

# A REVIEW OF TRENDS IN DIGITAL IMAGE PROCESSING FOR FORENSIC CONSIDERATION

Sapna Sameria<sup>1</sup>, Vaibhav Saran<sup>2</sup>, A.K.Gupta<sup>3</sup>

Department of Forensic Science

Sam Higginbottom Institute of agriculture Technology & Sciences

Deemed to be University, Allahabad

[sameria.sapna@gmail.com](mailto:sameria.sapna@gmail.com); [drvaibhavsaran@gmail.com](mailto:drvaibhavsaran@gmail.com); [akgupta\\_aaidu10@yahoo.co.in](mailto:akgupta_aaidu10@yahoo.co.in)

## ABSTRACT

Traditionally, our main form of transmission and storage for information has been by paper documents. But nowadays, most of the documents are exclusively electronically formed for better storage and efficient processing. Thus, digitalizing and hence making the field of Forensic Document examination to improve and go hand in hand with the trend as it has become very easy for a person to manipulate with any kind of document with the help of various image manipulation software. This paper refers the review of digital techniques used in the forensic analysis of the various kinds of documents. Also, the authors report that less work has been done on offline scanned documents and have suggested the need of use of latest Image Processing tools for the advancement of the related work.

**Keywords - Image Processing, Documents, Forensic**

## 1. INTRODUCTION

The analysis of Documents through Digital Image Processing has been as old as forgeries started emerging through these softwares. With the dramatic growth and widespread applicability of digitalization of documents, the forensic questioned document community has encountered

difficulty visualizing obliterated and altered handwriting using conventional methods. Over the past thirty years there has been a limited amount of research into using computers to enhance and automate the analysis performed by forensic document examiners. The technique of analysis of questioned documents for any alteration with the digital image processing is more accurate, non-destructive, faster and cheaper than other conventional methods of TLC and VSC. Thus, there is a need of a set of tools that can be applied to the image to check its authenticity and reach a conclusion to convince the court of law.

Some admirable work has been done in the related field by various researchers as described in the reviews below:

**Queiroz (1998)** presented techniques that allowed the processing of JPEG-compressed data without decompressing it, i.e., operations were performed in the "JPEG-compressed" domain. Techniques were presented for scaling, previewing, rotating, mirroring, cropping, recompressing, and segmenting JPEG-compressed data. While most of the results were applied to any image, he focussed on scanned documents as a primary image source.

**Carrier (2003)** used the theory of abstraction layers to describe the purpose and goals of digital forensic analysis tools. Abstraction layers were not a new concept but its usage in digital forensic analysis is not well documented. Using abstraction layers, he identified where tools can introduce errors and provide requirements that the tools must follow. His work examined the nature of tools in digital and proposed definitions and requirements.

**Srihari & Leedham (2003)** surveyed efforts to establish the scientific basis of forensic document examination – some of which are based on computational theories – as well as software tools to assist document examiners. They include: computer systems to provide the degree of match of questioned and known documents, systems that narrow – down the search from a repository of documents with known writers and tools that compare features and provide visualisation to assist the document examiner. In their paper, they reviewed some of the key techniques and results that were published over the past few years in providing support and computer- based tools to assist forensic document examination.

**Lukas *et al.* (2006)** presented a new approach to detection of forgeries in digital images under the assumption that either the camera that took the image is available or other images taken by that camera are available. Their method was based on detecting the presence of the camera pattern noise, which is a unique stochastic characteristic of imaging sensors, in individual regions in the image. The forged region was determined as the one that lacks the pattern noise. The presence of the noise is established using correlation as in detection of spread spectrum watermarks. They proposed two approaches- one where the user selects an area for integrity verification. Second, method automatically determines the forged area without assuming any prior

knowledge. They tested the methods both on examples of real forgeries and on non forged images.

**Johnson & Farid (2007)** described a technique for exposing digital image fakes by detecting inconsistencies in lighting. They showed how to approximate complex lighting environment with a low-dimensional model and, further, how to estimate the model's parameter from a single image. Inconsistencies in the lighting model were then used as evidence of tampering.

**Akram *et al.* (2010)** provided an overview of various methods used for digital image processing using three main components: Pre-Processing, Feature Extraction and the Classification. Their article examined the various methods used for document image processing in order to achieve a processed document having high quality, accuracy and fast retrieval.

**Maini & Aggarwal (2010)** presented the comparative analysis of various image edge detection techniques. They developed the software using MATLAB 7.0. They reported that Canny's edge detection algorithm performs better than all the operators under almost all scenarios.

**Shivakumar & Baboo (2011)** proposed a technique to detect copy – move forgery based on SURF and KD- Tree for multidimensional data matching. In this work demonstrate method with high resolution images affected by Copy- Move forgery.

