INTERNAL AND EXTERNAL FORGERY DETECTION OF IMAGE USING RECTANGULAR PROJECTION MODEL

Deepa, P.[1] & Mishmala Sushith (Associate Prof.)[2]
[1].CSE-dept,Kalignar Karunanidhi Institute of Technology, Anna university, Coimbatore, Tamil Nadu
[2.] IT-dept,Kalignar Karunanidhi Institute of Technology, Anna university, Coimbatore, Tamil Nadu
INDIA

ABSTRACT

In this work a decision fusion strategy for image forensics is presented, based Rectangular Projection Model on Theory of Evidence. The goal is to automatically review the information provided by several image forensics tools, allowing both a binary and a soft interpretation of the global output produced. The proposed strategy is easily extendable to an arbitrary number of tools, it does not require that the output of the various tools be probabilistic and it takes into account available information about tools reliability. The proposed framework exploits knowledge about tool performances and about compatibility between various tool responses, and can be easily extended when new tools become available. It allows both a “soft” and a “binary” (tampered/non tampered) interpretation of the fusion result, and can help in analyzing images for which taking a decision is critical due to convicting data. Our proposed system works in finding the copy past forgery of newly added object to the actual image wherein a region from an image is replaced with another region from the different image. The previous methodologies in finding identical regions suffer from their inability to detect the cloned region when it has been subjected to a geometric transformation. The proposed system works on distortion based features. These are obtained by using the features from the image.

Keywords: Binary, Soft Interpretation, Rectangular, Distortion, Image Forgery, MPEG-7.

INTRODUCTION

The digital information revolution and issues concerned with multimedia security have also generated several approaches to tampering detection [3]. Generally, these approaches could be divided into *active and passive–blind approaches*. The area of active methods simply can be divided into the data hiding approach and the digital signature approach. The area of blind methods tries to verify the integrity of digital images and detect the traces of tampering without using any protecting pre–extracted or pre–embedded information [11]. This area is regarded as a new direction and is growing noticeably. Number of published papers is growing and results obtained promise a significant improvement in forgery detection. Geometric transformations such as scaling or rotation are common tools employed by forgery creators [14, 22]. There are two basic steps in geometric transformations [17]. In the first step a spatial transformation of the physical rearrangement of pixels in the image is done. Coordinate transformation is described by a transformation function which maps the coordinates of the input image pixel to the point in the output image (or vice versa). The second step in geometric transformations is called the interpolation step. Here pixels intensity values of the transformed image are assigned using a constructed low–pass interpolation filter [16]. To compute signal values at arbitrary locations, discrete samples are multiplied with the proper filter weights when connecting them with w. This step brings into the image detectable periodic properties. We will be concerned mainly with following low–order piecewise local polynomials: nearest–neighbor, bilinear and bicubic. These polynomials are used extensively because of their simplicity and implementation unassuming properties. We analytically show periodic properties present in the covariance structure of interpolated

signals. Furthermore, we briefly show a blind method [2] capable of detecting the traces of interpolation. The method is a modified version of14 and is based on a set of derivative filters and radon transformation. Modifications are done in order to achieve the main goal of this paper. Our aim is to analyze how helpful is method in detecting and describing all geometric transformations present in the image [14,17]. In other words, for example, when an image has undergone both a dominant geometric transformation and a minor geometric transformation, we would like to detect both of them and generate suitable data for describing them (resizing factors and rotation angles) [14]. While we may have historically had confidence in the integrity of this images, today's digital technology has begun to erode this trust[1].In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature[16,18]. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories:

1) **pixel-based techniques** [1] that detect statistical anomalies introduced at the pixel level;
2**) format-based techniques** *[2]* that leverage the statistical correlations introduced by a specific lossy compression scheme;
3) **camera-based technique s**[3] that exploit artifacts introduced by the camera lens, sensor, or on-chip postprocessing;
4**) Physically based techniques** [4] that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera;
5**) geometric-based techniques** [1] that make measurements of objects in the world and their positions relative to the camera.

