct the virtual image by choosing its reference channel to be equal to the reference channel of the source image. When we create our forgery, we will copy a pixel from location (x_V^r, y_V^r) in the virtual image and paste it into location (x_D^r, y_D^r) in the destination image. At the location (x_D^r, y_D^r), the global model of the destination image's lateral chromatic aberration can be used to calculate the displacement between the reference and comparison channels. This quantity, known as the displacement vector $\mathbf{d}_D$, is given by the equation

$$\mathbf{d}_D(x_D^r, y_D^r) = \begin{pmatrix} x_D^r \\ y_D^r \end{pmatrix} - \begin{pmatrix} \alpha_D(x_D^r - x_D^0) + x_D^0 \\ \alpha_D(y_D^r - y_D^0) + y_D^0 \end{pmatrix} = \begin{pmatrix} (1-\alpha_D)(x_D^r - x_D^0) \\ (1-\alpha_D)(y_D^r - y_D^0) \end{pmatrix}. \tag{4}$$

Similarly, for a particular choice of model parameters α_V, x_V^0, and y_V^0 for the virtual image, the displacement vector at location (x_V^r, y_V^r) in the virtual image is given by

$$\mathbf{d}_V(x_V^r, y_V^r) = \begin{pmatrix} x_V^r \\ y_V^r \end{pmatrix} - \begin{pmatrix} \alpha_V(x_V^r - x_V^0) + x_V^0 \\ \alpha_V(y_V^r - y_V^0) + y_V^0 \end{pmatrix} = \begin{pmatrix} (1-\alpha_V)(x_V^r - x_V^0) \\ (1-\alpha_V)(y_V^r - y_V^0) \end{pmatrix}. \tag{5}$$

To ensure that the lateral chromatic aberration inside the pasted object matches the destination image's global model, the displacement vectors of the virtual image and the destination image must be equal at locations corresponding to the same point in the object, i.e. $\mathbf{d}_V(x_V^r, y_V^r) = \mathbf{d}_D(x_D^r, y_D^r)$. For this to occur, we note that by inspection of 4 and 5 the following is true:

$$\alpha_V = \alpha_D, \qquad \text{and} \qquad \begin{pmatrix} x_V^r \\ y_V^r \end{pmatrix} - \begin{pmatrix} x_V^0 \\ y_V^0 \end{pmatrix} = \begin{pmatrix} x_D^r \\ y_D^r \end{pmatrix} - \begin{pmatrix} x_D^0 \\ y_D^0 \end{pmatrix}. \tag{6}$$

Since the reference channel of the virtual image is copied from the reference channel of the source image, we know that $(x_V^r, y_V^r) = (x_S^r, y_S^r)$. By substituting this into (6), we can derive the following equation for the location of virtual image's optical center

$$\begin{pmatrix} x_V^0 \\ y_V^0 \end{pmatrix} = \begin{pmatrix} x_S^r \\ y_S^r \end{pmatrix} - \begin{pmatrix} x_D^r \\ y_D^r \end{pmatrix} + \begin{pmatrix} x_D^0 \\ y_D^0 \end{pmatrix}. \tag{7}$$

Since the points (x_S^r, y_S^r), (x_D^r, y_D^r), and $(x_D^0 y_D^0)$ are known, this equation completely specifies the location of the virtual image's optical center. We note that this location may lie outside of the borders of the virtual image.

Using the virtual image's model parameters, we can express a location in its comparison channel in terms of a location in its reference channel using the equation

$$\begin{pmatrix} x_V^c \\ y_V^c \end{pmatrix} = \begin{pmatrix} \alpha_V(x_V^r - x_V^0) + x_V^0 \\ \alpha_V(y_V^r - y_V^0) + y_V^0 \end{pmatrix} \tag{8}$$

Since $(x_V^r, y_V^r) = (x_S^r, y_S^r)$, we can use the inverse of the source image's lateral chromatic aberration model to express a location in the virtual image's reference channel in terms of a location in the source image's comparison channel as

$$\begin{pmatrix} x_V^r \\ y_V^r \end{pmatrix} = \begin{pmatrix} x_S^r \\ y_S^r \end{pmatrix} = \begin{pmatrix} \frac{1}{\alpha_S}(x_S^c - x_S^0) + x_S^0 \\ \frac{1}{\alpha_S}(y_S^c - y_S^0) + y_S^0 \end{pmatrix} \tag{9}$$

