

IMAGE FORENSICS

TEAM MEMBERS:

MINAL MUKTA (18BCE0826)
TRIPTI MISHRA (18BCE0888)

DIGITAL FORENSICS

FINAL ASSIGNMENT

TEAM: GRAVITY

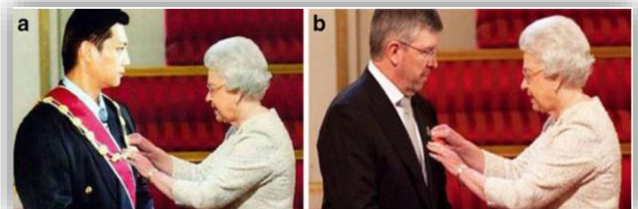
Abstract— The increasing rate of Cyber Crime has drawn spotlight toward Digital Forensics and cyber security. It is a branch of forensic science which trades with cybercrime. It necessarily includes the detection, recovery and investigation of material found in digital hardware. Digital images and recordings take most key part in digital crime scene investigation. They are the prime assertions of any cyber-crime scene. So, the responsibility of the image is basic. Digital Photography is having a rapid and steadily evolving scattering as of late, since it certifies anyone to take an instinctive number of good quality images, rapidly and at no cost, and to store them effortlessly on a symbolic number of digital assistance, or share them on the Internet. At the same time, with the broad availability of advanced tools for editing image like (e.g. Adobe Photoshop, Gimp), rework a digital photo, with little or no evident signs of tampering have become also very easy and boundless. A digitally corrected image can be uncertain from a bona fide image. The altering, be that as it may, may hinder some fundamental precise properties of the image. Under this presumption there are many distinct techniques are proposed that quantify and reveal statistical perturbations found in distinctive forms of tampered images.

Keywords— *Digital image forensics. Multimedia security. Image tempering detection. Image source authentication.*

Introduction

Images and videos have become the major instruction carriers in the digital era. The thoughtful potential of visual tools and the ease in their acquisition, transportation and storage is such that they are more and more exploited to transmit information, even sensible. As a effect, today images and videos represent a popular source of evidence, both in everyday life controversies and in trials. The simplest video in TV news is commonly taken as a certification of the truthfulness of the arrived news. In a similar way, video surveillance recordings can create fundamental probationary component in a court of law. Together with indisputable benefits, the accessibility of digital visual media brings a major fault. Image processing professionals can easily access and adjust image content, and therefore its meaning, without leaving visually evident traces. Moreover, with the spread of low-cost, user friendly editing tools, the art of fooling and counterfeiting visual content is no more confined to experts. As a consequence, the alteration of images for malicious purposes is now more universal than ever. Digital Image Forensics is that branch of multimedia security that, together with Digital Watermarking, desire at contrasting and exposing malicious image manipulation. In July 2010 Malaysian politician Jeffrey Wong Su En challenged to have

been knighted by the Queen Elizabeth II, as appreciation for his contribution to the universal aid organization Médecins Sans Frontières. A picture of him being awarded by the Queen of England followed his statement, diffused in local media. When questioned about the award still, the British High Commission in Kuala Lumpur made straightforward that the name of Mr. Wong was not added in the authoritative knighthood recipients lists, and that the photograph was incompatible with the usual protocol adopted for knighthood ceremonies. The image was eventually shown to be a splicing between an original ceremony photo and Mr. Wong's face, built to strengthen his popularity. This kind of episodes assisted in making more and more ambiguous the use of digital images as evidence.



A confirmation of their correctness is needed, before further relying on their content. For this logic, two questions about the past of the image have to be answered: a) Was the image trapped by the device it is claimed to be acquired with? b) Is the image still representing its original content? The first question is of major significance when the source of the image is the evidence itself, i.e. when the ownership of the capturing camera is negotiating, or when an accusatory content is such only if it was recorded by a precise device (e.g. video surveillance). The second question is of more general significance, and can be directly applied to the fraudulent knighthood picture case. Answering to those questions is relatively simple when the original image is known. In the case of the spurious knighthood, the simple availability of the original image was acceptable to expose the forgery. In practical events, though, almost no information can be considered to be known a priori about the original image. Investigators need therefore to verify the image history in a blind way. Digital image forensics (DIF) aims at contributing tools to support blind investigation. This brand-new practice stems from existing multimedia security-related investigation domains (e.g. Watermarking and Steganography) and exploits image processing and analysis tools to restore information about the history of an image.

