Proceedings of the 34th Accra Bespoke Multidisciplinary Innovations Conference & the Africa AI Stakeholders Summit
Academic City University College, Accra Ghana
19th – 21st December, 2022
www.isteams.net/accrabespoke2022

Towards the Development of Image Forgery Detection System Using Hashing Technique

[1]Maisango, Rakiya Aliyu, [2]Longe, O.B. [3]Dada Aborisade, [4]Idris Abubakar Muhammad & [5]Auwal, Yunusa Hassan

[1,2,3,]Cyber Security Programme, Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Abuja, Nigeria
Education Management Information Systems EMIS Special Schools Management Board Bauchi, Bauchi State, Nigeria
[4]Directorate of Management, Information Systems DMIS, National Open University of Nigeria, Abuja, Nigeria
[5]Energy Metering Engineer, Department of Technical Services, No 1 Niger Street Post Office Road, KEDCO HQ, Kano, Nigeria
E-mails: [1]rakmaisango@gmail.com; [4]midris@noun.edu.ng; [2]longeolumide@fulbrightmail.org; auwaluyunusa1986@gmail.com

ABSTRACT

The advancement of image manipulation techniques is a double-edged sword. On one hand, it facilitates the beautification of photos and thereby encourages people to express and share their ideas on visual arts of photo editing, on the other hand, it is much easier to forge the content of a given image without leaving any visible clues and thus helps forgers to deliver fake information. Forged photographs are appearing with a growing frequency. Without any doubt image authenticity now is a big matter of concern. Our efforts in this work is directed at further strengthening the ability to discover forged images. We inted to achieve this by employing hashing functions as a technique to enhace image forgery detection.

Keywords: Hashing, Forgery, Detection, Images, Techniques, Security, Transmission

Proceedings Reference Format
Maisango, Rakiya Aliyu, Idris Abubakar Muhammad, Longe, O.B. & Dada Aborisade (2022): Development of Image Forgery Detection System Using Hashing Technique. Proceedings of the 34th Accra Bespoke Multidisciplinary Innovations Conference & The Africa AI Stakeholders Summit. Academic City University College, Accra Ghana, 2022.
Pp 103-110. www.isteams.net/accrabespoke2022

1. INTRODUCTION

Digital image is an image or picture represented digitally. It is a numeric representation, normally binary, of a two-dimensional image. The digital image is a crucial means that is used to distribute information in internet, that is extensively used in almost every field (Zhang and Wang, 2018). With the advent of internet, images and videos are the most vulnerable media that can be exploited by criminals to manipulate for hiding the evidence of the crime. Sai and Satyanarayana, (2022) says that most people are not able to discriminate the real and fake images or edited documents, therefore the chances of forgery improved. Digital forgery is now easier with the advent of powerful and easily available manipulation tools over the internet and thus poses a huge threat to the authenticity of images and videos (Zhang and Wang, 2018).

There is no guarantee that the evidences in the form of images and videos are from an authentic source and also without manipulation and hence cannot be considered as strong evidence in the court of law. Also, it is difficult to detect such forgeries with the conventional forgery detection tools. Although many researchers have proposed advance forensic tools, to detect forgeries done using various manipulation tools, there has always been a race between researchers to develop more efficient forgery detection tools and the forgers to come up with more powerful manipulation technique (Nabi, 2022). Access to technologies like mobile phones contributes to the significant increase in the volume of digital visual data (images and videos). In addition, photo editing software is becoming increasingly powerful and easy to use. In some cases, these tools can be utilized to produce forgeries with the objective to change the semantic meaning of a photo or a video e.g. fake news (Nabi, 2022). The manipulation of digital images has become very common in recent years. Thus, it is possible to cut, clone, and resize an image very quickly, which makes it challenging to validate the integrity and authenticity of images. Furthermore, digital images can be used by forensic experts in their forensic investigations. In this context, digital image forensics (DIF) has emerged as an essential area of expertise focused on verifying the authenticity and integrity of digital files (Ferreira et al., 2020).