ARCHITECTURAL DIAGRAM

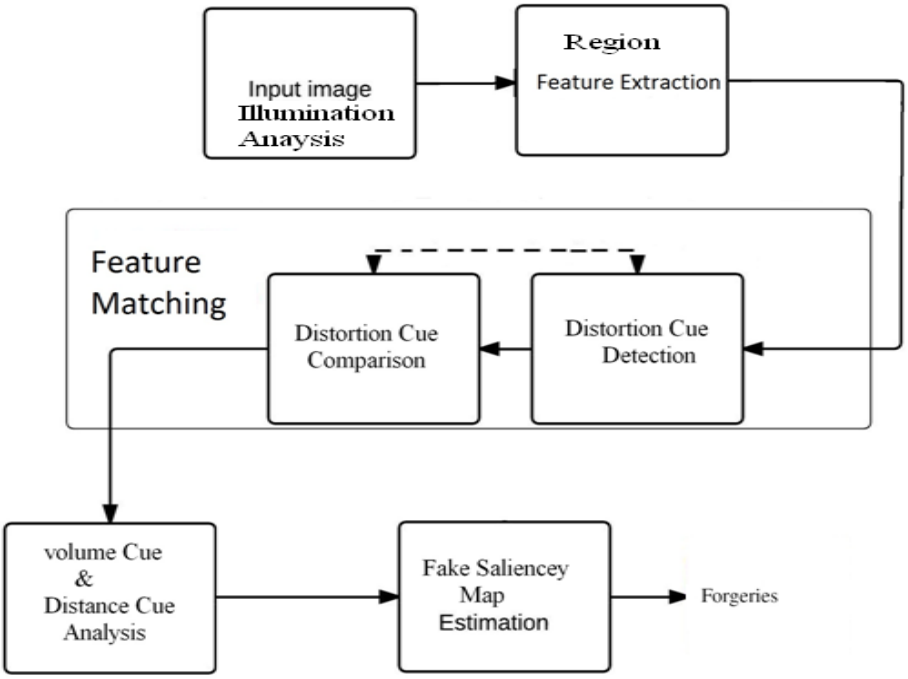

Fig (a): proposed architectural diagram

MATERIALS AND METHOD

Pixel-Based

The legal system routinely relies on a range of forensic analysis ranging from forensic identification (DNA or fingerprint) [23], to forensic deontology (teeth), forensic entomology (insects), and forensic geology (soil). In the traditional forensic sciences, all manner of physical evidence are analyzed. In the digital domain, the emphasis is on the pixel – the underlying building block of a digital image. It was described four techniques for detecting various form of tampering, each of which directly or indirectly analyzes pixel-level correlations that arise from a specific form of tampering.

Cloning

Perhaps one of the most common image manipulations is to clone (copy/paste) portions of the image to conceal a person or object in the scene. When care is taken it can be difficult to visually detect cloning. And, since the cloned regions can be of any shape and location, it is computationally impossible to search all possible image locations and sizes. Two computationally efficient algorithms have been developed to detect cloned image regions .The authors in first apply a block Discrete Cosine Transform (DCT)[13]. Duplicated regions are detected by lexicographically sorting the DCT block coefficients, and grouping similar blocks with the same spatial offset in the image. In a related approach, a principal component analysis (PCA) on small fixed-size image blocks to yield a reduced dimension representation. Duplicated regions are again detected by lexicographically sorting and grouping all of the image blocks [12]. In both cases, the DCT and PCA representation are employed to reduce computational complexity, and so that the clone detection is robust to minor variations in the image due to additive noise or lossy compression [14, 23].

Re-Sampling

In order to create a convincing composite, it is often necessary to re-size, rotate, or stretch portions of an image [18]. For example, when creating a composite of two people, one person may have to be re-sized to match the relative heights. This process requires re-sampling the original image onto a new sampling pattern, introducing specific periodic correlations between neighboring pixels. Because these correlations are unlikely to occur naturally, their presence can be used to detect this specific manipulation Consider the simple example of up-sampling a 1-D signal x(t) of length m by a factor of two using linear interpolation to yield y(t). The odd samples of the re-sampled signal take on the values of the original signal: $y(2i - 1) = x(i)$, $i = 1, \ldots, m$, while the even samples are the average of adjacent neighbors of the original signal:

