Forensic Detection of Digital Image Tampering Using Statistical Analysis

Md. Zahurul Haque
Department of Computer Science and Engineering
Jahangirnagar University
Dhaka, Bangladesh
jahurulhaque@manarat.ac.bd

Md Mahedi Hasan
Institute of Information and Communication Technology
Bangladesh University of Engineering and Technology
Dhaka, Bangladesh
mahedi0803@gmail.com

***Abstract*- Today, with an increasing volume of images being captured across an ever expanding range of devices, digital images are now ubiquitous in modern life. In parallel to advances in technology, we have socially come to understand events in a far more visual way than ever before. Digital images are now primary source of information in a wide range of fields from entertainment to mass media, from medical diagnosis to criminal justice, and even national security. This dependence on digital images, however, has brought with it a whole new set of issues and challenges which were not as apparent before. Due to the availability and increasing sophistication of advanced photo-editing software, there is a rampant problem of digital forgeries, which has seriously debased the credibility of digital images as definite records of events. As a consequence, doctored images are now appeared with a growing frequency in different application fields often leaving no visual clues of having been tampered with. On the other hand, for this reason digital image forensics has emerged as a new research field that aims to reveal tampering operations in digital images and to verify images authenticity. One of the primary goals of digital image forensics is to identify images and image regions which have undergone some form of manipulation or alteration. Because of the ill-posed nature of this problem, no catchall method of detecting image forgeries exists. Instead, a number of techniques have been proposed to identify image alterations under a variety of scenarios. But each of these methods possess their own limitations. This paper presents a comprehensive overview of the state of the art in the area of digital image forensics. An efficient statistical technique have also been presented for detecting region duplication, one of the most common forgeries on digital image.**

Keywords: **digital image, image Forgeries, image tempering.**

I. INTRODUCTION

The advent of low-cost and high-resolution digital cameras, and sophisticated photo-editing software, has made it remarkably easy to Control and alter digital images. Again, current software allows to create photorealistic computer graphics that viewers can find indistinguishable from photographic images [6, 7] or also creates hybrid generated visual content. Therefore, there is a great need for digital image forensic technique capable of detecting sophisticated image alterations.

The basic concept of image forgery is the digital manipulation of images with the aim of distorting some information in these images. For example, let us consider the creation of a digital forgery that shows a pair of famous movie stars, rumored to have a romantic relationship, walking hand-in-hand. Such a picture must be created by splicing together individual images of each movie star and overlaying the digitally created composite onto a sunset beach. In order to create a convincing match, it is often necessary to (1) re-size, rotate, or stretch portions of the image; (2) apply luminance non-linearity (e.g., gamma correction) to portions of the image in order to adjust for brightness differences; (3) copy and move in the same image or cut and paste in different image (4) add small amount of noise to conceal the evidence of tampering; and (5) re-save the final image (typically with lossy

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

compression such as JPEG). Although these manipulations are often imperceptible to the human eye, they may introduce specific correlations into the image. By detecting these correlations, they can be used as evidence of digital tampering.

Image forensic methods can be divided into only two simple categories: *semantics-based detection* and *non-semantics-based detection*. A majority of existing detection methods belong to *non-semantics-based* category where the statistical pattern in the image is first modeled and then the inconsistencies in this pattern are inspected across the image to search for clues of tampering. The basic assumption of these image-forensic methods is that images possess certain regularities, or invariant, that are disturbed by tampering. These invariant are often difficult to create synthetically and invisible to the inexperienced observer. Although tampering may not affect the image quality, changes to invariant are often measurable.

