Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 7, July 2019, pg.105 – 111

Detecting Digital Forgery Using Image Processing in Zero Day Attack

L. Haider Hameed Razzaq; Dr. Ghadah Al-Khafaji
Dept. of Computer Science, College of Science, Mustansiriyah University
Dept. of Computer Science, College of Science, Baghdad University
haideritsec@uomustansiriyah.edu.iq
Hgkta2012@scbaghdad.edu.iq, hgkta2012@yahoo.com

1- Abstract

Digital image processing represent the identity for the last century in computer graphic. Many companies started to develop software to meet the significant need for the new technologies, especially these software demanded by movies and films production.

Also, on the personal needs, image processing software are developed to the extent of zero coast for end users. This matter helped wide range of end user to build their skills to be professionals in photography jobs. On the other hands, the priceless of the image processing tools in addition to cheap computer device prices encourages other categories of end users to use these facilities illegally to forge the digital images to produce fake image content.

This research tried to focus on help organizations (In developed countries) who uses normal scanners to convert paper documents into digital images to discover if the stored digital images are forges or still authentic as the first timed scanned in order to use them with the guaranty as reference digital evidences for future. Discovering the technique used to forge the digital image or determine the portion pf the image where the tampering have been done is not considered in this paper.

2- Introduction

Digital imaging have become a characteristic for current and late in previous century, the significant development in mathematical bases pushed the application in this type of application. Many field in image processing are emerged because the high advancement in mathematical background, for instance compression data, enhancement, pattern recognition.

Image processing can be considered as double-edged sword, it can be used to help people, organization/business(s) and governments to solve a lot of problem, but unfortunately, in the same time it can be used for different illegal tasks such as forgery of original image

The forgery itself could be useful in some legal business, for instance movies creator, picturing studios for professionals and hobbies, on the other hand, some criminals can use very professional image processing tools to tamper the original content of the image to make displayed as the same (as much as it can) as the original image with some unnoticeable changed.

The current work tried to focus on the how to detect forgery in the digital image using image processing tools.

3- Image forgery

Linguistically, forgery is defined as the crime of falsely and fraudulently making or altering a document, as stated by (Meriam Webster, 2019)

Based on the history and utilization of digital forgery, there are some questions arises: What ethics are associated with digital forgery? Is the forgery of digital files right or wrong, Acceptable or not? Should people believe anything they see in pictures? Unfortunately, none of these questions till today have clear declaration. The only answer available now is "there are many image editor tools available for free", also these tools are simplified to be used not only by professionals, but also for users with low level skills in computer skills.

4- Mathematical base of digital image

According to (Seacrest, 2006), there are many models to represent image color. RGB is a standard method applied in projectors and monitors, in this method, with a combination of red, green, and blue light, anyone can create a color in the spectrum. So a color is represented by major three numbers: a red value, a green value, and a blue value, all between 0 and 1. For more explanation , 0 mean the lowest value for any color type (red; green air blue) and 1 refer to the maximum value that represent the same original colors, usually in RGB system, maximum vale reach 255 which represented mathematically by 1 Byte lead to the maximum value for all color values equal to 3 bytes.

When combining colors, black is represent the absence of any of the three. In contrast, white represent the combination of all three. The image smallest unit represent by pixel which represent the vales resulted from combination of the three color vales.

Figure 1.(a & b) represent two different segment (areas) of digital image, figure 1.A represent the black portion while Figure 1.B represent the white side.

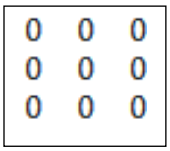


Figure (1.a) segment of black image

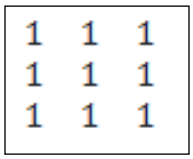


Figure (1.b) segment of black image

So, to change the color for any digital image, all what user need is manipulate the figures that represent the color combination (Intensity)

5- Tampering methods

Many researches have been done in this field of image processing, the results classified the method for different categories, in the next section, and this research will brief the most Common techniques, the major contents and tables derived from (Alex, 2017)

(Alex, 2017) **reviewed many research that already done in the field of tampering digital images as shown in (table 1)**