$y(2i) = 0.5x(i) + 0.5x(i + 1)$. (1) Since each sample of the original signal can be found in the re-sampled signal, the interpolated pixels can be expressed in terms of the re-sampled samples only: $y(2i) = 0.5y(2i - 1) + 0.5y(2i + 1)$. (2) That is, across the entire re-sampled signal, each even sample is precisely the same linear combination of its adjacent two neighbors. In this simple case a re-sampled signal can be detected by noticing that every other sample is perfectly correlated to its neighbors. This correlation is not limited to up sampling by a factor of two. A large range of re-samplings introduces similar periodic correlations. If the specific form of the re-sampling correlations is known, then it would be straightforward to determine which pixels are correlated to their neighbors. If it is known which pixels are correlated to their neighbors, then the specific form of the correlations can be easily

determined. But in practice neither is known. The expectation/maximization (EM) algorithm is used to simultaneously solve each of these problems [29]. The EM algorithm is a two-step iterative algorithm: (1) in the E-step the probability of each pixel being correlated to their neighbors is estimated; and (2) in the M-step the specific form of the correlations between pixels is estimated. Assuming a linear interpolation model [1,4], the E-step reduces to a Bayesian estimator, and the M-step reduces to weighted least squares estimation. The estimated probability is then used to determine if a portion of the image has been re-sampled.

Splicing

A common form of photo manipulation is the digital splicing of two or more images into a single composite [5]. When performed carefully, the border between the spliced regions can be visually imperceptible. The authors show that splicing disrupts higher-order Fourier [12] statistics, which can subsequently be used to detect splicing.

Image Preprocessing

The image division operator normally takes two images as input and produces a third whose pixel values are just the pixel values of the first image divided by the corresponding pixel values of the second image [1, 4, 28]. Many implementations can also be used with just a single input image, in which case every pixel value in that image is divided by a specified constant. The pixel values are actually vectors rather than scalar values (*e.g.* for color images) than the individual components (*e.g.* red, blue and green components) are simply divided separately to produce the output value [17]. The division operator may only implement integer division, or it may also be able to handle floating point division. If only integer division is performed, then results are typically rounded down to the next lowest integer for output. The ability to use images with pixel value types other than simply 8-bit integers comes in very handy when doing division.

Edge Classification

The given image is represented in scale-space by repeatedly smoothing with a Gaussian filter of increasing size. 12 levels in scale space are extracted. Then, the features' locations and scales are decided by using scale-adapted Laplacian of Gaussian (LoG) , which can indicate gradient changes and corners in the image[14,16]. For the LoG filter, the output of the standard LoG filter is convolved with a scale-adapted Gaussian filter, whereas a similar approach is adopted for the Guassian filter by using a multi-scale Guassian operator. Likely candidates for feature points are selected based on having certain values resulting from the LoG and Harris filters. For points having a Harris filter response greater than a prespecified threshold, we sort the points in decreasing order of LoG filter response. The N points with the maximum responses (subject to meeting exclusion zone criteria) are selected for signature extraction. An exclusion zone of M pixel is used around each feature to maintain a minimum spatial distance between two features. This is important because it is quite likely that points showing the highest response to the filters tend to come from the same objects or regions, and we wish to avoid clustering of features in certain areas of the image.

Feature Extraction

A circular region around each feature point (with a radius dependent on the scale) is scaled to a radius of 32 pixels, allowing for robustness to scale changes. This region is then subjected

to the trace transform, which is a generalization of the Radon transform. It generalizes the Radon transform by allowing for various functionals (in addition to the integral used in the Radon transform) to be applied over straight lines in the circular region. By a proper choice of a functional, invariance to rotation and scaling can be achieved. The trace transform is computed. By drawing samples (indexed by t) along lines parameterized by distance.

RDP Model Generation

In the RDP (Remote Desktop Protocol) model its used to communication between sever and OSI layer, the straight world line is first projected to a great circle on the viewing sphere and then projected to a conic on the image plane. This projection, where the purple lines denote the projection of a straight world lines. The conic is fitted from the projected points of purple world line. The points represent two endpoints and one midpoint of the candidate line and are back-projected into points, respectively. The points define a great circle, which is projected to the straight line in the space with the center of the viewing sphere. In contrast, the points lie on the forgery line, which could be presented as a conic section on the forgery object. The three points are back-projected to points on the viewing sphere, which defines another circle. Note this circle is not a great circle on the viewing sphere, because the forgery line is not satisfying this geometric constraint any more. In other words, the circle generated by the forgery line determines a plane section, which cuts the viewing sphere without passing the center of the view sphere, as shown as the red dotted circle. Thanks to this constraint of line, there are two effective bottom-up cues, the volume cue and the distance cue, which could be used to distinguished the forgery line.