Equations (6), (8), and (9) can be combined to express a location in the virtual image's comparison channel in terms of the corresponding location in the source image's comparison channel

$$\begin{pmatrix} x_V^c \\ y_V^c \end{pmatrix} = \begin{pmatrix} \alpha_D\left(\frac{1}{\alpha_S}\left(x_S^c - x_S^0\right) + x_S^0 - x_V^0\right) + x_V^0 \\ \alpha_D\left(\frac{1}{\alpha_S}\left(y_S^c - y_S^0\right) + y_S^0 - y_V^0\right) + y_V^0 \end{pmatrix} \tag{10}$$

where the optical center of the virtual image is given by (7). This equation is used to map each pixel in the source image's comparison channel to its corresponding location in the virtual image. The values of the virtual image's comparison channel are then determined at each pixel location through bicubic interpolation.

This process is repeated again using the remaining comparison channel. Finally, we create our anti-forensically disguised forgery by copying the desired object from the virtual image and pasting it into the destination image.

Our entire anti-forensic algorithm can be summarized briefly as follows:

1. Identify the location where an object will be copied from in the source image and location where it will be pasted in the destination image.
2. Estimate the lateral chromatic aberration model parameters for the source and destination images using Gloe et al.'s method.
3. Set the reference channel of the virtual image equal to the reference channel of the source image.
4. For each pixel in the source image's comparison channel, find its corresponding location in the virtual image's comparison channel using (10).
5. Perform interpolation to determine the values of the virtual image's comparison channel at pixel locations.
6. Repeat this process for the remaining comparison channel.
7. Copy the object from the virtual image and paste it into the desired location in the destination image.

4. SIMULATION AND RESULTS

In order to verify our anti-forensic attack's ability to disguise copy-and-paste forgeries, we conducted an experimental evaluation of its performance.

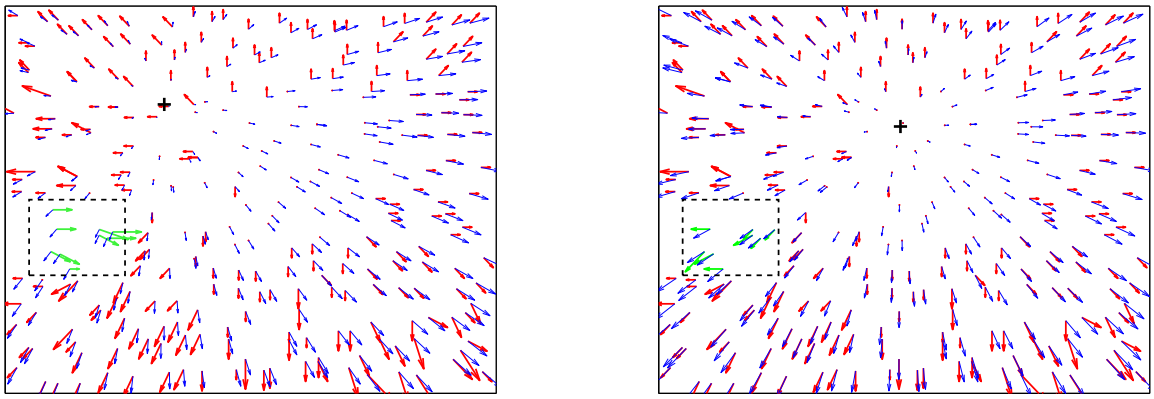
We began by creating a database of 102 unaltered source images of size 2304×3072 pixels captured by a Sony CyberShot DSC-W80 camera, and a database of 102 unaltered destination images of size 1536×2048 pixels captured by a Sony CyberShot DSC-V1 camera. The images in both databases were captured and stored as JPEGs using the default settings of each camera. We used these images to create a set of 102 anti-forensically disguised copy-and-paste forgeries. This was done by selecting a 300×400 pixel block from each image in the source image database, then copy-and-pasting it into an image in the destination image database using our anti-forensic attack. We repeated this process without the use of our anti-forensic attack to create an additional set of 102 "naively" constructed copy-and-paste forgeries.