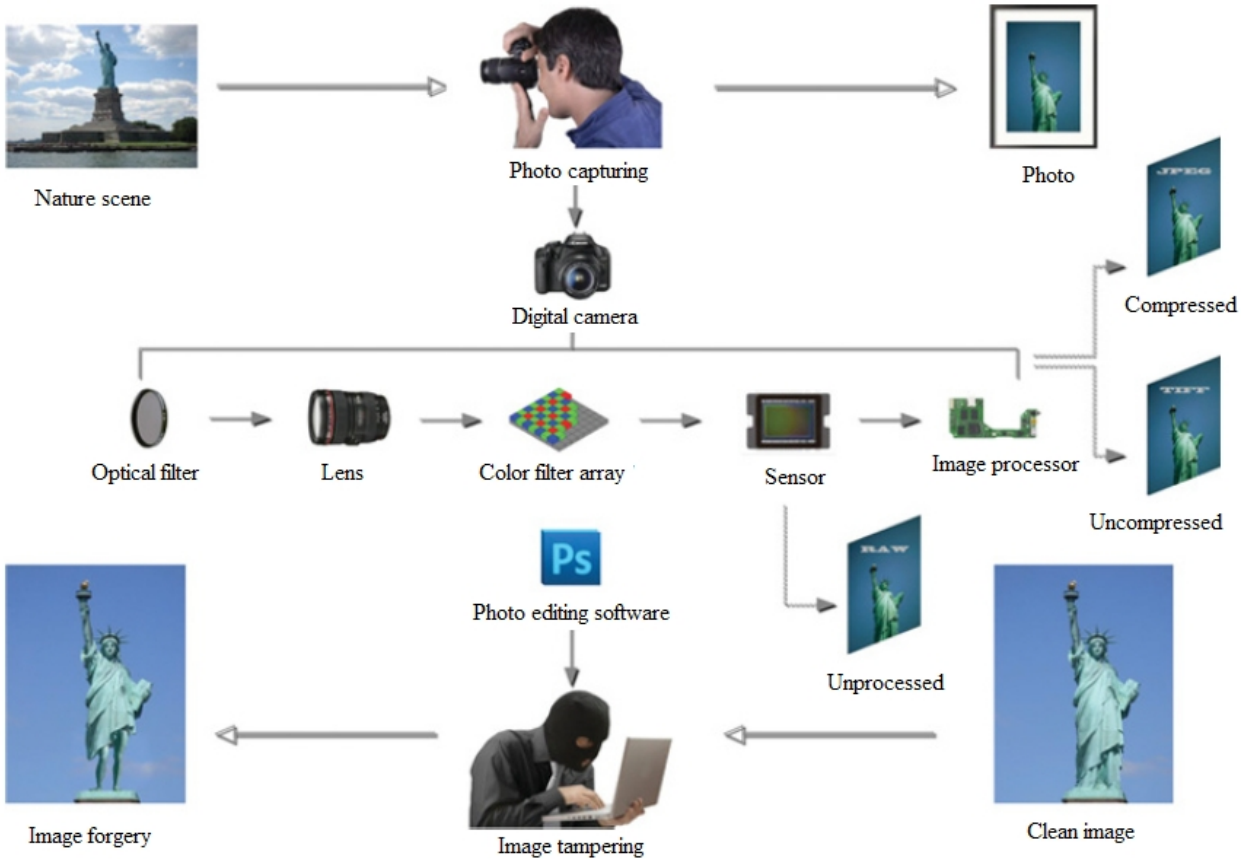

Figure 1: The procedure of making image forgery.

In this paper, statistical correlations result from most common digital forgery copy and move within the same image is determined. Finally a detection schemes is devised to reveal the correlations. The effectiveness of this technique is shown on a number of simple synthetic examples and on perceptually credible forgeries.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. Related Work

Previous image forensic work has mostly dealt with the identification of computer-generated objects within an image [8] as well as detecting lighting angle inconsistencies [9, 10]. Inconsistencies in aberration [11] also because the absence of color filter array (CFA) interpolation-induced correlations [12] are wont to identify inauthentic regions of a picture. Classifier based approaches have been proposed which identify image forgeries using a variety of statistical features [13-15]. Though these techniques are capable of detecting that a picture has undergone some sort of manipulation, they're unable to work out how a picture has been altered beyond the identification of manipulated image regions.

Active protection methods such as digital watermarking and signature also served as major solutions to protect the integrity of digital images. Active methods are based on the idea of a trustworthy camera [16, 17], proposed in the past as a way to grant the authenticity of digital images. A trustworthy camera computes a digital watermark [18–20] or a digital signature [21, 22] from the image at the instant of its acquisition. Any later modification of the image are often detected by checking the worth of the digital watermark or digital signature at the instant of its fruition. A major drawback of these solutions is that digital cameras are specially equipped with a watermarking a digital signature chip that, exploiting a private key hard-wired in the camera itself, authenticates every image the camera takes before storing it on its memory card. The implementation of a trustworthy camera would require the manufacturers to define a standard protocol. This requirement is too hard to be satisfied. Moreover, most digital imaging devices currently on the market lack watermarking or signature modules.

To overcome these problems, recently several methods for authenticating the contents of digital images have evolved. The purpose of this method is to verify the authenticity of the digital images with no prior knowledge and thus it is defined as passive. The passive methods of image tampering detection are more practical than active methods because they operate in the absence of any watermark or signature. These methods work on the idea that although digital forgeries may leave no visual clues that indicate tampering, they'll alter the underlying statistics of a picture.

It is also important to note that most image altering operations leave behind distinct, traceable “fingerprints” in the form of image alteration artifacts. Because these fingerprints are often unique to every operation, a private test to catch each sort of image manipulation must be designed. While detecting image forgeries using these techniques requires performing a large set of operation-specific tests, these methods are able to provide insight into the specific operation used to manipulate an image. Prior work which identifies image tampering by detecting operation-specific fingerprints includes the detection of re-sampling [23], double JPEG compression [24-26], as well as the parameterization of gamma correction [27]. Methods for detecting image forgeries have been proposed by detecting local abnormalities in an image’s signal-to-noise ratio (SNR) [24]. Additionally, the efficient identification of copy and move forgeries has been studied [28].

III. Types of Digital Image Forgery

Image editing means any processing applied to the digital image. There are many different reasons for modifying an image: the objective could be, for example, to improve its quality or to change its semantic content. In the former

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

case, the processed image will carry the same information as the original one, but in a more pleasant way. Hence, this kind of editing is known as "innocent." Conversely, in the latter case, the semantic information conveyed by the image is changed, usually by adding or hiding something. This kind of editing is known as "malicious".