Volume Cue Extraction

With the geometrical constraint, if three points on the image plane are projected from the straight world line, their back-projected points on the viewing sphere follow the geometrical constraint where Volume is the volume of tetrahedron made up by the center of viewing sphere and points of the great circle, as shown as the purple shadow. Statistically, the forgery line is highly unlikely to satisfy this geometrical constraint, as the blue shadow. So the volume cue is defined as a bottom-up cue where is the length of the forgery line in the image. The curves of the volume cue of each candidate line with different virtual focal length of the RDP model, where the volume cues of original lines are close to zero and the cues of forgery lines are more likely to be away from the zero. But in the experiments, the volume cue of the forgery line, which locates away from the image center, is not distinguished clearly with the cues of original lines, such as the right-most candidate line in the second sample. Note that with the virtual focal length , the RDP model degenerates and all the distortion values equal to zero, because the projective transformation of the Step 2 is invalidated and the incidence angle of every pixel vanishes identically.

Distance Cue Estimation

Same as the volume cue, the distance between the center and the plane, which is defined by three projected points on the viewing sphere, is also considered as a cue. Suppose the matrix is composed of a general point and three points on the view sphere which define the plane. Since for points on we can read off the plane coefficients [1, 8 &16].

Fake Saliency Map Generation

Segmentation of forgery objects in an image remains a challenging problem, as the forged object (or detected region) is usually noisy and incomplete [29]. In this section, we introduce a fake saliency map to maximum fake detection density. Firstly, the untrustworthy likelihood is employed to initialize seed. And then the fake saliency map is generated by the untrustworthy likelihood to express the location of forgery object. Finally, the forgery object is segmented by minimizing the energy function via graph cut, which achieves pixel-level segmentation [1]. Note that our fake saliency map is not constrained to a specific choice of the forensic methods, and here we still continue the distortion cues to describe this method [9, 7].

EXISTING SYSTEM

In The previous research, a novel technique based on transform-invariant features [30]. These are obtained by using the features from the MPEG-7 image signature tools. Results show the system of this technique requires more computational resouces in detecting copy-paste forgeries, with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring[1,4,14,19].Existing system uses a technique for detecting copy-paste forgeries with possible post-processing. It is based on the MPEG-7 image signature tools, which form a part of the MPEG-7 standard. This set of tools was designed for robust and fast image and video retrieval. The main issue in directly applying these tools to image forgery detection is that these tools were designed to find duplicate but separate, images, whereas we are trying to find identical regions in the same image. We perform modifications in the feature extraction and matching processes to efficiently detect copy-paste forgeries [12]. Major modification is in the feature matching process. Dispensed with the process as it is only suitable for separate images and fairly large cloned areas. In the context of CBIR, this may occur when the original version of a cropped image needs to be found. Instead, we have adopted a two-step approach matching features in feature and image spaces. Additionally, we have also modified the feature extraction process to extract a larger number of features with better resolution of components.

Drawbacks

The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. A common form of photo manipulation is the digital splicing of two or more images into a single composite. When performed carefully, the border between the spliced regions can be visually imperceptible; the authors show that splicing disrupts higher-order Fourier statistics, which can subsequently be used to detect splicing.

PROPOSED SYSTEM

The Proposed system explicitly employing the distortion cues can detect the forgery object in distortion image. By Proposing two bottom-up cues based on distortion constraint are provided to discriminate the authentication of the line in the image. Also a fake saliency map is used to maximum fake detection density, and based on the fake saliency map, an energy

function is provided to achieve the pixel-level forgery object via graph cut. Image manipulation has become much familiar by the growing easy access to powerful computing abilities. One of the most common types of image forgeries is the copy-paste forgery which works on replicating the same portion of the image, whereas our proposed system works in finding the copy past forgery of newly added object to the actual image wherein a region from an image is replaced with another region from the different image. The previous methodologies in finding identical regions suffer from their inability to detect the cloned region when it has been subjected to a geometric transformation. The proposed system works on distortion based features. These are obtained by using the features from the image.

