A Passive Image Forgery Detection Technique

Dr. Dayanand G. Savakar¹ and Mr. Raju Hiremath²,*

¹ Professor, Dept. of Computer Science, Rani Channamma University, Belagavi; dgsavakar@gmail.com
² Research Scholar, Dept. of Computer Science, Rani Channamma University, Belagavi; *rajuhiremath@rcub.ac.in

Abstract

The digital image is the main source of communication in the current scenario. The digital images are miscommunicated by using various image manipulation softwares. The digital images are altered in such a way that it is difficult to understand the originality of the contents. The proposed system addresses a passive approach to image forgery detection. In this system first, the input image is partitioned into blocks. Then various features are extracted from each block like energy, entropy, contrast, homogeneity, mean, standard deviation and variance then store it to the knowledge base. Next each block features are compared with knowledge base. The proposed system identifies original and forged images accurately. The result of experiment is much better than the existing techniques.

Keywords: Passive approach, forgery, contrast, homogeneity, energy, entropy, mean, standard deviation, variance.

1. Introduction

The image is the main stream in the digital communication medium. The various types of images are shared and communicated in day-day life. Now a day because of smart tools and technology it is difficult to recognize the genuine and fake images. The various techniques are proposed to identify the originality of an image [1-14]. The various attacks are utilized to forge the image such as copy-move splicing resampling etc..

The image forgery is nothing but manipulation or tampering of an image in such a way that it is difficult to identify. The image tampering identification methods are categorized as active and passive approach. In active methods secret code, public key and private key are used to validate the digital content. In active approach there are two forms Digital Signature and Digital Watermarking. In Digital Signature public and private key is utilized to validate the digital
document or content. In Digital Watermarking the secret code is embedded in the digital document or image further that secret code is utilized for validation.

In passive approach there are three kinds or methods copy-move, splicing and resampling. In copy-move the portion of a digital image is copied and insert into the source image. This method is utilized to hide the content of the image or to duplicate the content of the image. The various researchers address the copy-move forgery detection [1-5,8-10,14]. In splicing method, the portion of one image is copied and insert into different image. This method is adopted to cover the part of an image or to add new content to an image. The several researchers proposed the splicing forgery detection techniques [6,11]. In resampling method, the rotation or resized or scaling operation is performed in an image. The some of the authors presented the technique based on resampling method [13].

The rest of the paper is arranged as follows. Section 2 and 3 gives the related work and proposed methodology. Section 4 gives result and discussion and section 5 gives conclusions.

2. Related Work

The many research work conducted on passive image tampering identification [1-14]. In this paper the passive approach image forgery detection technique is addressed. The passive image forgery detection approach is classified as copy-move, splicing and resampling techniques.
2.1 Copy-move image forgery

The copy-move forgery detection technique is frequently used technique. The various researcher proposed techniques to identify the copy-move forgery in an image [1-5,8-10,14]. The various research work has been carried out to detect copy-move forgery detection using different techniques such as Convolution Neural Network [1,7], Discrete Cosine Transformation [1], Entropy [9], etc., The author Yanfen Gan et al. [14] presented the fusion technique for identification of duplicate forgery with the help Radial Harmonic Fourier Moments and SIFT. In this technique SIFT is used for extracting the features, then the unwanted features are removed using the adaptive Euclidian distance, nearest neighbor and Random sample consensus. Next the input image is segmented into texture patches using Simple Linear Iterative Clustering technique. Finally, the geometric operations are performed. The proposed system achieved good performance as compared with other techniques.

The author [5] proposed the block-based copy-move tamper identification technique using DCT, cellular automata and patch match. In this technique Discrete Cosine Transformation and cellular automata is utilized for fetching the features from an image. Then the features are matched using patch matching technique. The proposed system produced good result in terms of accuracy. The improved copy-move image tampering identification method is proposed by B. Rakesh Babu and Dr. S. Narayana Reddy [1] based on deep learning approach. In this technique the features are fetched with the help of CNN and the extracted features are matched utilizing Deep learning technique. The proposed system detects and localized forged part in an image with good accuracy.