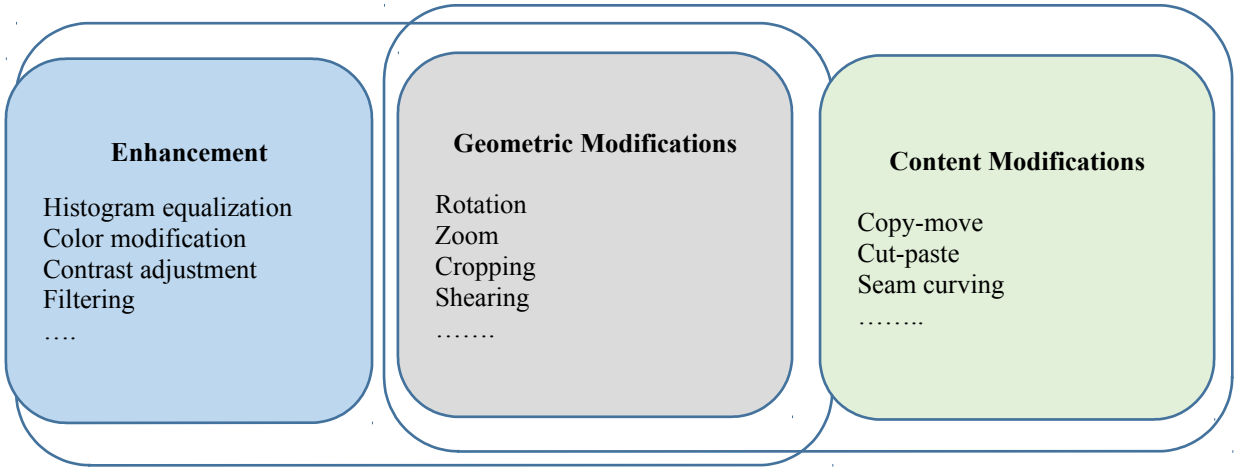

Figure 2: Different types of editing operations applicable to digital images.

Figure 2 provides a simple classification of three categories of editing operations, along with some examples for each identified class. Concerning malicious modifications, the most important are surely the copy-move attacks and cut-and-paste attacks.

Copy-move is one of the most studied forgery techniques. It consists in copying a portion of an image (of arbitrary size and shape) and pasting it in another location of the same image. Clearly, this technique is useful when the forger wants either to hide or duplicate something that is already present in the original image.

Cut-and-paste or splicing, is the other important image forgery technique: starting from two images, the attacker chooses a region of the first and pastes it on the second, usually to alter its content and meaning. Splicing is probably more common than copy-move, because it is far more flexible and allows the creation of images with a very different content with respect to the original.

In *Image Re-sampling* in order to create a high quality forged image, some selected regions have to undergo geometric transformations like rotation, scaling, stretching, skewing, flipping etc. The interpolation step plays a central role in the re-sampling process and introduces non-negligible statistical changes. Nevertheless, it is also introduces some specific periodic correlations into the image.

IV. Detecting Region Duplication Forgery

In this paper a recently developed technique as proposed by literature [2] is introduced to address region duplication forgery, one of the most critical task in digital image forensic. This technique is based on an efficient region duplication detection algorithm which is robust to distortions of the duplicated regions. This method detect image forgeries based on the assumption that most digital manipulations will disturb some statistical property of an image.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

A. Problem Definition

A common manipulation in tampering with digital image is known as *region duplication*. It is a simple and effective operation to create digital image forgeries, where a continuous portion of pixels in an image, is copied and pasted to a different location in the same image, after possible geometric and illumination adjustments.

B. Existing Methods

A majority of recently developed methods directly find exact duplicated copies of small-pixel blocks in an image. Though the front-end linear image domain is mostly on pixels, some specific image representation schemes such as wavelet [29], bit-plane decomposition [30], and multi-scale decomposition are also used. Since a brute-force match of all pixel blocks of a given size in an image has a running time quadratic in the size of the image, therefore to overcome this complexity, low dimensional representation of pixel blocks are employed for efficient computation, for example principal component analysis (PCA) [31], DCT [32] and singular value decomposition (SVD) [33]. A common step used in these methods is to lexicographically sort pixel blocks so that identical blocks end up as adjacent pairs in the sorted list. Recently, kd-tree [34] and hashing-based Bloom filter [35] techniques have been proposed to further speed up the sorting process.

However, in practice, copy–move alone can seldom create plausible forgeries. More likely, as in the example of figure [3], the duplicated regions are subjected to geometric and illumination transforms to be better blended into the surroundings at the target location. As such distortions alter the correspondence between pixels in duplicated regions, straightforward matching of blocks of pixels or transform coefficients computed from the pixel values becomes much less effective.

