Copy Move Forgery Detection for Digital Image Forensics using Edge Detection and Color Auto-Correlogram

Hlaing Htae Khaung Tin, Si Thu and J.Samuel Manoharan,
1Faculty of Information Science, University of Information Technology, Yangon, Myanmar,
2Department of Physics, Ban Maw University, Myanmar,
3Department of ECE, Sir Isaac Newton College of Engineering & Technology, Nagapattinam, South India

Abstract: Fake image or picture detection is evolving as one of the famous and popular research themes among researchers in the field of digital image forensics area. Fake image or picture is fake by exhausting many different techniques but the highest common method is copy move counterfeit finding for digital forensics. The goal of fake image detection using copy move forgery detection technique remains to discover image spaces that are matching image or very similar image. In general, digital image forensics methods can be defined into two different methods. They are active approach and passive approach. In active approaches are watermarking and digital signatures. And in passive approaches have three techniques in general. In this copy move forgery detection system is collected 250 images which contain the images of people, flowers, fruits, animals and toys. They are copy move, splicing and retouching techniques. This paper shows copy move forgery detection technique for fake image detection and the major challenges are affect technique and efficient time complexity of proposed technique.

Keywords: Image Forensic, Copy Move, Forgery Detection, Fake image, Digital forensics, Colour auto-corrlogram.

I. INTRODUCTION

Copy move forgery detection technique be situated by copying the portion from a target image and moving that portion on unchanged image by misleading the user. This fake image detection technique can be defined by two different approaches; active approaches and passive or blind approaches.

The digital imaging case deals with two major problems. The original photo identification and image integrity. To solve these problems forensic researchers developed image authentication algorithms and prevent attacks from fake image. Copy-move is the greatest common handling technique. This means that athing in an image is pasted together after the first copy where a picture is different. Fake copy-move is generally intended to be successful two purposes. They are duplication of objects and concealment of truth.

A fake can cover up an image or object in the intended image. It must be removed to confuse the public and spread false information. According to my scientific limitations, only the best detectors detect digital imaging therapies based on the framework of conceptual theory. To fill this gap, we will design based on the forensic tools used in this paper and move them into theoretical test theory and practice.

This research paper is designed as the six sections. The literature review of digital image forensics and copy move detection presented in section 2. The general design of image detection techniques (types of image forgery detection) also shown in section 3. These procedures are further divided into active approach and passive methods. The edge detection presented in section 4 and proposed copy move detection described in part 5. The evaluation of the system performance and comparison the proposed methods and conclusion is shown in part 6.

II. LITERATURE REVIEW

This research paper shows a study of various image forgery techniques under passive approaches and a survey of various attempts in copy move forgery detection. In this digital image forensics is the most interested field in information technology environment. Image forensics has changed to explore the integrity and authenticity of digital images and to find the driving force after imitation imaging in this area.

Fake image or picture is forged by consuming many dissimilar techniques but the most collective method is copy move forgery detection for digital forensics which include copying a region of image and pasting/moving it anywhere in the same image to secrete or reproduce a part of the image to transform the information taken by it. The copy move forgery detection technique is broadly investigated region in digital image forensics area. [1]

Photo analysis is a fundamental component of a variety of activities. It can be as simple a task as a complex task, such as reading or generating barcode numbers. In the field of forensic medicine, a crime scene can be photographed. It is the main source of evidence that is used to link suspicious scenes.

The screenshot or copy/paste image is different from other photos. This is usually the case very specific purpose for capturing each image. The different method of detecting method proposes detecting the circle using Randomized Algorithm (RCD). This research first selects the four extremes. Set the search distance to see if there is a random in the image. The probability circle through which the extreme points are determined after determining the probability. The community was involved in the process of gathering evidence to investigate the author and imagine possible circle or not. [3]

Hough Transformation (HT) is an important part of the image effectively search for lines or curves in an image. Research papers that have been studied for over 2,500 years prove with its variations, simplifications, possessions and applications in different arenas. [4]

