Robust Detection of copy move forgeries for scanned documents using multiple methods

Anirudh Prabhu[1], Zil Shah[2] and Manan Shah[3]

**[1] St.Francis Institute of Technology,
Mumbai, Maharashtra 400103, India**

**[2] St.Francis Institute of Technology,
Mumbai, Maharashtra 400103, India**

**[3] St.Francis Institute of Technology,
Mumbai, Maharashtra 400103, India**

Abstract

Cybercrime and forgeries are growing at an alarming rate. There are a lot of places on the web that store scanned documents for future use. These documents are prone to damage and tampering. Misuse of such documents can turn out to be very dangerous. This paper proposes an easy way of detecting modifications made in scanned documents. The algorithm used for this purpose is a very simple pixel detection program.

Keywords: *— Forgery, Copy Move Detection, Block Based Detection, Feature Based Detection, Pixel Overlapping, Block Comparison, Border Pixels, Pixel Count.*

1. Introduction

All records are now going digital. In many places in the world old records are scanned and digital copies are maintained. But this makes it prone to hackers. The hackers can easily modify the scanned image and make it look the way they want. This paper proposes a technique to find if any part of the picture has been modified, changed or deleted. We achieve this by simply by matching pixels and comparing them. When the image is converted to pixels, we can match them with each other. Whenever there has been a modification in the image, however convincing to the naked eye, there is always a pixel overlapping at the border and edges of the modification. We hope to find this by matching pixels of the document. This method will also help us find which part of the image has been modified. This is a very useful method when it comes to changing names in criminal records or changing dates in deadlines or changing names in merit certificates or even altering marks in exam records if they have been scanned and digitally stored.

2. Previous Work

Work has been done prior to this paper in the field of digital copy-move forgeries. The two most commonly used approaches have been block-based detection techniques and feature based detection techniques. Block based techniques predominantly deals with pixel based image comparison (taking small blocks of pixels at a time). Whereas feature based techniques use features of an image for their comparison instead of blocks. Feature based technique is transform invariant, that is if appropriate features are selected, invariance to a number of transformations can be achieved.

3. Our Approach

Since the paper deals with only signature forgery detection, feature transformation does not play a vital role in this subject. We use block based image detection technique along with border pixel comparison to achieve most optimum results. Since all the previous papers deal with only a single aspect, our technique is expected to produce a better result. By the use of this novel technique we intend to provide an almost full-proof method for digital signature forgery detections.

3.1 Methods we propose

The paper proposes three basic algorithms which when run one after the other, results in robust forgery detection. We name the three algorithms as follows:

1. Border pixels
2. Block comparison
3. Pixel count

A. Border Pixel algorithm

Border pixel algorithm is a basic algorithm which checks the pixels near the signature block. This algorithm was designed for documents where signatures are an integral part of the documents. These documents are where some signatures are overwritten. We detect these forgeries by checking the pixels near the signature and it compare s it to any other border pixel in the document. If the background color in the signature block varies from the background color in the rest of the document, then the signature is a forgery. This method has certain shortcomings. In order to overcome these faults we use the other two algorithms.

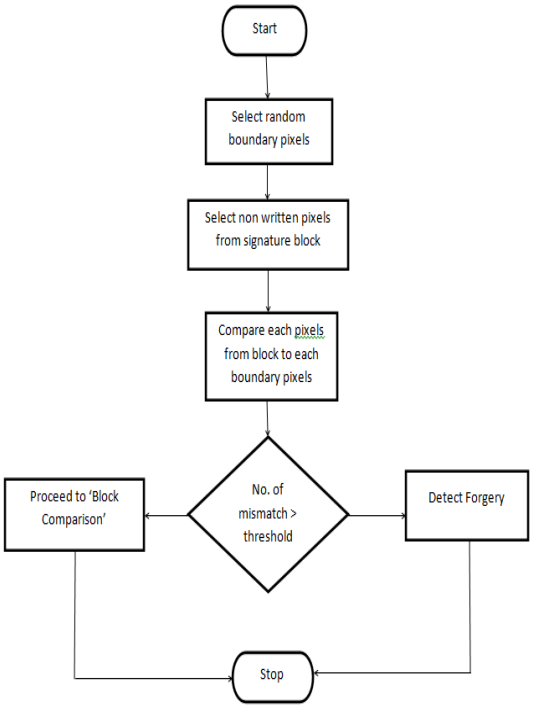

Fig 1 Flow chart for 'Border Pixel'

B. Block Comparison algorithm

Block comparison is the algorithm which is implemented as the next level in the in forgery detection algorithm. The procedure in block comparison tries to find out deletions and cover ups in the image. In this method, a certain blank block of the image is selected & it is checked for authenticity using the border pixels methods. Later this block is compared with all other background blocks of data (the parts with no writing). If there is a subtle mismatch, then it is found.

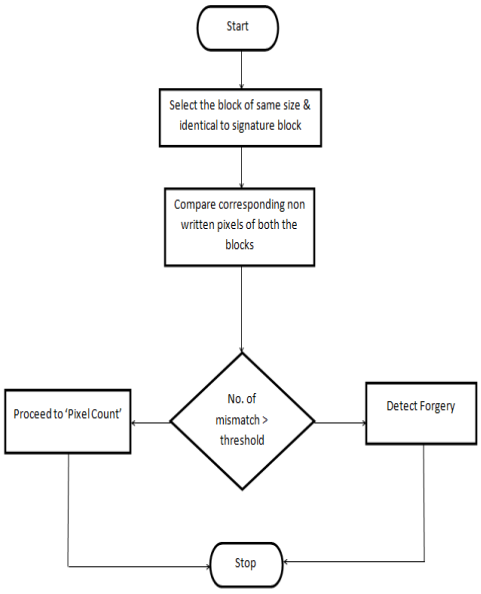

Fig 2 Flow chart for 'Block Comparison'

C. Pixel Count algorithm

The pixel count is the third and final method for detection of forgery or tampering of the document. Pixel count applies a simple yet efficient way to detect changing of the document. In pixel count the total no pixel are counted and then they are compared with the product of resolution of the image. If they are equal then the document is authentic, else the document's quality has been compromised.