1.2 Motivation for the Study

The motivation to go into this special area of cybersecurity is bound out of the incessant manipulation of digital images thus creating a threat towards the authenticity of an image done by individuals and criminals. The urge to curb or minimize these excesses therefore gingers my deep interest to explore more into digital image forgery detection whose goal is to **verify the authenticity of digital images**. Seminar is a requirement for the Masters program in ACETEL also as a Cyber Security Student the issue of security is very vital more especially nowadays that Cyber Crime is being exploited at a very tremendous rate. Digital image forensic is one of the crucial issues baffling our communities.

1.3 Research Problem

The advancement of image manipulation techniques is a double-edged sword. On one hand, it facilitates the beautification of photos and thereby encourages people to express and share their ideas on visual arts of photo editing, on the other hand, it is much easier to forge the content of a given image without leaving any visible clues and thus helps forgers to deliver fake information. Forged photographs are appearing with a growing frequency. Without any doubt image authenticity now is a big matter of concern (Ferreira *et al*., 2020).

1.4 Aim and Objectives

The aim of this work is to develop image forgery detection technique using hashing technique. This aim will be achieved using the following objectives:

1. Analyzing different types of image forgery techniques
2. Discussion of available image forgery detection techniques.
3. Development of image tampering detection method.
4. Testing the efficiency of the image detection technique.

2. RELATED WORKS

Image Manipulation, Forgery, tampering or image editing refers to any operation that can be done to a digital image by software on a computer or other digital devices such as tablets and mobile phones. Common image manipulations not only include pixel-level operations such as resampling an image to reduce its size, but also include content-level operations such as removing an object from a digital photo. No matter which level operations are applied, an original image exists for each manipulation product (Katzenbeisser, 2000). One can know the changes by simply comparing the product to the original. According to different patterns of these changes, one can identify the subcategories of image manipulation. For example, image steganography embeds additional information in the image by slightly altering the image pixels at certain positions (Katzenbeisser, 2000). The changes made to the original image are relatively subtle with respect to the magnitude of pixel values in the image, e.g., the least significant bit (LSB) embedding method alters the pixel values by only -1 or +1. Therefore, it is hard to see the manipulation clues by visual comparison between the product and the original.

There must be an original for a tampered image; the tampered image contains both tampered regions and un- tampered areas . It would be very easy for one to identify the tampered regions by visually comparing the product to the original. However, when one is given a tampered image without its original as the reference, it is hard to judge the forgery (Wang *et al*., 2006). Editing a real-world photo through computer software or mobile applications is one of the easiest things one can do today before sharing the doctored image on one's social networking sites. Although most people do it for fun, it is suspectable if one concealed an object or changed someone's face within the image. Before questioning the intention behind the editing operations, we need to first identify how and which part of the image has been manipulated. It therefore demands automatic tools for identifying the intrinsic difference between authentic images and tampered images (Lilei, 2018).

Image forgery detection methods are organized into two classes, namely, active and passive techniques. The active techniques require prior knowledge of elements initially associated with the original image, such as watermarking or steganographic data (Lilei, 2018). On the other hand, passive techniques do not rely on previous information regarding the original image to determine its authenticity. These techniques involve determining whether an image has undergone typical forging operations such as copy-move or spatial transformations (resizing, rotation, and stretching) (Lilei, 2018).

Different Types Of Image Forgeries

- **Copy-move forgery** Copy-move is one of the most widespread image tampering technique, also it is very difficult to identify this type forgery as the copied image is taken from the same image. "In Copy-Move image forgery, a part of the image is copied and pasted to another part of the same image. It simply requires the pasting of image blocks in same image and hiding important information or object from the image." (Kaur and Sharma, 2015) This method involves copying of some area of an image superimposing it on some other area of the same image.
- **Image Splicing** "Image splicing is a technology of image compositing by combining image fragments from the same or different images without further post-processing such as

smoothing of boundaries among different fragments." (Zhang, 2008). Image splicing forgery involves composition or merging of two or more images changing the original image significantly to produce a forged image.