Advantages Of Proposed

- Adapting the MPEG-7 image signature tools for use in the new application of image forgery detection.
- feature matching approach to the one used by the MPEG-7 standard for image signature tools in order to deal with a different problem context.
- Employing matching feature constraints to un-improve cloned region detection via clustering and does not work for externally modified images.
- Evaluating the previous technique on a variety of images subjected to a significant number of post-processing operations copy-move forgeries involve concealing one region in an image by overlaying another region from the same image. The most seemingly obvious way of detecting copied and pasted regions in the same image would be to verify small clusters or blocks of pixels for matches all across the image. However, there are two major issues with this approach. Firstly, this would be a computationally intensive approach, as matching blocks (or other shapes) of pixels would become infeasible with increasing size of the image. Secondly, such an approach would fail in case of minor changes such as addition of noise or multiple image compression. In order to circumvent these drawbacks of this direct approach, researchers have developed various techniques which can be classified into two main categories: *block-based* and *feature-based.*

ALGORITHMS TO BE USED
Rectangular Distortion Projection Model Algorithm

For the forgery detecting, RDP model is modified based on unified model .The RDP model describes a projection mapping from 2D space points to 2-D distorted image points through a unit sphere, which is called a viewed clearly, . The virtual X and Y origin are termed as principal projection center (image center), $f_v > 0.$ respectively. The center has coordinates with the length $[0, 0, -f_v]^T$. The image formation is modeled as follows.
Considering a 3-D point with Cartesian coordinate $\mathbf{P}_w = [X_w, Y_w, Z_w]^T$ system with respect to viewing sphere. The spherical projection point

$$\mathbf{P}_s = [x_s, y_s, z_s]^T \text{ of } \mathbf{P}_w$$

on the viewing sphere surface has the form, where , and denote

$$\|\mathbf{P}_w\| = \sqrt{X_w^2 + Y_w^2 + Z_w^2}, \text{ and } (\phi, \theta)$$

the 2-D spherical coordinates of the spherical point $\mathbf{P}_s$, ϕ is the directional angle and is the incidence angle. The spherical point $\mathbf{P}_s$ is projected on the normalized image plane as the homogeneous coordinates $\mathbf{p} = [u_p, v_p, 1]^T$. This projection is a projective transformation respected to the virtual optical center, as in the pinhole model. The homogeneous coordinates of is obtained

$\mathbf{p} = \mathbf{K}_s \mathbf{P}_s$ Where $\mathbf{K}_s$ is the camera intrinsic matrix given by with the virtual length.

$$\mathbf{K}_s = \begin{bmatrix} f_v & & \\ & f_v & \\ & & 1 \end{bmatrix}$$

Distance Cue

Same as the volume cue, the distance between the center O and the plane, which is defined by three projected points P_{s_i} on the viewing sphere, is also considered as a cue. Suppose the matrix $\mathbf{M} = [\mathbf{P}, \mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3]$ is composed of a general point P and three points $\mathbf{P}_i$ on the view sphere which define the plane Π. Since $\det(\mathbf{M}) = 0$ or points on we can read off the plane coefficients as

$$\Pi = (D_{234}, -D_{134}, D_{124}, -D_{123})^T$$

Where D_{jkl} is the determinant formed from the jkl rows of matrix. Note in this matrix, $\mathbf{P}_i$ the is represented by homogeneous coordinates as $\mathbf{P}_i = [x_i, y_i, z_i, 1]^T$ so they define a plane and the dimension of matrix $[\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3]$ is 4×3 The distance between the plane Π and any 3-D point $\mathbf{P}_0 = [x_0, y_0, z_0]^T$ is computed by

$$\text{Dis} = \frac{|x_0 D_{234} - y_0 D_{134} + z_0 D_{124} - D_{123}|}{\sqrt{D_{234}^2 - D_{134}^2 + D_{124}^2}}.$$

As in the previous description, the original line in the distorted image, which is projected from the straight world line, is formed by the great circle $\mathbf{G}_L$ on the viewing sphere. So the center of the viewing sphere should be on the plane defined by the great circle $\mathbf{G}_L$ and has $\text{Dis} = 0$ shown as the purple dotted circle in Fig. 4. Oppositely, the forgery line cannot be back-projected into the great circle and has Dis > 0, , shown as the red shadow in Fig. 4. So we define the distance between the plane generated by line and center of viewing sphere as a bottom-up cue w^D .

$$w^D = \frac{|D_{123}|}{\sqrt{D_{234}^2 - D_{134}^2 + D_{124}^2}}.$$

Note that the center of the viewing sphere locates on the origin $[0, 0, 0]^T$ of frame, so the first three terms on the nominator in that the curves of the distance cue of each candidate line

with different virtual focal length of the RDP model. Compared with the volume cue, the distance cue could be useful to classify the candidate lines, which locates away from the image center. But in the experiments, we find the distance cue is short of robustness against the noise and has a lower precision than the volume cue.