2.2. Splicing forgery detection

The splicing forgery is nothing but the portion of one image is copied and insert into different image. The researcher proposed the splicing forgery detection techniques [6,11] using different techniques. The author Nam Thanh Pham et al. [11] presented hybrid image retrieval technique for detecting the image splicing forgery. In this method the first phase is image retrieval, in which the image is segmented into background part and spliced part. Then the SIFT and Zernike moment features are extracted. Finally, the regions are matched using various manipulation operations. The proposed method efficiently retrieved the spliced part of an image. The author [6] proposed an enhanced image tamper identification technique employing MWC-Net (Multi-task Wavelet Corrected Network). In this technique the MWC-Net is utilized to wavelet up-pooling and wavelet pooling for compression and reconstruction of features of splicing forged images. Then the MWC-Net employs multi-task approach for enhancing the ability of the learning. The experiment result shows good result for identification and localization of the splicing forgery is good related to the other techniques.
2.3 Resampling forgery detection

The image forgery detection of type resampling is nothing but the rotation, resizing and scaling operation is performed on the image. The A. Flenner et. al [13] proposed the resampling counterfeit identification technique sourcing A-Contrario analysis and deep learning. In this technique there are three phases are there. In first phase from the image blocks resampling features are evaluated. In the second phase the heat map is generated using deep learning classifier which specifies the resampled image block. In the last phase a-contrario hypothetical testing technique. The proposed system competently identifies and locates the resampling forgery in an image.

3. Proposed method

The proposed technique addresses a passive forgery detection method. In this technique first input the original or forged image as Img. Then the block-based technique is adopted. The block size is assigned as 5. Next the binary image of the original or forged image is created and opened for writing the data into the file. The Img is divided to R, G, B channel blocks. Then the contrast, homogeneity, energy, entropy, mean, standard deviation and variance features are extracted from each block. Next save the features to the knowledge base.

3.1 Feature Extraction

The different types of texture and statistical features are extracted such as contrast, homogeneity, energy, entropy, mean, standard deviation and variance. The various notations are used for evaluation of the texture features are as follows.

\[
\begin{align*}
    p(i, j) & \quad \text{Element (i,j) in GLCM (Gray Level Co-occurrence Matrix)} \\
    N & \quad \text{Number of gray levels in the quantized image} \\
    p_x(i) & \quad \sum_{j=1}^{N} p(i, j). \\
    p_y(j) & \quad \sum_{i=1}^{N} p(i, j). \\
    q(i, j) & \quad \sum_{k} p(ik)p(jk) \\
    \mu_x & \quad \sum_{i=1}^{N} i \cdot p_x(i) \\
    \mu_y & \quad \sum_{j=1}^{N} j \cdot p_y(j) \\
    \sigma_x^2 & \quad \sum_{i=1}^{N} (i - \mu_x)^2 \cdot p_x(i) \\
    \sigma_y^2 & \quad \sum_{j=1}^{N} (j - \mu_y)^2 \cdot p_y(j)
\end{align*}
\]

The equations utilized to calculate the textual features of an image is showed in Table 1.
Table 1
The different textual features and their equations

<table>
<thead>
<tr>
<th>Function Name</th>
<th>Equation</th>
<th>Reference No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>$\sum_{i=1}^{N} \sum_{j=1}^{N} p(i,j)^2$</td>
<td>15</td>
</tr>
<tr>
<td>Contrast</td>
<td>$\sum_{i=1}^{N} \sum_{j=1}^{N} (i - j)^2 p(i,j)$</td>
<td>15</td>
</tr>
<tr>
<td>Homogeneity</td>
<td>$\sum_{i=1}^{N} \sum_{j=1}^{N} \frac{p(i,j)}{1 + (i - j)^2}$</td>
<td>15</td>
</tr>
<tr>
<td>Entropy</td>
<td>$\sum_{i=1}^{N} \sum_{j=1}^{N} p(i,j) \log p(i,j)$</td>
<td>15</td>
</tr>
</tbody>
</table>

The statistical features are extracted from each block as described as follows.