**Nigam & Mishra (2011)** used a novel approach to decipher the obliteration by using commercially available image processing software Adobe Photoshop Version 7.0 instead of any conventional method. In their first study a graphite pencil handwriting obliterated with ballpoint which cannot be discerned visually are taken for experimental purpose and in second study a case of

addition and alteration in handwriting was discussed. To decipher the hidden and altered content, they used techniques like tonal adjustment using curves, brightness/contrast and threshold mode. The application of the tool is non destructive in nature and support to almost all types of image file formats. The results obtained by this tool were visually very effective for court presentation as well as interpretation.

**Deshpande & Kanikar (2012)**

discussed classification of image forgery detection techniques and important techniques for pixel based forgery detection. But the approach takes into account only shifting of copied regions. Another technique is discussed for fast copy-move detection. Then both the approaches are analysed and compared.

**O'Brien & Farid (2012)** described a new forensic technique that focused on geometric inconsistencies that arise when fake reflections are inserted into a photograph or when a photograph containing reflections is manipulated. This analysis employed basic rules of reflective geometry and linear perspective projection, makes minimal assumptions about the scene geometry, and only requires the user to identify corresponding points on an object and its reflection. The analysis was also insensitive to common image editing operations such as resampling, color manipulations, and lossy compression. They demonstrated this technique with both visually plausible forgeries of our own creation and commercially produced forgeries.

**Pan et al.(2012)** studied the concept of image splicing which is a simple and common image tampering operation, where a selected region from an image is pasted into another image with the aim to change its content. Their study was based on the fact that images from different

origins tend to have different amount of noise introduced by the sensors or post-processing steps, we describe an effective method to expose image splicing by detecting inconsistencies in local noise variances. Their method estimated local noise variances based on an observation that kurtosis values of natural images in band-pass filtered domains tend to concentrate around a constant value, and is accelerated by the use of integral image. They demonstrated the efficacy and robustness of our method based on several sets of forged images generated with image splicing.

**Murali et al. (2012)** proposed methodologies to identify unbelievably manipulated digital photo images and succeeded to identify forged region by given only the forged image. Formats are additive tag for every file system and contents are relatively expressed with extension based on most popular digital camera uses JPEG and other image formats like png, bmp etc. They have designed an algorithm running behind with concept of abnormal anomalies and identify the forgery regions.

**Dezfoli et al. (2013)** attempted to look into trends of applications of digital forensics and security at hand in various aspects and provide some estimation about the future research trends in this area. They studies that rapid evolution of computers and mobile phones has caused these devices to be used in criminal activities. Providing appropriate and sufficient security measures is a difficult job due to complexity of devices which makes investigating computer crimes in the cyber world.

**Saran et al. (2013)** studied the resemblance of slant in handwriting of closed genotypic family members in a sample of 360 families, using computational method based on MATLAB, followed by the statistical

evaluation of the parameter. Their study showed a significant resemblance of slant of offspring's of family members.

**Birajdar & Mankar (2013)** overviewed that manipulation of digital images has become easy due to powerful computers, advanced photo-editing software computers, advanced photo-editing software packages and high resolution capturing devices. Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt was made to survey the recent developments in the field of digital image forgery detection and complete bibliography is presented on blind methods for forgery detection. First, various image forgery detection techniques were classified and then its generalized structure was developed. An overview of passive image authentication was presented and the existing blind forgery detection techniques were reviewed. The present status of image forgery detection technique was also discussed along with a recommendation for future research.

**Remya (2014)** focused onto the property of contrast enhancement which is mainly to adjust the brightness globally. Using the most latest technology in the literature : two algorithms to find the contrast enhancement for the manipulation of digital images. First algorithm focus on the detection of global contrast enhancement applied to previously JPEG compressed images. Here images are converted to non-overlapping blocks ie histogram of images, then gap/peak detection of blocks are performed. Locate the gap and peak bins. Pixel value mappings are analyzed theoretically, and difference between the pictures are obtained by identifying the zero-height gap fingerprints. Second method is used to identify the composite image created by enforcing contrast adjustment on any of the source

regions/over the entire region of the image. This is followed by finding out the positions of the peak/gap bins, and clustering them for identifying the contrast enhancement applied to different source regions. Finally checking for the similarity between peak/gap bins reference vectors calculated for both forged region and unforger region. If it is found to be dissimilar then the image is treated as a forged one.

**Burvin & Esther (2014)** studied the most common form of digital image or photographic manipulation operation which is known as image splicing or image composition. They defined it as the process that crops and paste regions from same or separate sources. Thus, they analysed various automatic image forensic techniques for detecting digital image splicing.

**Konstanskis & Yannakooudakis et al. (2014)** used MATLAB and found a system for writer identification from the historical lines of text, where features are extracted and used to recognise individuals. Their main goal was to analyse documents of different writing styles in order to identify the writers. They considered a complete 2D probability distribution that takes into account all possible combinations of angle pairs, outperforming original code. They took the images from the Greek digital library Helliomnimon available online.