To capture the dynamics of sensory motion, calculated each of the auto-correlograms from the spike timeseries and removed their lines (LAT) and time constants (TAU). [7] The similar technique is used for units of vivorecordings and neurons. To prevent these errors, calculate the estimation for high transient accuracy directly from the spike frequency to the auto-correlogram. And calculate that reduce all the information recorded for each sensor cell at the individual sensor cell level. [5]
There are three types of copy move search methods. These are (1) block-based detection, (2) lock-based detection, and (3) brute force detection. The easy way out to the problem of a fake copy-move is brute force detection, which involves comparing the image to the version that changed it. The problem with this technique is its computer complexity. Automated correlation is a development over a complete search engine. On the other hand, it can only be used after copying big image patches.[7]

Fake copy move approach is one of the greatest commonly used and easy to carry image handling tools. The first is the problem of common ground. The challenge of the lack of a common standard perimeter the comparison and reproduction of existing accessible procedures. Although large datasets are available, data sets need to be developed to study the methods used to visualize geometric transformations and the methods used to create fake transitions. In addition, the available methods were not assessed on the foundation of a common enactment matrix that could facilitate the comparison of methods. The robustness of the procedures is also a problem. No separate algorithm can handle the advantages of various post processing tasks, such as jpeg compression. [8]

III. KINDS OF IMAGE FORGERY DETECTION METHOD

This part shows the kinds of image forgery detection methods. The arrangement of this method is chiefly classified into two separate methods. They are active method and passive method. Active approaches are watermarking and digital signatures in passive methods are copy move, splicing and retouching techniques in general.

In active method, the image hinge on approximately extra pre introduced information such as digital watermark supplement or ascribing digital signature on the appearance at this period of the image record. The lack of confidential information embedded in digital images has led many new researchers to focus on the new passive or blind method in the field of artificial intelligence. These methods check for changes that are happening in the same feature-rich event by verifying the digital image.[9]

Under the active approach the digital watermark is a tool that grant customer on the way to implant digital material, which familiar relate on the digital document similar image to exclusively classify ownership or creator of the digital image. And the digital signature is a cryptographic occurrence namely a mathematical word and it is procedure which supplements the digital signature on the digital manuscript similar an image to deliver assertion for no modification working on the digital image. [9]

The passive method is sub allocated into numerous groups established on the tampering achieve on the digital images. Specifically, classifications are copy move, image splicing and image retouching. Figure 1 shows the classification of the image forgery detection procedures. Image splicing forgery is the simple act of simply cutting a portion of an image from the same or different source image. The image retouching forgery is an art and science of image alteration where the visual imagery contents improved by execution numerous changes using the accessible picture in section software. [9]

This paper shows copy move forgery detection method for fake image detection. This detection is extensive image tempering method that familiar to operate the digital image content. It is a kind of image counterfeit where a portion is copied and pasted on additional in the matching image frame either to fake or to duplicate the object in the image manifold or many times. This proposed edge detection and copy move detection technique shown in the next section.

In figure 3 also an illustration of copy move forgery image which shows a novel image and its copy move appearance. And another example shows in the following figure 4(a) and (b).
The above figure 2(a) is an original picture then the figure 2(b) is a sample of copy move forgery image.

Fig 3. A copy move images

The black puppy is copied without any transformation as seen in figure 4(b). While the black puppy is same size in the original image, before pasting, as shown in figure 4(a). The proposed technique is detecting the duplicated image and incorrect information.

Fig 4(a) An original image

Fig 4(b) Copy move image for black puppy in right side of the image

The green flower pot in the middle of the image is copied without any transformation as seen in figure 5(b). While the green flower pot is different size in the original image, before pasting, as shown in figure 5(a). The proposed technique is detecting the duplicated image and incorrect information.

IV. PROPOSED EDGE DETECTION

The edges of the image are areas of high intensity and a jump the intensity starting one pixel to another. A pixel can make a significant difference in the quality of the image. Edge detection of the image significantly decreases the sum of data and A filters out non-critical information while preserving the important features of the image.