C. Proposed Method

Region duplication can be formalized as a 2D linear transform between image regions. Let us denote pixel locations in the source region and its duplication as Ω_S and Ω_T, respectively. Now, assuming only gentle changes in the pixel intensities in tampering the image I, region duplication leads to $I(\Omega_T) \approx I(T(\Omega_S))$, where T is a linear *manipulation transform* including translation, rotation, scaling, perspective and their combinations. Therefore, detecting region duplication involves recovering Ω_S and Ω_T, along with the manipulation transform T.

To find these parameters [3] proposed a region duplication method whose key steps are:-

1. RGB images are converted to greyscale images since the duplicated regions are detected in the illumination domain.
2. Key points are detected in the input image using a local image feature description algorithm, where feature vectors are collected. Initial matching of key points are made based on the similarity between the feature vectors.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure 3: (Left) Original un-tampered images. (Right) Forgeries created with region duplication (image courtesy: (top) from literature [31] and (bottom) from literature [37]).

3. The initial matching of key points are then refined iteratively with the robust RANSAC estimation [36], after which only reliable correspondences between key points are kept. Further an affine transform between the two corresponding sets of key points are estimated.

4. Two correlation maps are generated, which contain the correlation coefficients of each pixel with its correspondences obtained with the estimated affine transform and its inverse to a pair of duplicated regions.

5. All pixels corresponding to the duplicated regions are found by thresholding the correlation maps. The results are further merged, filtered and smoothed to obtain location and extent of the detected duplicated regions.

The primary step in proposed method is to find image key points and collect image features at the detected key points. One of the most effective key point and feature computation algorithms is known as the *scale-invariant feature transform* (SIFT) [38]. The SIFT key points are found by searching for locations that are stable local extreme in the scale space [39]. At each key point, a 128-dimensional feature vector is generated from the histogram of local gradients in its neighborhood. To ensure that the obtained feature vector is invariant to rotation and scaling, the size of the neighborhood is determined by the dominant scale of the key point, and all gradients within are aligned with the key point's dominant orientation. Furthermore, the obtained histograms are normalized to unit length, which renders the feature vector invariant to local illumination changes [38]. The detected SIFT key points are then tentatively matched based on their feature vectors using the *best-bin-first* algorithm [40].

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

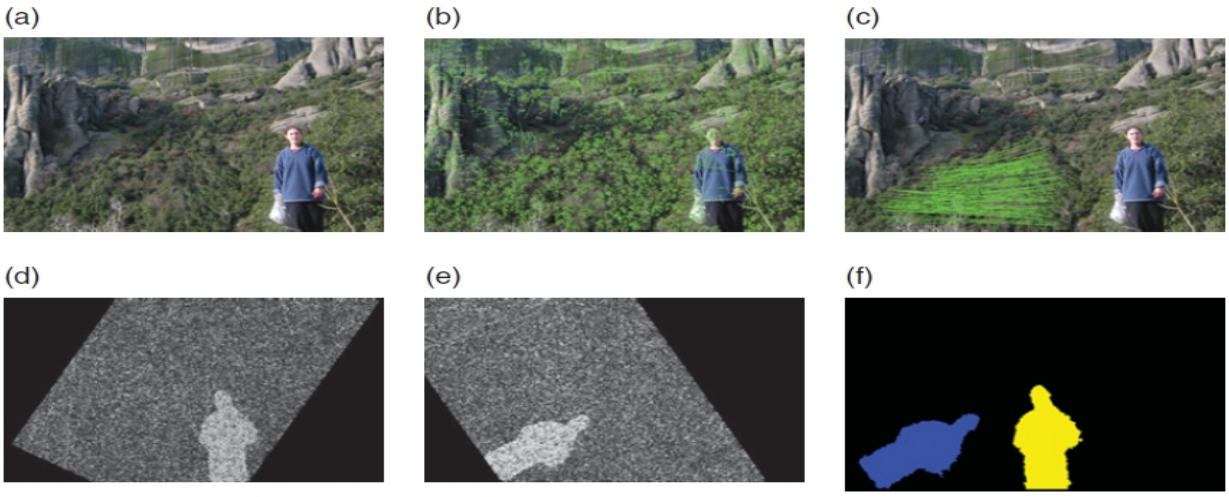

Figure 4. (a) An tampered image with region duplication forgery. (b) Detected SIFT key points in the image. (c) Matched key points after the RANSAC algorithm. (d and e) region correlation maps generated with the estimated affine transforms. Brighter pixel intensity signifies stronger correlation. (f) Detected duplicated regions.