Combining Volume And Distance Cues

To achieve a better forensic detection, it is helpful to combine two distortion cues. They can be simply combined for a combined w^C cue as follows:

$$w^C = \log(w^V w^D + 1)$$

Where w^V is computed and w^D is computed. The curves of the combined cue with different virtual focal length of the RDP model, where the forgery lines are separated with the original lines.

EXPERIMENTAL RESULTS
Precision

In the field of accuracy calculation, **precision** is the fraction of **Total number of Test Inputs** that are **Correct Result** to the find:

$$\text{precision} = \frac{|\{\text{Correct Result}\} \cap \{\text{Total number of Test Inputs}\}|}{|\{\text{Total number of Test Inputs}\}|}$$

Recall

Recall in of accuracy calculation is the fraction of the documents that are **Correct Result** to the input that are **Total number of Test Input.**

$$\text{recall} = \frac{|\{\text{Correct Result}\} \cap \{\text{Total number of Test Inputs}\}|}{|\{\text{Correct Result}\}|}$$

	1. PSNR for Existing Method		2. PSNR for Proposed Method	
	Expected	actual	Expected	Actual
Image 1(16 bit)	20+	19.62	20+	17.57
Image 2(24 Bit)	30+	30.19	20+	25.00

Table 1: Converting 20 to 100 % we get the following values

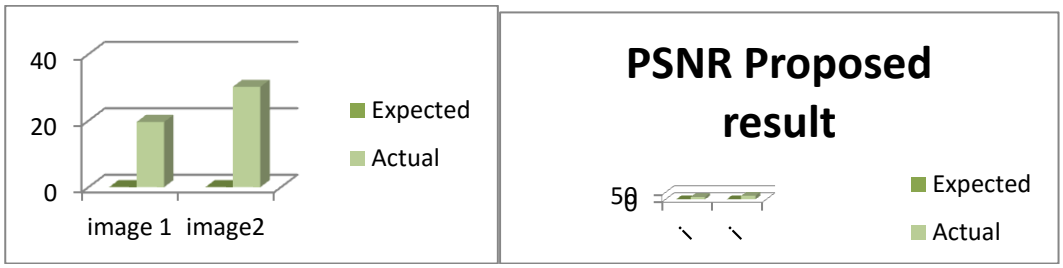

Fig 1 : Converting 20 to 100 % we get the following values

Interchanging The Original And Tampering

Image 1(16 bit)	20+	17.28	20+	19.8
Image2(24 Bit)	30+	24.62	30+	30.09

Table 2: Converting 20 to 100%we get the following vlues

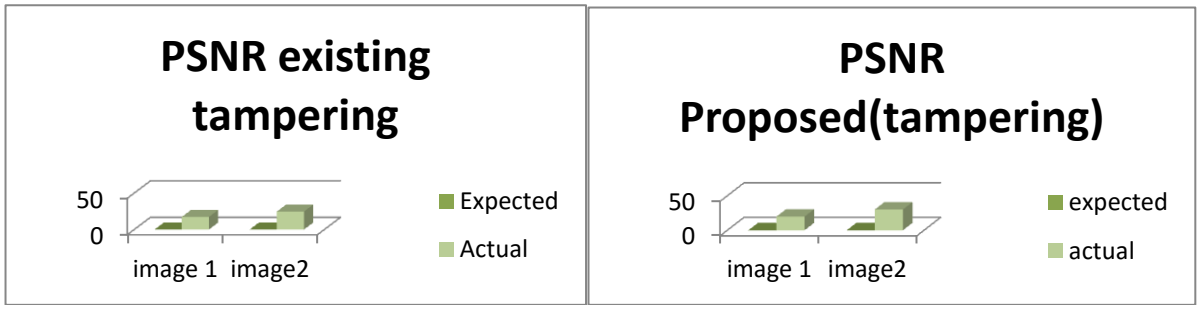

Fig 2: Converting 20 to 100%we get the following vlues

RESULT

Existing result	Proposed result
Image1 65.3	92.37
Image2 65.4	90.81

Table 3: Converting 30 to 100 % we get the following values

Fig 3: Converting 30 to 100 % we get the following values

Precision and recall are then defined as:

$$\text{Precision} = \frac{tp}{tp + fp},$$

$$\text{Recall} = \frac{tp}{tp + fn}$$

Recall in this context is also referred to as the true positive rate or sensitivity, and precision is also referred to as positive predictive value (PPV); other related measures used in classification include true negative rate and accuracy. True negative rate is also called specificity.

$$\text{True negative rate} = \frac{tn}{tn + fp}$$

$$\text{Accuracy} = \frac{tp + tn}{tp + tn + fp + fn}$$

It is possible to interpret precision and recall not as ratios but as probabilities:

- **Precision** is the probability that a (randomly selected) retrieved document is relevant.
- **Recall** is the probability that a (randomly selected) relevant document is retrieved in a search.