- **Image Retouching** "In Image Retouching, the images are less modified. It just enhances some features of the image. There are several subtypes of digital image retouching, mainly technical retouching and creative retouching." (Burvin and Esther, 2014) .Image is carried out to either reduce or improve certain features of the image. Retouching may require rotation, scaling, or stretching of an image before combining it with other image
- **Lighting Condition** This type of forgery can be easily done by splicing two different images together. Often such spliced images are from different scene and having different lightning conditions and so it is very difficult for image forger to match exact lightning condition of one image with other. Such variation in lighting conditions can be used to identify the tempering in the image (Johnson and Farid, 2005).

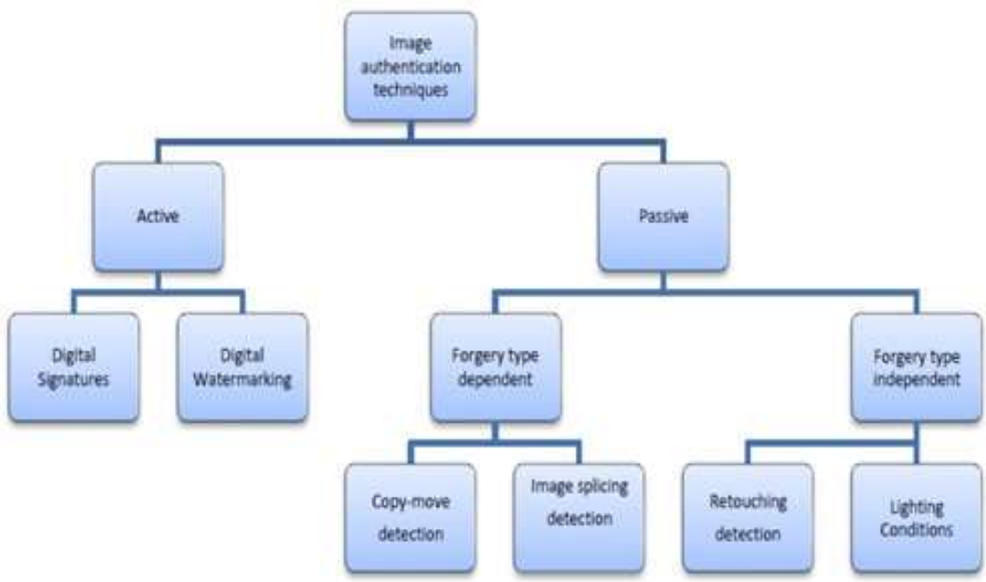

Figure 1 A **comprehensive study on image forgery**
Source: tabular representation of types of image forgery - Search (bing.com)

3. RESEARCH METHODOLOGY

In the proposed system we are enhancing the accuracy and efficiency rate of detecting forgery in the existing system. In this, we use two techniques for detection of the duplicate region. The first technique is by applying PCA (Principle Component Analysis) on the small fix size image Block 32x32. The eigenvalues and eigenvector for each block are calculated.

After applying lexicographic sorting, the duplicate regions of the image are automatically detected. In other proposed algorithm, matches are been searched among the DCT representation of image segments. DCT coefficients are lexicographically arranged and adjacent identical pairs are considered as potentially tampered regions to avoid the computational burden of a brute force comparison. After the lexicographical sorting, similar blocks are detected and forged region is found. The level of quantization is first estimated for each of 64 DCT frequencies from a region of the image which is presumed to be authentic. The inconsistencies between the DCT coefficients (D) and the estimated amount of quantization (Q) are computed as Variations in B across the image.

4. SYSTEM IMPLEMENTATION

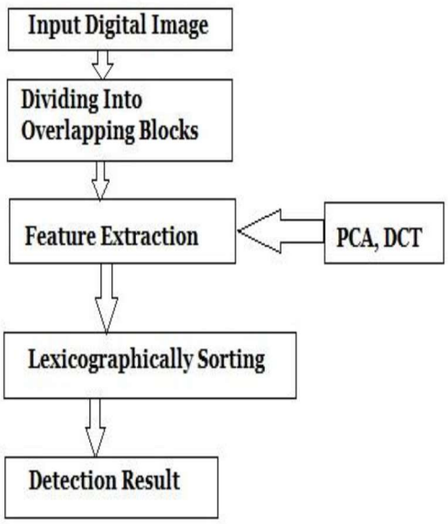

Figure 2: Block Diagram for System of Image Forgery Detection

Input Digital Image:
The input image for our system can be taken from any local storage. For this, we can take help of UI with browse function; to import the image.