The second step is to get the geometric transform between the duplicated regions which can be modeled as affine transform of pixel coordinates. Given two corresponding pixel locations from a region and its duplicate as $\vec{x} = (x, y)^T$ and $\vec{\tilde{x}}_i = (\tilde{x}, \tilde{y})^T$, respectively, they are related by a 2D affine transform specified by a 2 ×2 matrix T and a shift vector $\vec{x}_0$.

$$\begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = \begin{pmatrix} t11 & t12 \\ t21 & t22 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \tag{1}$$

To obtain a unique solution to the unknowns, (t_{11}, t_{12}, t_{21}, t_{22}, x_0, y_0), at least three pairs of corresponding key points are required that are not *collinear*. In practice, due to imprecise matching, (1) may not be satisfied exactly. Therefore the *least squares* objective function using matched key points is formed as follows

$$L(T, \vec{x}_0) = \sum_{i=1}^{N} \left\| \vec{\tilde{x}}_i - T\vec{x}_i - \vec{x}_0 \right\|_2^2, \tag{2}$$

To prune out unreliable key point correspondences and obtain accurate transform parameters simultaneously, a widely used robust estimation method known as the *random sample consensus* (RANSAC) algorithm [36] is used. The main advantage of RANSAC matching algorithm is that it can estimate the model parameters with a high degree of accuracy even when a significant number of mismatched pairs are present. Using the initial matching of SIFT key points, the following two steps is run N times:

1. Randomly select three or more pairs of matched key points that are not collinear. Using the chosen pairs of key points, estimate T and shift vector $\vec{x}_0$ by minimizing the objective function given in (2).

2. Using the estimated T and , classify all pairs of matched SIFT key points into *inliers* or *outliers*.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

The RANSAC algorithm returns the estimated transform parameters that lead to the largest number of inliers. According to experiments done in literature [2] default values for N = 100 and β = 3 lead to better empirical performance. With the estimated affine transform, each pixel is compared to its transformation to find identical regions. In practice, because the estimated affine transform can be the inverse of the actual transform (from pixel level, it is not possible to differentiate which region is the source and which one is the duplicate), the correspondence of $\vec{x}$*is checked* using both the estimated affine transform, $\vec{x}_f = T(\vec{x} + \vec{x}_0)$and its inverse $\vec{x}_b = T^{-1}(\vec{x} - \vec{x}_0)$

Taking the forward transform as example, the similarity between $\vec{x}$ and $\vec{x}_f$is evaluated with the *correlation coefficients* between the pixel intensities within small neighboring areas of each location. Denoting the pixel intensity at location $\vec{x}$ as $I(\vec{x})$, and $\Omega(\vec{x})$ as the 5 × 5 pixels neighboring area centered at $\vec{x}$, the correlation coefficient between the two pixel locations is computed as follows.

$$c_{f(\vec{x})} = \sum_{\vec{s} \in \Omega(\vec{x}), \vec{t} \in \Omega} ¿¿ \quad (3)$$

The correlation coefficient for the inverse transformed $\vec{x}_b$is computed in a similar manner. The correlation coefficient is in the range of [0, 1], with larger value indicating higher level of similarity. Further, it is invariant to local illumination distortions. Any illumination changes consistent within the local neighborhood will cancel out each other. The computed $c_f(\vec{x})$ and $c_b(\vec{x})$ are placed into correlation maps, shown in figures 4(d and e). The correlation maps are then smoothed and merged to obtain the duplicated regions.

D. Performance Analysis

To evaluate the performance of the proposed algorithm, literature [2] created a set of automatically generated forged images with duplicated and distorted regions. Forged images were generated based on 25 uncompressed PNG true color images of size 768 × 512 pixels [41]. It also introduce two quantitative measures to evaluate the performance of proposed method. Let us denote Ω as pixels in the true duplicated regions and $\widetilde{\Omega}$ as pixels in the detected duplicated regions,

Pixel detection accuracy (PDA) rate: The fraction of pixels in duplicated regions that are correctly identified, as

$$\text{PDA} = ¿\widetilde{\Omega} \cap \Omega \vee \frac{¿}{¿\Omega \vee ¿¿} ¿$$

Pixel false positive (PFP) rate: The fraction of pixels in unhampered regions that are detected as from duplicated regions, as $\text{PFP} = ¿\widetilde{\Omega} - \Omega \vee \frac{¿}{¿\widetilde{\Omega} \vee ¿¿} ¿$

For comprehensive performance evaluation, any region duplication detection method must consider both the PDA and the PFP rates. Good algorithm should detect as many as possible pixels in the duplicated regions. On the other hand, it should reduce the number of pixels in unhampered regions that are detected as from duplications. In proposed method, PDA/PFP rates can be manipulated by adjusting the correlation threshold c. The trade-offs

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

between the PDA and PFP rates are completely described with the *receiver-operator characteristics* (ROC) curve. To generate the ROC curves, [2] produced different PDA/PFP rates by changing the threshold in the correlation map c in the range of [0.00 – 0.95] with step size 0.05.