Note that the random selection refers to a uniform distribution over the appropriate pool of documents; i.e. by **randomly selected retrieved document**, we mean selecting a document from the set of retrieved documents in a random fashion. The random selection should be such that all documents in the set are equally likely to be selected. Note that, in a typical classification system, the probability that a retrieved document is relevant depends on the document. The above interpretation extends to that scenario also (needs explanation). Another interpretation for precision and recall is as follows. Precision is the average probability of relevant retrieval. Recall is the average probability of complete retrieval. Here we average over multiple retrieval queries.

Example image

Fig (b): Forged Image

CONCLUSION AND DISCUSSION

Image forgeries are most familiar method of forgery where parts of an image are replaced with other parts from the same image. The copied and pasted regions may be subjected to various image transformations in order to conceal the tampering better. Conventional techniques of detecting copy-paste forgeries usually suffer from the problems of false positives and susceptibility to many image processing operations. We have proposed a geometric-based method for detecting a forgery object via distortion. The geometry constraint on the viewing changes of radial distortion projection model is employed to support two bottom-up cues. Furthermore, a fake saliency map is generated by untrustworthy likelihood, to segment the forgery object. The experiments demonstrated the performance of our method in both simulated data and real images. The applications showed that potential usage of our fake saliency map in other common digital images.

FUTURE ENHANCEMENT

We have provided some results of detecting inconsistent regions by using our technique and have compared it with another technique applicable to motion and distortions. Quantitative and qualitative results show that our technique provides better results in selecting the regions with inconsistent. Which can be applied in future for videos forgery detection. And for audio data forging, that still remains a challenging task in signal processing research.

ACKNOWLEDGMENT

The authors would like to thanks the anonymous reviewers for their constrictive commands and also thanks to all reviewers.

REFERENCES

[1] H. Farid, "A survey of image forgery detection," IEEE Signal Process. Mag., vol. 2, no. 26, pp. 16–25, 2009.
[2] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Image Communication, vol. 25, no. 6, pp. 389–399, 2010.
[3] A. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
[4] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, no. 5, pp. 188–197, 2009.
[5] H. Fu, Z. Cao, and X. Cao, "Embedded omni-vision navigator based on multi-object tracking,"*Mach. Vision Appl.*, vol. 22, no. 2, pp. 349–358, 2011.
[6] A. W. Fitzgibbon, "Simultaneous linear estimation of multiple view geometry and lens distortion," in *CVPR*, 2001, vol. 1, pp. 125–132.
[7] R. Hartley and S. B. Kang, "Parameter-free radial distortion correction with center of distortion estimation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 8, pp. 1309–1321, Aug. 2007.
[8] J. Tardif, P. Sturm, M. Trudeau, and S. Roy, "Calibration of cameras with radially symmetric distortion," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 9, pp. 1552–1566, Sep. 2009.
[9] Z. Kukelova and T. Pajdla, "A minimal solution to radial distortion autocalibration," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 12, pp. 2410–2422, Dec. 2011.
[10] B. Mičušík and T. Pajdla, "Estimation of omnidirectional camera model from epipolar geometry," in *CVPR*, 2003, vol. 1, pp.
[11] v. Christlein, c. Riess, j. Jordan, c. Riess, and e. Angelopoulou, "an evaluation of popular copy-move forgery detection approaches,"*ieee trans. Inf. Forensics security*, vol. 7, no. 6, pp. 1841–1854,dec. 2012.
[12] s. Bayram, h. T. Sencar, and n. Memon, "an efficient and robust method for detecting copy-move forgery," in *proc. Ieee int. Conf. Acoust., speech signal process. (icassp)*, washington, dc, usa, apr. 2009, pp. 1053–1056
[13] m. Ghorbani, m. Firouzmand, and a. Faraahi, "dwt-dct (qcd) based copy-move image forgery detection," in *proc. 18th int. Conf. Syst.,signals image process. (iwssip)*, jun. 2011, pp. 1 4.
[14] s.-j. Ryu, m. Kirchner, m.-j. Lee and h.-k. Lee, "rotation invariant localization of duplicated image regions based on zernike moments," *ieee trans. Inf. Forensics security*, vol. 8, no. 8, pp. 1355–1370,aug. 2013.
[15] v. Christlein, c. Riess, and e. Angelopoulou, "on rotation invariance in copy-move forgery detection," in *proc. Ieee workshop int. Inf. Forensics secur. (wifs)*, dec. 2010, pp. 1–6.
[16] e. Ardizzone, a. Bruno, and g. Mazzola, "copy-move forgery detectionvia texture description," in *proc. 2nd acm workshop multimedia forensics, secur. Intell.*, new york, ny, usa, 2010, pp. 59–64.
[17] x. Bo, w. Junwen, l. Guangjie, and d. Yuewei, "image copy-move forgery detection based on surf," in *proc. Int. Conf. Multimedia inf. Netw. Secur. (mines)*, nov. 2010, pp. 889–892.
[18] x. Pan and s. Lyu, "region duplication detection using image feature matching," *ieee trans. Inf. Forensics security*, vol. 5, no. 4,pp. 857–867, dec. 2010.
[19] i. Amerini, l. Ballan, r. Caldelli, a. Del bimbo, and g. Serra, "a sift-based forensic method for copy–move attack detection and transformation recovery," *ieee trans. Inf. Forensics security*, vol. 6,no. 3, pp. 1099–1110, sep. 2011.