Dividing Into Overlapping Block:
The input image is divided into the blocks which are overlapping in nature. This is done because working on the whole image in one go can be extra overhead for the algorithms which can result in lowering the accuracy and efficiency of the system. These overlapping blocks also help us to find the region of the forgery after the successful working of the algorithms because overlapping blocks tells us about the neighbouring pixels in the image.

Feature Extraction—PCA, DCT:

PCA (Principal Component Analysis) is the common feature extraction method in image processing. PCA finds the eigenvectors of a covariance matrix with the highest eigenvalues and then use those to extract the data into a new sub-space of equal or fewer dimensions.

Table 1: Comparative study of existing techniques.

S. No.	Paper title	Method used	Tampering detection type	Pros/cons	Publication year
1.	Detection of copy-move forgery in digital image [13]	DCT	Copy-move region is detected	Will not work in noisy image	2003
2.	Exposing digital forgeries by detecting duplicated image regions [14]	PCA	Exact copy-move region is detected automatically	Time complexity is high	2004
3.	Robust detection of region duplication in digital image [16]	Similarity matching	Copy-move region detected in noisy conditions	Time complexity is reduced [14]	2006
4.	A sorted neighbourhood approach for detecting duplicate reason based on DWT and SVD [10]	DWT-SVD	Efficiently detects forged region	Time complexity is less compared to other algorithms [14]	2007
5.	A new approach for detecting copy-move forgery detection in digital image [17]	DWT	Exact copy-move region is detected	Works well in noisy and compressed image	2008
6.	Detection of copy-move forgery in digital images using SIFT algorithm [9]	SIFT	Copy-move region is detected	Detects false result also	2008
7.	Identifying tampered regions using singular value decomposition in Digital image forensics [8]	SVD	Copy-Move region is detected accurately	Will not work in highly noised & compressed image	2008
8.	Fast copy-move forgery detection [15]	Improved PCA	Exact Copy-Move region is detected	Works well in noisy, compressed image	2009
9.	Detect digital image splicing with visual cues [6]	DW-VAM	In spliced image, forged region is detected	Work only in the Splicing	2009
10.	Fast, automatic and fine-grained tempered JPEG image detection via DCT coefficient analysis [19]	Double Quantization – DCT	Tampered region is detected accurately	Works only in JPEG Format	2009
11.	Copy-move forgery detection in digital image [18]	SVD	Forged region is detected	Will not work well in noisy image	2010
12.	DWT-DCT based Copy-Move image forgery detection [11]	DCT-DWT	Forged region is detected accurately	Will not work in highly compressed image	2011
13.	An integrated technique for splicing and copy-move image forgery detection [7]	DCT-SURF	Copy-Move and spliced both region detected	Works well for both copy-move and splicing	2011
14.	Improved DCT-based detection of copy-move forgery in digital image [22]	DCT	Copy-move region detected accurately	Works well if the image blurred & compressed	2011
15.	A robust detection algorithm for copy move forgery in a digital image [23]	DCT	Exact copy-move region detected	Works well if the image is noisy or blurred	2012

It converts a matrix of n features into a new data set of less than n features that's why it reduces the number of features by constructing a new one with smaller number variable which captures a significant portion of information found in the original features. This means that a featured image can be processed similarly as an ordinary image generated by an image sensor. DCT is a powerful transform to extract proper feature for image processing. After applying DCT to the entire face image, some of the coefficients are selected to construct the feature vector. Most of the approaches in a zig-zag manner. In some cases, the low-frequency coefficients are discarded to its variation. DCT can be used to achieve a higher true feature extracting rate by using discriminate coefficients (DCS) as a feature vector. Discrimination power analysis (DPA) is based on DCT Coefficient properties and discrimination concepts. It searches the coefficient which has both powers to discriminate classes better than others. The DTA based approach achieves the performance of PCA of better with less coefficient.