Fig 5(a) An original image

Fig 5(b) Copy move image for green flower pot in the middle of the image

The edges remain scale-dependent and the edges may have new edges, but to some extent the edges are without width. If precise edges are specified, all objects will be placed and simple possessions such as area, perimeter and shape can be easily measured. Therefore, the edges are used to estimate the boundaries and segmentation of the scene.

A. Sobel Technique

The Sobel edge detection technique consists of 3 x 3 convolution kernels, a kernel is rotated at 90 °, as shown in Figure 6. These kernels are calculated to react too vertically and horizontally maximum in relation to the pixel grid of the images, which is a kernel for both verticalcooordination.
The kernels can be used distinctly with the input images to create capacities, separating the gradient module in each location. These things can be joined to catch the exact magnitude of the gradient at each fact and the location of the gradient.

![Fig. 6 Masks Used for Sobel Operator](image)

**B. Robert Technique**

Robert cross operator performs simple and fast, 2-D spatial measurements in images. The pixel value at each fact of the production represents the predictable total size of the spatial gradient of the input image at that fact.

The operative contains $2 \times 2$ convolution kernels as presented in Figure 7. One kernel is purely that the additional rotates at $90^\circ$. This is much related to the Sobel operator.

-1 0 +1  0 +2 +1  0 0 0  -1 -2 -1

$G_x$

$G_y$

![Fig. 7 Masks Used for Robert Operator](image)

**C. Prewitt Technique**

The Prewitt operator is related to the Sobel operator and can detect vertical and horizontal edges of images. Prewitt operators’ portion two modules. The vertical edge element is designed with the kernel $G_x$ and the horizontal edge module with the kernel $G_y$, as shown in Figure 8 | $G_x | + | G_y |$ provides an indication of the gradient concentration in the recent pixel.

-1 0 +1  1 0 -1  0 0 0  -1 0 +1  0 0 0

$G_x$

$G_y$

![Fig. 8 Masks Used for Prewitt Operator](image)

**D. Canny Technique**

Canny's edge detection process is widely recognized as the most appropriate edge detector. The Canny procedure uses the most appropriate edge detector created on the set of conditions, which includes looking the greatest edges by reducing the error rate, making the edges as much as possible to the actual edges to maximize localization, and making the edges only one when a single edge exits for minimal reaction. Rendering to Canny, to obtain the least possible response, the best filter that encounters the three criteria can be estimated professionally using the first derivative of the Gaussian function.

The first step is to smooth the image using Gaussian filter. Next, look for the gradient of the image by providing a smoothed image through the convolution operation with Gaussian derivatives both vertically and horizontally. This process reduces the difficulties related with edge discontinuity by recognizing the robust edges, and associated weak edge processing, in addition to maintaining noise reduction levels.

Eventually, hysteresis is work to prevent the band. Streaking is a breakdown of the edge contour caused by the shocking operator's expenses above and below the threshold.

**V. PROPOSED COPY MOVE FORGERY DETECTION USING COLOR AUTO-CORRELOGRAM**

One of the most important performances for copy move image retrieval is color histogram. It is effective for calculation and good for searching results. Designed for an $m \times n$ image I, the colors of the appearance is quantized to $C_1, C_2, \ldots C_k$. The colour histogram $H(I) = \{h_1, h_2, \ldots h_k\}$, where the number of pixels is $C_i$.

$$\Pr(P \in C_i) = \frac{h_i}{m \times n} \quad (1)$$

The colour histogram also shows the prospect of any pixel in image I, which is colour $C_i$. The weakness of the histogram performance is that there is no space data in the colour histogram.

Colour auto-correlogram techniques have been proposed to combine spatial data with colour histograms. Auto-correlogram of image I for colour $C_i$ can be determined with distance k.

$$\gamma^{(k)}_{C_i} = \Pr(|p_1 - p_2| = k, p_2 \in I, p_1 \in I, C_i) \quad (2)$$

The correlogram feature of image represent in figure 9 in what way the spatial autocorrelation of colour modifications with space.