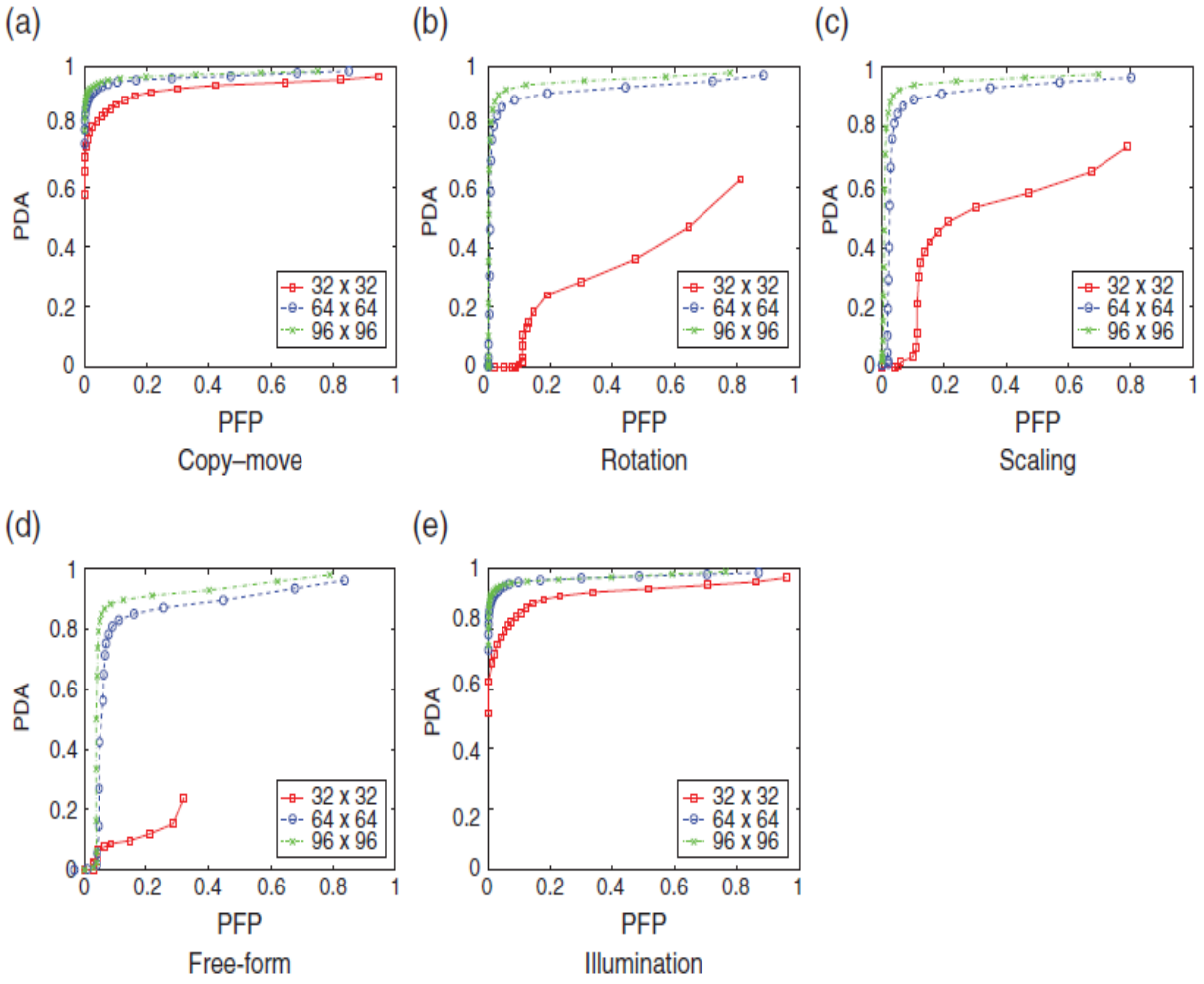

Figure 5: ROC curves of different tampering operations and different block sizes. Results are averaged over 100 randomly synthesized forgeries with region duplications.

V. Experiments

Figure 6 illustrates the effectiveness of proposed forgery detection method for solving some real-word problems. Forged images in the first two rows are generated with the splicing algorithm developed by literature [20], which creates a natural transition between duplicated region and the surroundings at the target location. In the "deer" image, the duplicated region is rotated, scaled and mirrored. In the "cherry" image, the duplicated region is rotated and overlapped with the source region.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