## 2. CONCLUSION

Significant work has been done through various Digital Image Processing software and its tools, even MATLAB, in the field of Handwriting analysis and various aspects of Image Forgery. These methods have been successful in extracting the features and establish individuality. However, no such work has been reported where Offline Scanned Documents are analysed for any kind of alteration present. Thus, there is a need to come up with the latest Image Processing Toolbox with

which alterations in Offline Scanned Documents and other forms of documents can be identified and a more precise foolproof opinion can be given in the court of law.

### 3. REFERENCES

- [1] **Akram, S., Dar, M.U.D. and Quyoum, A., (November 2010)** “Document Image Processing – A review”, *International Journal of Computer Applications*, **Volume 10**, Issue 5, pp. 35-40.
- [2] **Birajdar, G. J. and Mankar, V. H. (October 2013)** “Digital Image Forgery Detection Using Passive Techniques: A Survey”, *Elsevier – Digital Investigation*, **Volume 10**, Issue 3, pp. 226-245.
- [3] **Burvin, P. S. and Esther, J. M., (march-april 2014)** “Analyses of Digital Image Splicing Detection”, *IOSR Journal of Computer Engineering*, **Volume 16**, Issue 2, pp. 10-13.
- [4] **Carrier, B., (Winter 2003)** “Defining Digital Forensic Examination and Analyses Tools Using Abstraction Layers”, *International Journal of Digital Evidence*, **Volume 1**, Issue 4, pp. 1-12.
- [5] **Deshpande, P. and Kanikar, P. (2012)** “Pixel based digital image Forgery Detection Technique”, *International Journal of Engineering Research and applications*, **vol. 2**, pp. 539- 543.s
- [6] **Dezfoli, F. N.; Dehghantanha, A.; Mahmoud, R. And Binti, N. F., (2013)** “Digital Forensic Trends and Future”, *International Journal of Cyber-Security and Digital Forensics*, **Volume 2**, Issue 2, pp. 48-76.
- [7] **Johnson, M. K. and Farid, H., (August 2007)** “Exposing Digital Forgeries in Complex Lighting Environments”, *IEEE transactions in Information Forensics and Security*, **Volume 2**, Issue 3.
- [8] **Konstantakis, M. K. and Yannakoudakis, E. J., (October 2014)** “A Writer Identification System of Greek Historical Documents using MATLAB”, *International Journal of Emerging Technology and Advanced Engineering*, **Volume 4**, Issue 10, pp. 609– 617.
- [9] **Lukas, J.; Fridrich, J. and Goljan, M., (February 2006)** “Detecting Digital Image Forgeries Using Sensor Pattern Noise”, *Storage and Retrieval for Image and Video Database*, **Volume 6072**, pp 362-372.
- [10] **Maini, R. and Aggarwal, H., (2010)** “Study and Comparison of the Various Image Edge Detection Techniques”, *International Journal of Image Processing*, **Volume 3**, Issue 1, pp. 1-12.
- [11] **Murali, S.; Chhitapur, G. B.; S, P. H. and Anami, B. S., (December 2012)** “Comparison and Analyses of Photo Image Forgery Detection Techniques”, *International Journal on Computational Sciences & Applications*, **Volume 2**, Issue 6, pp. 45-56.
- [12] **Nigam, R. K. And Mishra, P. (2011)** “Forensic Examination of Obliteration and Alteration in Handwriting using Digital Image Processing”, *Malaysian Journal of Forensic Sciences*, **Volume 2**, Issue 1, pp. 64-66.

- [13] **O'Brien, J. F. and Farid, H., (January 2012)** "Exposing Photo Manipulation with Inconsistent Reflections", *ACM Transactions on Graphics*, **Volume 31**, Issue 1.
- [14] **Pan, X.; Zhang, X. and Lyu, S., (2012)** "Exposing Image Splicing with Inconsistent Local Noise Variances", *Proceedings of IEEE International Conference of Computer Photography*, pp. 1-10.
- [15] **Queiroz, R. L., (December 1998)** "Processing JPEG-Compressed Images and Documents", *IEEE Transactions on Image Processing*, **Volume 7**, Issue 12, pp. 1661-1672.
- [16] **S, Remya., (Sep-Oct 2014)** "Digital Image Forgery Detection by Contrast Enhancement", *IOSR Journal of Computer Engineering*, **Volume 16**, Issue 5, Version IX, pp. 1-7.
- [17] **Saran, V.; Kumar, S.; Ahmed, S. and Gupta, A. K., (October 2013)** "Similarities of Slant in Handwriting of Close Genotypic Family Members", *International Journal of Computer and Electronics Research*, **Volume 2**, Issue 5, pp. 648-650.
- [18] **Shivakumar, B. L. and Baboo, S. S., (July 2011)** "Detection of Region Duplication Forgery in Digital Images using SURF", *International Journal of Computer Science Issues*, **Volume 8**, Issue 4, pp. 199-205.
- [19] **Srihari, S. N. and Leedhan, G., (November 2003)** "A Survey of Computer Methods in Forensic Document Examination", *Proceedings of the 11<sup>th</sup> Conference of the International Graphonomics Society*, pp. 278-281.