5. EXPECTED CONTRIBUTION TO KNOWLEDGE

The detection of image manipulation is very important because an image can be used as legal evidence, in forensics investigations, and in many other fields. The pixel-based image forgery detection aims to **verify the authenticity of digital images without any prior knowledge of the original image.** Digital images are used to convey information as we humans tend to trust what we perceive. Owing to the development in tools and technology, manipulation of digital image is becoming drastically easy and more frequent. Digital images are forged beyond visual comprehension for the ulterior motives. Forgery detection in digital images is necessary to unravel the truth.

6. CONCLUSION

Image forgery is a big threat as new and new tools are available with cheaper price for forging digital image. As there are many types of image forgeries, viz, copy-move forgery, image splicing, image retouching, and lighting condition, it is very difficult to have an image forgery identification techniques which applies to all types of forgeries

REFERENCES

1. Berthet and J. -L. Dugelay,2020 "A review of data preprocessing modules in digital image forensics methods using deep learning," 2020 IEEE International Conference on Visual Communications and Image Processing (VCIP),pp. 281-284, doi: 10.1109/VCIP49819.2020.9301880.
2. William D. Ferreira, Cristiane B.R. Ferreira, Gelson da Cruz Júnior, Fabrizzio Soares,2020 A review of Digital image forensics, Computers & Electrical Engineering, Volume 85, ,106685,
3. ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2020.106685.
4. (https://www.sciencedirect.com/science/article/pii/S0045790620305401)
5. Zheng, Lilei & Zhang, Ying & Thing, Vrizlynn. (2018). A Survey on Image Tampering and Its Detection in Real-world Photos. Journal of Visual Communication and Image Representation. 10.1016/j.jvcir.2018.12.022.

6. Nabi, S.T., Kumar, M., Singh, P. *et al.2022"* A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions". *Multimedia Systems* **28,** 939–992 (2022). https://doi.org/10.1007/s00530-021-00873-8
7. @http://cs231n.github.io/convolutional-networks/
8. Katzenbeisser S, Petitcolas F. 2000, Information hiding techniques for steganography and digital watermarking. Artech house; .
9. Farid H. 2004 Creating and detecting doctored and virtual images: Implications to the child pornography prevention act. Department of Computer 970 Science, Dartmouth College, TR2004-518 2004;13.
10. Rotman B. Becoming beside ourselves 2008 The alphabet, ghosts, and distributed human being. Duke University Press; .
11. Wang W, Dong J, Tan T 2009. A survey of passive image tampering detection. In: IWDW; vol. 9. Springer;:308–22.
12. He J, Lin Z, Wang L, Tang X. 2006 Detecting doctored JPEG images via DCT coefficient analysis. In: Proceedings of ECCV. :423–35.
13. Sai Achyuth, P., Satyanarayana, V. (2023). Image Forgery Detection Techniques: A Brief Review. In: Yadav, S., Haleem, A., Arora, P.K., Kumar, H. (eds) Proceedings of Second International Conference in Mechanical and Energy Technology. Smart Innovation, Systems and Technologies, vol 290. Springer, Singapore. https://doi.org/10.1007/978-981-19-0108-9_37
14. Xiaoqiang zhang and Xuesong wang, 2018, "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem." IEEE Access, vol.6.
15. Amanpreet Kaur and Richa Sharma, 2013 "Optimization of Copy-Move Forgery Detection Technique," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4,
16. Zhen Zhang, Ying Zhou, Jiquan Kang, and Yuan Ren, "Study of Image Splicing Detection," Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, vol. 5226, pp. 1103-1110, 2008.
17. Susama G Rasse, "Review of Detection of Digital Image splicing Forgeries with illumination color estimation," International Journal of Emerging Research in Management & Technology, vol. 3, no. 3.
18. [4] P. Sabeena Burvin and J. Monica Esther, "Analysis of Digital Image Splicing Detection," IOSR Journal of Computer Engineering, vol. 16, no. 2, pp. 10-13, Mar-Apr 2014.
19. [5] Micah K. Johnson and Hany Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," ACM Multimedia and Security Workshop, 2005.