Table1 Papers states common image operations and detecting techniques

Title of the paper	**Image operation**	**Tamper detection techniques**
"Digital image tamper detection techniques- A comprehensive study"	Retouching, spelling ,copy-paste, cropping, cloning	Edge blurring
"Digital image tamper detection tools"	Copy move, , noising, blurring resize, image splicing	Laplace filter, PCA, DCT, DWT, SVD
"Tampering and copy move forgery detection using SIFT feature"	Copy move, block, feature based methods.	,PCA,DCT,DWT,SIFT
"Image splicing & copy move forgery detection"	Copy move splicing	Multiscale WLD,LBP,LLB,SVM
"Efficient copy move forgery detection for detection for digital images"	image splicing, Copy move	Statistical & block characteristics
"Comparison and analysis of photo image forgery detection techniques "	Copy move, copy paste , copy **create**	JPEG compression analysis, edge detection, localization
"Survey of image forgery detection"	Copy move, cropping cloning splicing ,resize,	Pixel, format, camera physically, geometric based.
"Image forgery detection A survey"	Copy move	JPEG compression, block based
"Image forgery detection based on semantic"		Framework semantic ontology commonsense knowledgebase
"copy move image forgery detection method using steerable pyramid transform and texture descriptor"		SPL,LBP
"Copy move forgery detection based on patch match"		Localization
"Improving the detection and location of duplicated regions in copy move image forgery"		SIFT MIFT localization
"Copy move image forgery detection using mutual information"		Region duplication
"Detection false captioning using common sense reasoning"	Distorting, deletion, insertion, photo montage false captioning	AI (detection duplication). Segmentation classification(ROI)

The above table show rich information for each studied technique

It is obvious that the researches done on Copy-Move operation as tampering technique is higher number compared to the other techniques, because this process is available on all of the software that utilized to process the digital image, also the table show that there are 13 out of 16 different detection techniques are developed. On the other hand, splicing image and insertion tampering technique represent the lowest share of the achieved studies reaching no more than 6 and 1 out of the 16 papers respectively, the reason can be concluded logically depend on the relation concept between the paste and insert process.

It is obvious that all previous studies concerns on studying the methods of tampering and the technique used to discover the forge.

The issue arise here is discussed below scenario With the professional tools used in creation, editing digital image, it is not impossible to overcome the detection techniques, in this case the displayed digital image will considered authentic and treated as formal document. If the tampered digital image result in false value with detection technique, then it will be treated as formal legal document.

Let us imagine a school or university in developed country adopted very simple way to transfer hand written certifications into digital image using light scanner, the image for these papers are stored on Hard Disk drive, DVD or any other media. When beneficiary requested a copy of his/her certificate with degree, it will be easy to manipulate the digital image and make it display in different degrees as tapered in purpose. If the managers relies totally on the method of tempering detection and this technique failed, it will considered the none authentic certification as authentic.

6- Disadvantages of previous studies

The failure reasons regarding using previous approaches are different, but the simple reason is mismatching between the tamper method and detection techniques, the adopted software not necessarily designed to discover the method of tampering.

7- The new attack

"Zero day Knowledge" is A zero-day vulnerability a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals. Applying this attack to digital image yield none identified tapered image even if the software are up to date. The scenario imagining the criminal adapted a new method of tampering which is not studied yet (considered in the Zero Day Interval), all issued document in this term will considered (practically) as authentic since the test result will be positive for authenticity, for more details see (Symantec, 2019).

8- The suggested proposal

For achieving 100% assuring that there is no changing in the digital image pixel, the research suggested to design verification system that consist of two layers

8-1 Layer 1

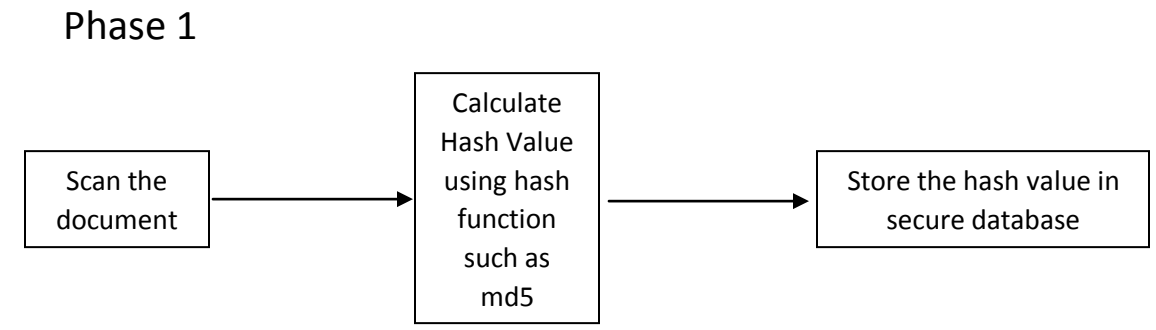
In this layer the verification system will tell the beneficiaries if there is any tapered have been done to the stored image file, by treating the digital image as digital file and calculate the digits value using suitable hashing techniques. This layer does not care of