In practice, a forger may copy from any location in the source image and paste into any location in the destination image. These locations have a significant impact on the performance of Johnson and Farid's forgery detection technique. A forgery will be difficult or impossible to detect if the displacement vectors in the copy and paste regions have similar angular orientations. This is likely to happen if these regions occur at similar locations with respect to the optical centers of the source and destination images.

When constructing the forgeries used in our experiment, the block copied from each source image was located halfway from the image's top and 100 pixels from its right edge. It was pasted halfway from the top and 100 pixels from the left edge of its corresponding destination image. These locations were chosen to provide the most favorable conditions for Johnson and Farid's detection algorithm by maximizing the expected angle between the displacement vectors in the copy and paste regions. Since this corresponds to the least favorable experimental setup for a forger, our results can be interpreted as a minimax evaluation of our anti-forensic attack, thus providing a lower bound on its performance.

Next, using the green channel as the reference channel, we measured the green-to-red and green-to-blue lateral chromatic aberration of each image in the set of anti-forensically disguised forgeries, naively constructed forgeries, and unaltered source images. This was done using Gloe et al.'s method to obtain a series of locally estimated displacement vectors and global model parameters for each image. Locally estimated displacement vectors were obtained using search blocks of size $W = 64$ pixels with an upsampling factor of $u = 5$ and a maximum search displacement of $\Delta = 3$ pixels.

Fig. 4 shows a typical example of the locally estimated and globally modeled displacement vector fields from a naively constructed forgery and an anti-forensically disguised forgery. The falsified image region is marked with



(a) Naively Constructed Forgery

(b) Anti-Forensically Disguised Forgery

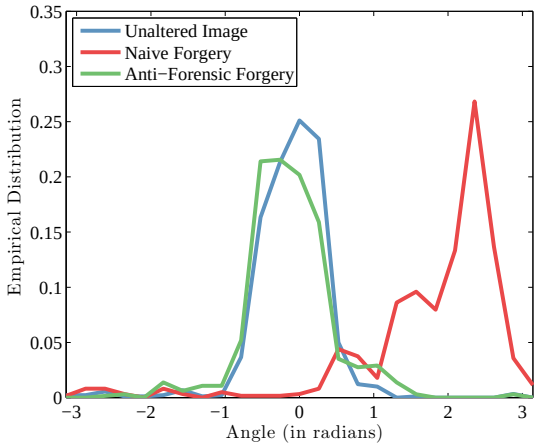
Figure 4. Green-to-red lateral chromatic aberration displacement field of (a) a naively constructed forgery and (b) an anti-forensically disguised forgery. Displacement vectors determined using the global model are shown in blue. Locally measured estimated displacement vectors are shown in green within the falsified region and red elsewhere. For display purposes, vectors have been scaled by a factor of 200.

a dashed line, and locally measured displacement vectors in this region are shown in green. We can easily see that in the falsified region of the naively constructed forgery, there are large angular errors between locally estimated displacement vectors and the global model. By contrast, in the falsified region of our anti-forensically modified image, the locally estimated displacement vectors closely match the globally estimated model. These results indicate that our anti-forensic attack can successfully prevent localized inconsistencies in the lateral chromatic aberration of cut-and-paste forgeries.

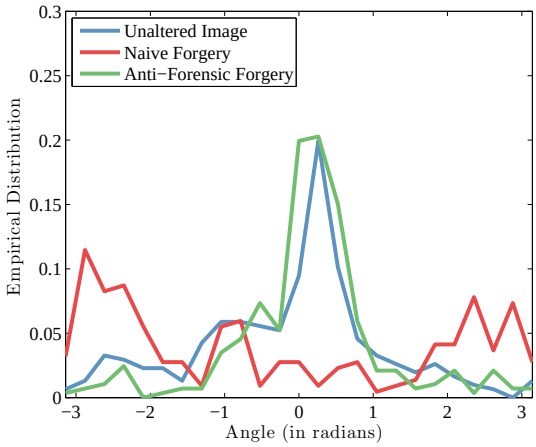
We used Johnson and Farid's technique to search each image in the set of anti-forensically disguised forgeries, naively constructed forgeries, and unaltered destination images for evidence of falsification by computing the angular error between the locally estimated displacement vectors and the global model. The errors were then aggregated and used to empirically estimate the distribution of angular errors within the paste region of each set of images. These distributions are shown in Fig 5. By examining this figure, we can clearly see a high occurrence rate of large angular errors in the paste region of the naively constructed forgeries. For forgeries constructed using our anti-forensic attack, large angular errors occur far less frequently. Furthermore, the distribution of angular errors in the set of anti-forensically disguised forgeries closely matches the distribution of angular errors in the set of unaltered images. This indicates that our anti-forensic attack can successfully fool Johnson and Farid's forgery detection technique.