**Mean:** The average values of the pixels of each block [16].

$$i_m = \frac{1}{K} \sum_{k=1}^{K} i(k) \quad (1)$$

**Standard Deviation:** The Deviation from the mean of pixel values of each block [16].

$$i_{sd} = \sqrt{\frac{\sum_{k=1}^{K} (i(k) - i_m)^2}{(K-1)}} \quad (2)$$

**Variance:** The Square of the Standard Deviation [16].

$$i_v = \frac{\sum_{k=1}^{K} (i(k) - i_m)^2}{(K-1)} \quad (3)$$

The extracted features are stored into binary file. After feature extraction each block features are matched with all blocks. If matched blocks are greater than 10 then the image is identified as forged. Otherwise, the image is original.
3.1 Algorithm: A Passive image forgery detection technique

**Input:** Input image

**Output:** Display Original or Forged Image

**Start**

**Step1:** Read image as Img

**Step2:** Assign Block size Bsize=5

**Step3:** Create the binary file as Img_bfile.asv

**Step4:** Divide the Img into R, G, B Channel blocks rbk, gbk, bbk

**Step5:** Extract contrast, homogeneity, energy, entropy, mean, standard deviation and variance features from each block rbk, gbk, bbk

**Step6:** Save the features to knowledge base as ffile

**Step7:** Compare the features of each block to the knowledge base

**Step8:** If matched_block > 10 then

- Display “Forged Image”
- Else
- Display “Original Image”

End if

**Stop**
3.2 Methodology

Fig. 2. The proposed methodology
4. Result and Discussions

The testing the proposed system our own dataset will be utilized. In this dataset total 100 images are there, in those original 50 images and forged 50 images.

Performance evaluation

The performance of the proposed system is analyzed by calculating the accuracy of the result obtained. The accuracy is evaluated by sum of correctly recognized original images and the sum of correctly recognized forged images which is divided by sum of correctly recognized original and forged images added with sum of wrongly recognized original and forged images. The accuracy (Ac) of the proposed system is evaluated using the Eq (4). The confusion matrix used for performance measure is shown in Table 2.

\[
    Ac = \frac{TP + TN}{TP + TN + FP + FN} \times 100
\]  

Where,

TP= The sum of correctly recognized original images.
TN= The sum of correctly recognized forged images.
FP= The sum of wrongly recognized original images.
FN= The sum of wrongly recognized forged images.

Table 2
Confusion matrix

<table>
<thead>
<tr>
<th>Predicted Value</th>
<th>Actual value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Positive</td>
</tr>
<tr>
<td>Positive</td>
<td>True Positive</td>
</tr>
<tr>
<td>Negative</td>
<td>False Negative</td>
</tr>
</tbody>
</table>

TP= True Positive, TN= True Negative, FP= False Positive

Table 3
Comparison of our method with other methods.

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Forgery Type</th>
<th>Ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. Rakesh Babu1, Dr. S. Narayana Reddy [1]</td>
<td>Copy-Move</td>
<td>95.02%</td>
</tr>
<tr>
<td>Muhammad Naveed Abbas et al [4]</td>
<td>Copy-Move</td>
<td>87.00%</td>
</tr>
<tr>
<td>Dayanand G. Savakar and Raju Hiremath [9]</td>
<td>Copy-Move</td>
<td>94.29%</td>
</tr>
<tr>
<td>Nam Thanh Pham et.al [11]</td>
<td>Splicing</td>
<td>84.89%</td>
</tr>
<tr>
<td>Ritu Agarwal and Mallika Pant [12]</td>
<td>Copy-Move and Splicing</td>
<td>93.33%</td>
</tr>
<tr>
<td>Proposed method</td>
<td>Copy-Move</td>
<td>96.00%</td>
</tr>
</tbody>
</table>
5. Conclusion

The passive image forgery detection technique is frequently used forgery types. In which one of the popular types of forgery copy-move forgery is addressed. In suggested system first the image is partitioned into blocks then, the different texture features like contrast, energy, entropy, homogeneity and statistical features like mean, standard deviation and variance extracted from each block. Then the extracted features are stored into the knowledge base. Next the features of each block are compared with knowledge base. If the more than 10 blocks are matched then it displayed as forged image or else it displayed as original image. The proposed system higher accuracy compared with other methods.

References