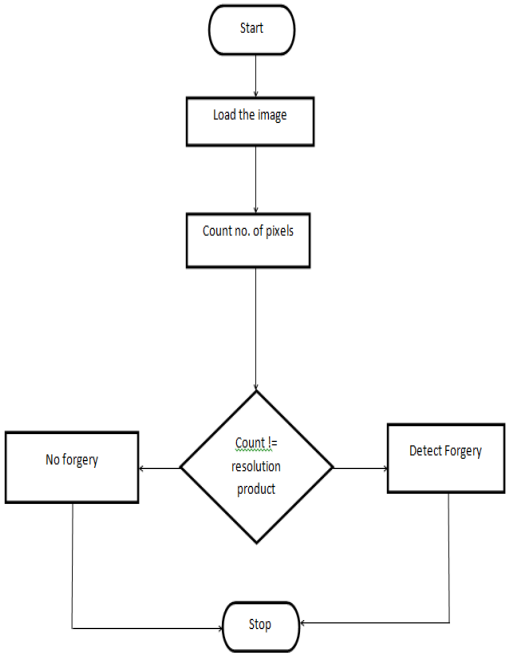

Fig 3 Flow chart for 'Pixel Count'

3.2 Algorithm

1. Select the block of signature from an image of a document which is to be checked for forgery.
2. Apply 'Border pixel algorithm':
   i. Select no. of random pixels which are located at the boundary of a document.
   ii. Select some random non-written pixels from the signature block.
   iii. Compare each pixels from block to each selected boundary pixels using L*a*b* color model.
3. Here, if there are mismatches, it indicates forgery.
4. If 'Border pixel' detects forgery then stop, else proceed to 'Block comparison algorithm'.
5. 'Block comparison':
   i. Select the block of same size as the block under consideration in the document & identical to same.
   ii. Compare corresponding non-written pixels of both the blocks.
6. Here, also same test applies as in Border method & it also has same disadvantage as of Border method.
7. If 'Block comparison' detects forgery then stop, else proceed to 'Pixel Count algorithm'.
8. 'Pixel count':-
   i. Count the no. of pixels.
   ii. If the no. of pixels is greater or less than the resolution product, then conclude forgery.
9. 'Pixel count' is a fool-proof method, which eliminates all the doubts regarding forgery & provides the result.

'Pixel count' is much more efficient than 'Border pixel' or 'Block comparison', but it takes more time. Thus, to minimize the complexity 'Border pixel' and 'Block comparison' are applied before 'Pixel Count'.

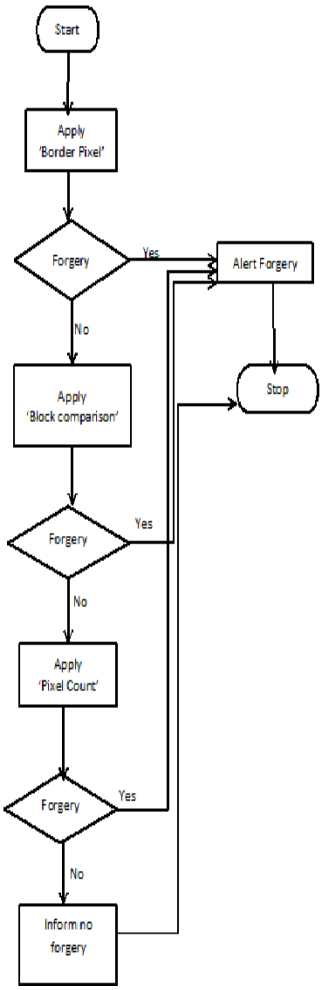

Fig 4 Flow chart for entire process

4. Conclusions/Future Scope

The method proposed in this paper can be implemented and improved accordingly. If this method is implemented then the software can be used in many countries which

are undergoing digitization of their old records. This technique helps everyone, even the common man to scan their own documents and check for authenticity. This method can be improved by covering other types of forgeries like signature forgery, forged letter head/Stamp etc.

References

[1] Offline Signature Verification Using Critical Region Matching by Bansal, A.; Nemmikanti, P.; Kumar, P.
[2] Signature verification using fractal transformation by Kai Huang; Hong Yan
[3] Signature verification and forgery detection system by Yusof, M.H.M.; Madasu, V.K.
[4] Detecting copy-paste forgeries using transform-invariant features by Kakar, P.; Sudha, N.
[5] Robust method for detection of copy-move forgery in digital images by Khan, S.; Kulkarni, A.
[6] Pseudo-Coloring with Histogram Interpolation by Cheng-Hsiung Hsieh; Chih-Ming Lin; Fung-Jung Chang
[7] Study on a Image Matching Algorithm Based on Sphere Similarity of Color Histogram Intersection by Yihong Lu; Jia Hu; Decai Huang

Anirudh Prabhu is a student from St. Francis Institute of Technology, Mumbai. He is currently pursuing a Bachelor's Degree in Computer Engineering. His area of interest lies in Human Computer Interaction and its Applications.

Zil Shah is also from St. Francis Institute of Technology, Mumbai. His area of interest is Computer Visualization.

Manan Shah is studying in St. Francis Institute of Technology, Mumbai. His area of interest is Game Development.