To further verify this result, we statistically characterized the performance of Johnson and Farid's detector under our anti-forensic attack. This was done by classifying an image as a forgery if the angular error within the paste region exceeded a detection threshold. The detection threshold was varied over a range of values, and the results were recorded. The probabilities of detection P_D and false alarm P_{FA} were determined for each threshold by respectively calculating the percentage of forgeries that were correctly classified, and the percentage of unaltered destination images that were incorrectly classified. These results were used to generate the receiver operating characteristic (ROC) curves shown in Fig. 6.

In these ROC curves, the blue line represents the performance of a decision rule that randomly classifies an image as a forgery with probability P_{FA}, i.e. making a random guess. As we can see from Fig. 6, our anti-forensic attack is able to reduce the performance of Johnson and Farid's forgery detection technique to a similar or equivalent level for both the green-to-red and green-to-blue lateral chromatic aberration. Additionally, we used this data to compute the anti-forensic susceptibility of Johnson and Farid's detection technique to our anti-forensic attack. The anti-forensic susceptibility S_α is a measure of the decrease in effectiveness of a forensic detector caused by an anti-forensic attack.[14] A susceptibility of 1 indicates that the attack was able to render the

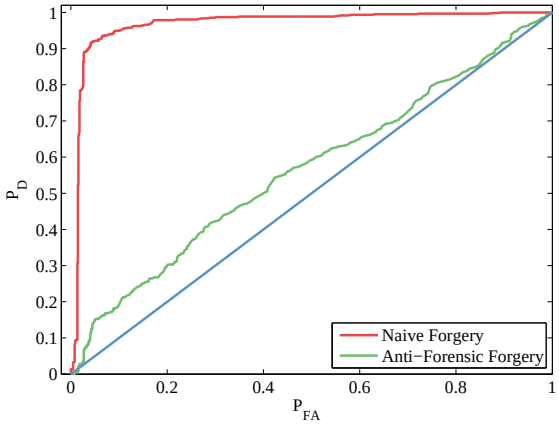


(a) Green-to-Red Angular Error Distribution

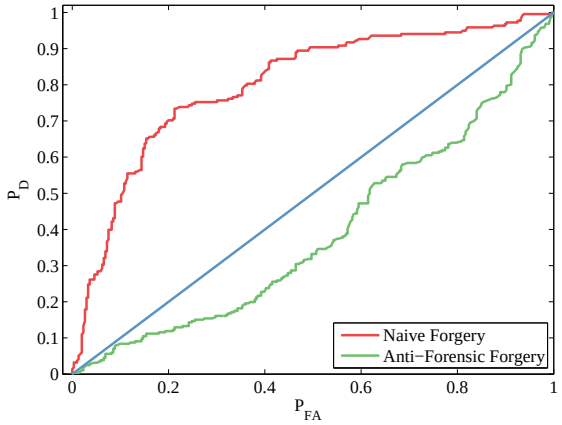


(b) Green-to-Blue Angular Error Distribution

Figure 5. Empirical estimates of the angular error distribution within the paste region of anti-forensically disguised forgeries, naively constructed forgeries, and unaltered destination images for (a) green-to-red and (b) blue-to-red lateral chromatic aberration measurements.



(a) Green to Red LCA



(b) Green to Blue LCA

Figure 6. Receiver operating characteristic curves for Johnson and Farid's copy-and-paste forgery detector when tested against naively constructed forgeries and anti-forensically disguised forgeries.

forensic technique completely ineffective, while a susceptibility of 0 indicates that the attack had no effect. Our results, which are shown in Fig. 7, show that Johnson and Farid's forensic technique was completely susceptible to our attack for green-to-blue lateral chromatic aberration, and susceptible with a rate of at least 0.8 for green-to-red lateral chromatic aberration. The results in Figs. 6 and 7 clearly show the success of our anti-forensic attack.