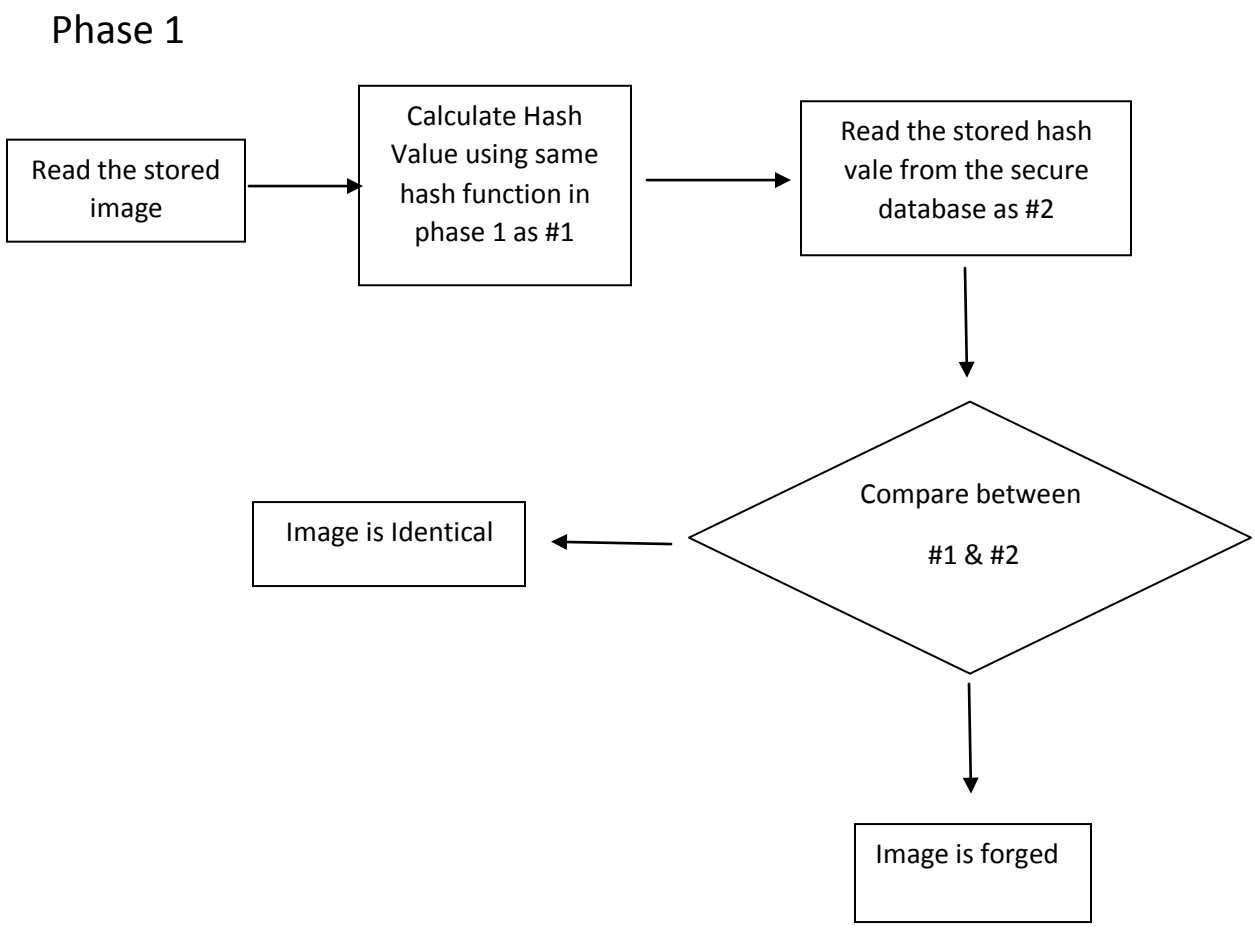
discovering the part of the image where the forge made. Instead, it concern to tell one of two test values (Yes (for tampering) and No (for none tampering).

8-2 Layer two

This layer will executed if the result of layer one was "Yes", then further investigation can be done to determine the portion of the image were the tapering have been made using one of the previous suggested techniques listed in table 1.

The good thing is, even if the technique used to forge the digital image is new approach and considered unknown and there is no specific technique assigned to detect the forge location, the proposed system will answer the main question "is the digital image is Authentic OR Not?"





9- Expected Results

The expected result for this model of verification is ideal, for both type of digital forgery attack (the known attack and zero day attack), both types will be identified in layer one, since it base on digits vale not the pixel value, for the unknown attack (zero day attack), it will be discovered in layer one but fail to fine the right place where the tamper done.

References

[1]. Alex, C. a. (2017). STUDY OF IMAGE TAMPERING AND REVIEW OF TAMPERING DETECTION TECHNIQUES. *International Journal of Advanced Research in Computer Science*, 963-967. Retrieved from STUDY OF IMAGE TAMPERING AND REVIEW OF TAMPERING DETECTION TECHNIQUES.

[2]. *Meriam Webster*. (2019, 3). Retrieved from Meriam Webster: https://www.merriam-webster.com/dictionary/forgery?src=search-dict-box.

[3]. Seacrest, T. (2006). *Mathematical Models of Image Processing.* Retrieved from https://www.math.hmc.edu/seniorthesis/archives/2006/tseacres/tseacres-2006-thesis.pdf.

[4]. Symantec, e. o. (2019). *Emerging Threats*. Retrieved from Symantech: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.