LITERATURE SURVEY

The years from 1999-2007 were a sort of “Golden Age” for digital forensics. During this period digital forensics became a sort of magic window that could see into the yesteryear and into the criminal head. Network and image forensics made it possible to hold up time and monitor crimes as they were being engaged even many months after the fact. Forensics became so comprehensive and reliable that it evaded from the lab and onto the TV screen, organizing the so-called “CSI Effect.” This Golden Age was described by: The comprehensive use of Microsoft Windows, and specially Windows XP.

- Relatively scanty file formats of forensic involve mostly Microsoft Office for evidences, JPEG for digital snapshots; and AVI and WMV for video.
- Examinations largely restrained to a single computer organization belonging to the case of the investigation.
- Storage devices provided with standard interfaces, fixed using removable cables and connectors, and assured with portable screws.
- Multiple merchants selling tools that were reasonably satisfying at recovering allotted and deleted files. The broad failure of the market to accept encryption technology for data-at-rest built it relatively secure to develop and advertise forensic tools that were actually profitable to a wide range of customers. These means allowed someone with almost limited training to hunt for email messages, restore deleted files and function basic file carving.

Today much of the previous decade’s development is quickly becoming inappropriate. Digital Forensics is facing a problem. Hard-won powers are in jeopardy of being diminished or even dropped as the consequence of advances and crucial changes in the computer industry:

- The growing capacity of storage devices means that there is frequently insufficient chance to create a forensic image of a subject device, of technique of the data once it is found.
- The strengthening prevalence of embedded flash storage and the proliferation of hardware contact means that storage devices can no longer be readily get rid of or imaged.
- The proliferation of operating systems and file patterns is dramatically strengthening the requirements and intricacy of data exploitation tools and the cost of tool advancement.
- Whereas cases were formerly limited to the analysis of a single device, progressively cases require the analysis of numerous devices followed by the correlation of the found evidence.
- Pervasive encryption means that even when data can be retrieved, it frequently cannot be processed.
- Service of the “cloud” for remote processing and repository, and to split a single data edifice into elements, means that frequently data or code cannot even be found.

Among digital forensics specialists, the best approach for fixing the coverage problem is to buy one of every tool on the market. Clearly, this path only works for well-funded society. Even then, there are many scenes in which commercial tools fall and practitioners must depend on open source software. Although some of this software is very satisfying, other tools are poorly documented, out-of-date, and even dropped out. Sadly, even though many specialists rely on open source tools, there is no admitted or funded clearing house for open source forensics software.

S. Bayram, et al. offered a technique for the detection of doctoring in digital image. Doctoring mostly involves multiple processes, which typically involve a sequence of elementary image processing processes, such as scaling, rotation, contrast shift, smoothing, etc. The technique used is based on the three categories of statistical features consisting of binary similarity, image quality and wavelet statistics. The three categories of forensic elements are as follows:

1. Image Quality Measures: These focuses on the contrast between a doctored image and its original version. The original not being available, it is imitated via the blurred version of the test image.
2. Higher Order Wavelet Statistics: These are extracted from the multi scale disintegration of the image.
3. Binary Similarity Measure: These measures capture the correlation and balance properties between and within the low significance bit planes, which are more likely to be altered by manipulations. To deal with the detection of doctoring effects, firstly, single tools to detect the basic image-processing operations are progressed. Then, these individual “weak” detectors assembled together to detect the presence of Swaminathan et al. introduced a method to estimate both in-camera and post-camera operation fingerprints for verifying the virtue of photographs. This paper introduces a new technique for the forensic analysis of digital camera images. The elemental fingerprints of the various in-camera processing processes can be estimated through a detailed imaging model and its segment analysis. Any change or disagreements among the estimated camera-imposed fingerprints, or the existence of new types of fingerprints suggest that the image has withstood some kind of processing after the initial capture, such as tampering or stenographicaphic embedding. H. Cao et al. designed a new ensemble handling detector to simultaneously detect a wide range of manipulation types on local image patches. Fan et al. proposed to correlate analytical noise features with equivalent image file format header features for manipulation detection. M. C. Stamm and K. J. R. Liu, proposed different processes not only for the detection of global and local contrast enhancement but also for diagnosing the use of histogram equalization and for the detection of the global extension of noise to a previously JPEG-compressed image.