5. CONCLUSIONS

In this paper, we have propose an anti-forensic method to disguising lateral chromatic inconsistencies in copy-and-paste image forgeries. Our anti-forensic attack works by using a model to determine the expected lateral chromatic aberration of pixels in the image region where a copied object is to be pasted. Next, the image that the object is copied from is modified so that its lateral chromatic aberration within the object region matches the expected lateral chromatic aberration of the region of the image to where it will be pasted. Finally, the

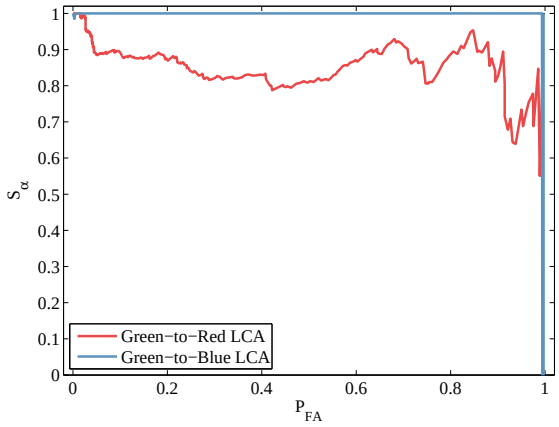


Figure 7. Plot of the anti-forensic susceptibility of Johnson and Farid's detector to our anti-forensic attack.

modified image is resampled along the pixel grid, and the object is copied and pasted into the target image. We demonstrated the effectiveness of this method by creating a series of anti-forensically falsified images, and demonstrated that their lateral chromatic aberration was indistinguishable from authentic images. Finally we demonstrated that our proposed anti-forensic attack can successfully fool the state-of-the-art forensic technique to detect copy-and-move forgeries using lateral chromatic aberration.

REFERENCES

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

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

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

[4] Wu, Z.-H., Stamm, M. C., and Liu, K. J. R., "Anti-forensics of median filtering," in [*Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*], 3043–3047 (2013).

[5] Barni, M., Fontani, M., and Tondi, B., "A universal technique to hide traces of histogram-based image manipulations," in [*Proceedings of the ACM Workshop on Multimedia and Security*], 97–104, ACM, New York, NY, USA (2012).

[6] Costanzo, A., Amerini, I., Caldelli, R., and Barni, M., "Forensic analysis of SIFT keypoint removal and injection," *IEEE Trans. on Information Forensics and Security* **9**(9), 1450–1464 (2014).

[7] Comesana-Alfaro, P. and Perez-Gonzalez, F., "Optimal counterforensics for histogram-based forensics," in [*Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*], 3048–3052 (2013).

[8] Gloe, T., Kirchner, M., Winkler, A., and Böhme, R., "Can we trust digital image forensics?," in [*Proc. Int. Conference on Multimedia*], 78–86, ACM, New York, NY, USA (2007).

[9] Kirchner, M. and Böhme, R., "Synthesis of color filter array pattern in digital images," in [*Proc. SPIE-IS&T Electronic Imaging: Media Forensics and Security*], **7254** (2009).

[10] Stamm, M., Lin, W., and Liu, K., "Temporal forensics and anti-forensics for motion compensated video," *IEEE Trans. on Information Forensics and Security* **7**(4), 1315 –1329 (2012).

[11] Johnson, M. K. and Farid, H., "Exposing digital forgeries through chromatic aberration," in [*Proceedings of the 8th Workshop on Multimedia and Security*], 48–55, ACM, New York, NY, USA (2006).

[12] Gloe, T., Borowka, K., and Winkler, A., "Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics," *Proc. SPIE-IS&T Electronic Imaging: Media Forensics and Security* **7541**, 754107–754107–13 (2010).

[13] Harris, C. and Stephens, M., "A combined corner and edge detector.," in [*Alvey vision conference*], **15**, 50 (1988).

[14] Stamm, M., Lin, W., and Liu, K., "Anti-forensics for frame deletion/addition in MPEG video," in [*Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*], 1749–1752 (Mar. 2012).