![Fig. 9 Sample colour auto-correlogram feature](image)
In this copy move detection system is collected 250 images which contain the images of people, flowers, fruits, animals and toys in the following table 1.

<table>
<thead>
<tr>
<th>Categories of image</th>
<th>Number of images</th>
<th>Image Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>50</td>
<td>128x128, 512x512</td>
</tr>
<tr>
<td>Flower</td>
<td>50</td>
<td>128x128, 240x160</td>
</tr>
<tr>
<td>Fruit</td>
<td>50</td>
<td>128x128, 512x512</td>
</tr>
<tr>
<td>Animal</td>
<td>50</td>
<td>128x128, 512x512</td>
</tr>
<tr>
<td>Toy</td>
<td>50</td>
<td>512x512</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>250</strong></td>
<td><strong>128x128, 240x160, 512x512</strong></td>
</tr>
</tbody>
</table>

A. Assessment of the System Performance

The performance of detection of the system can be measured in terms of its accuracy. System accuracy is to measure the related images to the query in the entire image of the detecting image. The system will calculate the accuracy values of each class in images database.

To evaluate the system, it has collected 250 images which contain the images of people, flower, fruit, animal and toy. The system uses the holdout method to evaluate the performance. The accuracy is calculated by the following equation 3, equation 4.

\[
\text{Precision} (P) = \frac{TP}{TP+FP} \quad (3)
\]

Where,

TP = True Positive, FP = False Positive

\[
\text{Recall}(R) = \frac{TP}{TP+FN} \quad (4)
\]

Where,

TP = True Positive, FN = False Negative

The dualistic arrangement of the F1 score (also F-score or F-measure) is a portion of a test's correctness in statistical analysis. In F1 score studies together the precision and the recall of the check to calculate the score: \( p \) is the quantity of right positive outcomes divided by the quantity of all optimistic outcomes give back by the identifier, and \( r \) is the amount of correct positive results divided by the amount of all related tasters (all tasters that would have been recognized as positive) in equation 5. The F1 score is the harmonic mean of the precision and recall, where an F1 score influences its greatest value at 1 and worst at 0. [2]

\[
F1 \text{ Score} = 2 \cdot \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)
\]

Where,

F1 score = a measure of a test's accuracy

<table>
<thead>
<tr>
<th>Images</th>
<th>True Positive</th>
<th>False Positive</th>
<th>False Negative</th>
<th>Precision</th>
<th>Recall</th>
<th>F1 score</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>45</td>
<td>2</td>
<td>3</td>
<td>0.9574</td>
<td>0.9375</td>
<td>0.9473</td>
</tr>
<tr>
<td>Flower</td>
<td>40</td>
<td>4</td>
<td>6</td>
<td>0.9090</td>
<td>0.8695</td>
<td>0.8887</td>
</tr>
<tr>
<td>Fruit</td>
<td>40</td>
<td>5</td>
<td>5</td>
<td>0.8888</td>
<td>0.8888</td>
<td>0.8888</td>
</tr>
<tr>
<td>Animal</td>
<td>42</td>
<td>2</td>
<td>6</td>
<td>0.9543</td>
<td>0.875</td>
<td>0.9129</td>
</tr>
<tr>
<td>Toy</td>
<td>45</td>
<td>3</td>
<td>4</td>
<td>0.9547</td>
<td>0.9148</td>
<td>0.9246</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>210</strong></td>
<td><strong>16</strong></td>
<td><strong>24</strong></td>
<td><strong>0.9292</strong></td>
<td><strong>0.8974</strong></td>
<td><strong>0.9128</strong></td>
</tr>
</tbody>
</table>

CONCLUSION

This research paper describes the design and implementation of copy move image detection for digital image forensics. When a new query image enters to the system as an input, it extracts image features and check the edge detection, colour auto-Correlogram features to provide similar or same region of the user's query images. With the purpose of improve the presentation and accuracy of copy move image finding using precision, recall and f1 score created by the experimental outcomes.

Acknowledgments

I would like to say a big thanks a lot to my family for giving me constant motivation and encouragement during this research work.

References