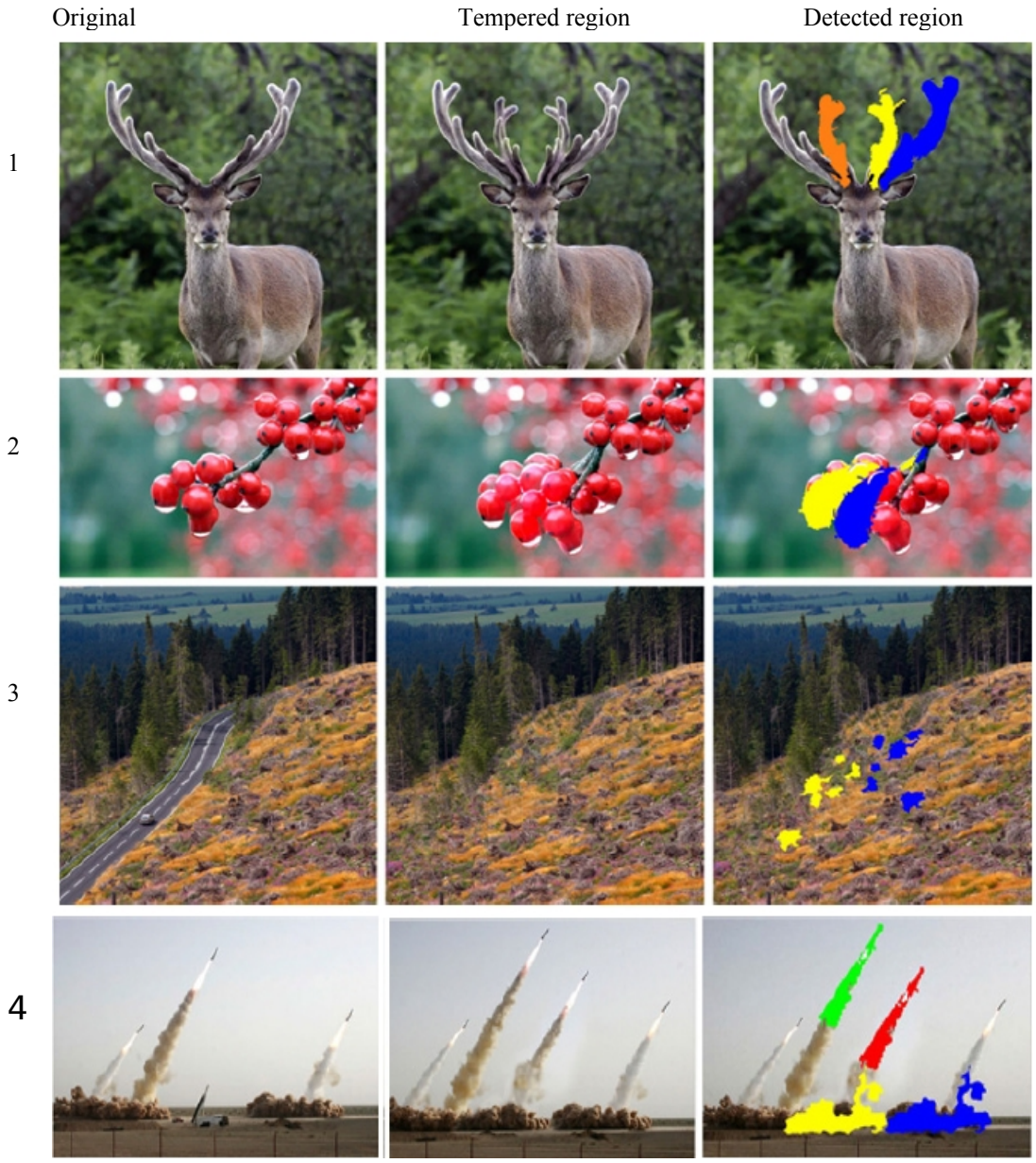

Figure 6: Detection results of the proposed method for a set of more challenging forgeries. Colors are added to differentiate the regions detected by the introduced method as duplicates of each other.

The third row shows a forgery created with the *Smart Fill* tool in the Image Doctor 2 software (Alien Skin Software LLC 2007). An unpublished algorithm was used to create this forgery which is more sophisticated; instead of using a continuous duplicated region of relatively large size, smaller regions containing mostly textures are combined and arranged to cover larger region at the target location. The image shown in the fourth row appeared on the front pages of several internationally recognized newspapers as well as several major news websites in 2008. Shortly after this image was published, doubts were raised regarding its authenticity. The introduced method is able to recover the two major regions that are believed to have been duplicated from other parts of the image.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. CONCLUSIONS

The advent of low-cost and high-resolution digital cameras, and sophisticated photo-editing software, has made it remarkably easy to regulate and alter digital images. These digital forgeries, by misleading our perception, have an increasingly negative social impact. They are much more vulnerable compared to their non-digital counterparts. The most simple and effective operation to create digital image forgeries is copy-move or region duplication. Most existing region duplication detection methods are based on directly matching blocks of image pixels or transform coefficients, and are not effective when the duplicated regions have geometric or illumination distortions. In this paper an efficient region duplication detection method is described which is robust to distortions of the duplicated regions. This method starts by estimating the transform between matched SIFT key points, which are insensitive to geometric and illumination distortions, and then finds all pixels within the duplicated regions after discounting the estimated transforms. This method shows effective detection results on an automatically synthesized forgery image database with duplicated and distorted regions.

ACKNOWLEDGMENT

This paper is based on the work of first 5 papers entitled in references. I am very much grateful to them. Since the paper is not written for any official submission, no permission is taken for using those forged images.

REFERENCES

[1] M. C. Stamm and K. J. Ray Liu, "Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints" in *IEEE Transactions on Information Forensics and Security* (Volume: 5, Issue: 3, Sept. 2010)

[2] "*Handbook of Digital Forensics of Multimedia Data and Devices*", first edition, edited by Anthony T.S. and Shujun Li., published 2015 by John Wiley & Sons Ltd.

[3] A. Piva, "An overview on Image Forensics", *ISRN signal processing*, vol. 2013, 2013.