[20] p. Kakar and n. Sudha, "exposing postprocessed copy–paste forgeries through transform-invariant features," *ieee trans. Inf. Forensics security,* vol. 7, no. 3, pp. 1018–1028, jun. 2012.
[21] h. Bay, a. Ess, t. Tuytelaars, and l. Van gool, "surf: speededup robust features," *comput. Vis. Image understand.,* vol. 110, no. 3,pp. 346–359, jun. 2008
[22] q. Liu, n. Linge, and v. Lynch, "implementation of automatic gas monitoring in a domestic energy management system," *ieee trans. Consum. Electron.,* vol. 58, no. 3, pp. 781–786, aug. 2012.
[23] q. Liu, g. Cooper, n. Linge, h. Takruri, and r. Sowden, "dehems: creating a digital environment for large-scale energy management at homes," *ieee trans. Consum. Electron.,* vol. 59, no. 1, pp. 62–69,feb. 2013.
[24] m. Akhin and v. Itsykson, "clone detection: why, what and how?" In *proc. 6th central eastern eur. Softw. Eng. Conf. (cee-secr),* 2010,pp. 36–42.
[25] a. M. Bronstein, m. M. Bronstein, y. Carmon, and r. Kimmel, "partial similarity of shapes using a statistical significance measure," *ipsj trans. Comput. Vis. Appl.,* vol. 1, pp. 105–114, mar. 2009.
[26] i. Amerini, l. Ballan, r. Caldelli, a. D. Bimbo, l. D. Tongo, and g. Serra, "copy-move forgery detection and localization by means of robust clustering with j-linkage," *signal process., image commun.,* vol. 28, no. 6, pp. 659–669, jul. 2013.
[27] b. Liu, c.-m. Pun, and x.-c. Yuan, "digital image forgery detection using jpeg features and local noise discrepancies," *sci. World j.,*vol. 2014, pp. 1–12, mar. 2014, art. Id 230425.
[28] p. Arbelaez, m. Maire, c. Fowlkes, and j. Malik, "contour detection and hierarchical image segmentation," *ieee trans. Pattern anal. Mach. Intell.,* vol. 33, no. 5, pp. 898–916, may 2011.
[29] r. Achanta, a. Shaji, k. Smith, a. Lucchi, p. Fua, and s. Süsstrunk, "slic superpixels compared to state-of-the-art superpixel methods," *ieee trans. Pattern anal. Mach. Intell.,* vol. 34, no. 11, pp. 2274–2282, nov. 2012.
[30] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun," Segmentation-Based Image Copy-Move Forgery Detection Scheme" *Senior Member, IEEE.VOL,.10,n0.3,march 2015.*