WHAT IS DIGITAL IMAGE AND WHAT IT IS COMPOSED OF?

A digital image is a pattern of pixels arranged in an organized way, showing a precise image. Pixels are the meagreness unit in the image. We accumulate images or shift them from one position to another inside the pc or transport them to another remembrance like flash memory as an array of bits (0, 1). Images are divided mainly into two types:

- pixel images
- vector images.

Acronym	Full Name
JPEG	Joint photograph experts group
BMP	Bitmap pictures
GIF	Graphics interchange format

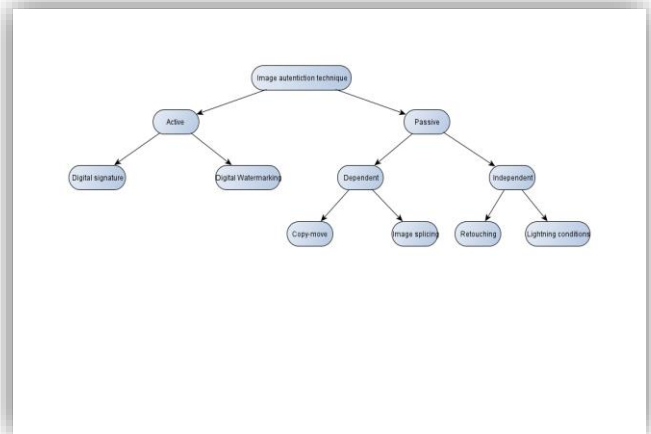
PNG	Portable network graphics
TIFF	Tagged image file format
PSD	Photoshop document
XCF	Experimental Computing facility
AI	Adobe illustrator artwork
CDR	Corel draw image

- A. Pixel images (bitmap images) — We handle with these every day (normal digital images). PNG, JPEG, TIFF, and GIF are different pixel images. Each category is defined by its own procedures and devices. They are pixel-based; capacity is linked to its particulars; they are best for editing and manipulating and are not scalable.
- B. Vector images — These photographs are used for cartoons, logos, descriptions, etc. and are controlled by special courses like Corel=draw with a mathematical calculation. When we do services like enlarging or stretching, the resolution of the photograph will stay constant. Types of vector images are AI, CDR, SVG, and EPS. An image is an array of picture elements, as mentioned above, but there are several image types:
- binary image
 - gray scale image
 - colored image
 - multispectral image.
- A. Binary image is an array of two dimensions of bits. It has dual colors, typically white and black — 0s represent white-colored pixels, and 1s represent black-colored pixels.
- B. Gray scale images are those images where each pixel is illustrated with two bits, representing the power of the white/black colors (00 represents white color, 11 represents black color) and the values between these two restrictions represent the power of the gray color.
- C. Colored images, or are known as RGB images, (red, green, blue), are the images that accommodate a variety of colors. This type of image is portrayed inside the memory by a eight bit for each pixel. Each pixel contains an amount of red, green, blue power, and is stored as bits:
Red green blue 00 00 00.
- D. Multispectral images are impressions consisting of multilayers of colors, with every layer viewing specific colors.