[4] Hailing Huang, Weiqiang Guo, Yu Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm" *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008*

[5] M. Ali Qureshi, M.Deriche "A Review on Copy Move Image Forgery Detection Techniques" in 11th International Multi-Conference *on Systems, Signals & Devices (SSD)*, 2014

[6] G. W. Meyer, H. E. Rushmeier, M. F. Cohen, D. P. Greenberg, and K. E. Torrance, "An experimental evaluation of computer graphics imagery," *ACM Transactions on Graphics*, vol. 5, no. 1, pp. 30–50, 1986.

[7] "Fake or foto," 2012, http://area.autodesk.com/fakeorfoto.

[8] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M. P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics," in *Proc. ACM Multimedia*, Singapore, 2005, pp. 239–248.

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

[10] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in *Proc. ACM Multimedia and Security Workshop*, New York, NY, 2005, pp. 1–10.

[11] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in *Proc. ACM Multimedia and Security Workshop*, Geneva, Switzerland, 2006, pp. 48–55.

[12] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Trans. Signal Process.* vol. 53, no.10, pp. 3948–3959, Oct. 2005.

[13] T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in *Proc. IEEE Int. Symp. Circuits Systems*, Vancouver, BC, Canada, May 2004, vol. 5, pp. V-688–V-691.

[14] S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," *J. Electron. Image.*,vol. 15, no. 4, p. 041102, 2006.

[15] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, "A classifier design for detecting image manipulations," in *Proc. ICIP*, Oct. 2004, vol. 4, pp. 2645–2648.

[16] G. L. Friedman, "Trustworthy digital camera: restoring credibility to the photographic image," *IEEE Transactions on Consumer Electronics*, vol. 39, no. 4, pp. 905–910, 1993.

[17] P. Blythe and J. Fridrich, "Secure digital camera," in *Proceedings of the Digital Forensic Research Workshop (DFRWS '04)*, pp. 17–19, 2004.

[18] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2001.

[19] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*, Signal Processing and Communications, Marcel Dekker, 2004.

[20] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Water—Marking and Steganography*, Morgan Kaufmann, San Francisco, Calif, USA, 2nd edition, 2008.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications*

of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
[22] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Fla, USA, 1st edition, 1996.
[23] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Trans. Signal Process.*, vol. 53, pp. 758–767, Feb. 2005.
[24] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proc. 6th Int. Workshop on Information Hiding*, Toronto, Canada, 2004,pp. 128–147.
[25] T. Pevný and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 247–258, Jun. 2008.
[26] J. Luká˘s and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. Digital Forensic Research Workshop*, 2003, pp. 5–8.
[27] H. Farid, "Blind inverse gamma correction," *IEEE Trans. Image Process.*, vol. 10, pp. 1428–1433, Oct. 2001.
[28] J. Fridrich, D. Soukal, and J. Luká˘s, "Detection of copy-move forgery in digital images,"
[29] Myna AN, V. MG and Patil CG 2007 Detection of region duplication forgery in digital images using wavelets and log-polar mapping. *ICCIMA '07: Proceedings of the International Conference on Computational Intelligence and Multimedia Applications*. IEEE Computer Society, Washington, DC, pp. 371–377.
[30] Ardizzone E and Mazzola G 2009 Detection of duplicated regions in tampered digital images by Bitplane analysis. *ICIAP '09: Proceedings of the 15th International Conference on Image Analysis and Processing* Springer-Verlag, Berlin, Germany, pp. 893–901.
[31] Popescu A. and Farid H., "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515. Department of Computer Science, Dartmouth College, Hanover, NH. 2004
[32] Fridrich J, Soukal D and Lukas J "Detection of copy-move forgery in digital images" *Digital Forensic Research Workshop*, Cleveland, OH. 2003
[33] Li G, Wu Q, Tu D and Sun S 2007 A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. *ICME*, Beying, China, pp. 1750–1753.
[34] Mahdian B and Saic S 2007, "Detection of copy-move forgery using a method based on blur moment Invariants" *Forensic Science International* **17**(2–3) 180–189.
[35] Bayram S, Taha Sencar H and Memon N 2009 An efficient and robust method for detecting copy-move forgery. *IEEE International Conference on Acoustics, Speech and Signal Processing*, Washington, DC.
[36] Fischler MA and Bolles RC 1981 Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography. *Communications on ACM* 24(6), 381–395
[37] Farbman Z, Hoffer G, Lipman Y, Cohen-Or D and Lischinski D 2009 Coordinates for instant image cloning. *ACM Transaction on graphics* 28(3), 1–9.
[38] Lowe D 2004 Distinctive image features from scale-invariant keypoints. *IJCV* 60(2), 91–110.
[39] Lindeberg T 1994 "*Scale-Space Theory in Computer Vision*" Kluwer Academic Publishers, Dordrecht, the Netherlands.
[40] Beis J and LoweD1997 Shape indexing using approximate nearest-neighbor search in high-dimensional spaces. *CVPR* San Juan, Puerto Rico, pp. 1000–1006.
[41] Franzen R 1999 Kodak lossless true color image suite source. http://r0k.us/graphics/kodak. Accessed on 31 January 2015.