CLASSIFICATION OF IMAGE AUTHENTICATION TECHNIQUES:

Forgery detection resolves to establish the authenticity of images. For attestation of images different methods have been advanced. We broadly segregate these techniques into two classes:

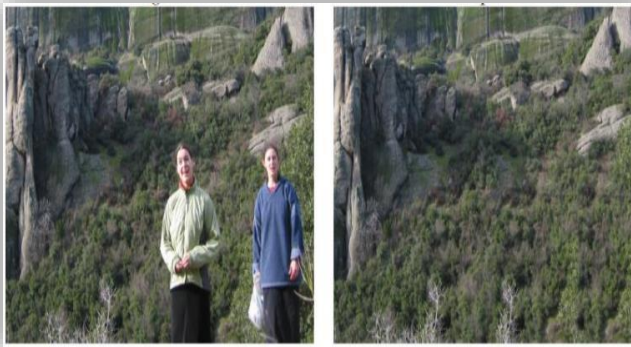
- Active authentication and
- Passive authentication.



The distribution is based on the information whether the initial image is available or not. Under individual class the techniques are further sub divided.

1. Active Authentication:
In active authentication systems preceding information about the image is crucial to the means of authentication. It is bothered with data hiding where a few codes are installed into the image at the time of origin. Authenticating this code authenticates the individuality of image. Active authentication practices are further segregated into two types: digital watermarking and digital signatures.
 - a. Digital water marks are inserted into the photographs at the point of image addition or in processing phase and digital identifications insert some insignificant information, usually derived from image, at the acquisition end into the image. The main disadvantage of these appeals remains that they are to be infused into the images at the time of documentation using special equipment thus past information about image becomes indispensable.
2. Passive Authentication:
Passive authentication also called image forensics is the technique of attesting images with no specification of prior instruction just the image itself. Passive techniques are depended on the presumption that even though tampering may not leave any optical trace, but they are likely to transform the underlying stats. It is these disagreements that are used to expose the tampering. Passive techniques are further organized as forgery dependent methods and forgery independent methods. Forgery dependent detection methods are invented to reveal only definite type of forgeries such as copy-move and splicing which are dependent on the category of forgery carried out on the image while as forgery independent methods detect forgeries independent of forgery type but based on artifact fragments left during technique of re-sampling & due to lighting inconsistencies .
 - a. Copy-move Forgery Detection:

Copy-move is the most trendy and common photo tampering art because of the simplicity with which it can be carried out. It engages copying of some region in an image and converting the same to some other region in the image. Since the photocopied region reside to the same image therefore the effective range and color remains consistent with the rest of the image.



Original

Tampered

a. Image Splicing:

Image splicing forgery system associates formation or merging of two or more figures changing the authentic image significantly to develop a forged image. In case images with varying background are incorporate then it becomes very tough to make the borders and boundaries indistinct.



b. Image Retouching:

Image retouching is one more category of image forgery tool which is most frequently used for monetary and aesthetic applications. Retouching operation is driven out mostly to upgrade or lower the image features. Retouching is also done to set up a convincing union of two images which may involve rotation, resizing or stretching of one of the photographs.

c. Lighting Condition:

Images that are mixed during tampering are captured in distinct lighting conditions. It becomes problematic to match the lighting condition from

linking images. This lighting inconsistency in the compound image can be used for revelation of image tampering. By considering angle of light source for distinctive objects and community in an image, differences in lighting are brought to light in the image and tampering can be disclosed.

METHODS AND TOOLS IN DETECTION PROCESS

1. Principal Component Analysis (PCA):

Initially Principal Component Analysis (PCA) is applied on small fixed-size blocks to yield a reduced dimension representation. In a grayscale image consisting of P^2 number of pixels, PCA is applied on small blocks of B^2 pixels ($B \times B$ dimension) which are assumed to be very small than actual dimension of forged object of the image. PCA provides robustness and good sensitivity in detecting additive noise and lossy JPEG compression, minor intensity variation, but it doesn't work for small angular transformations.

2. DWT-DCT:

In this method, out of total P^2 pixels, DWT and DCT features of blocks of B^2 non overlapping pixels are calculated and lexicographically sorted to detect forged area. In the first step, DCT of all the B^2 pixels are calculated and coefficients of cosine transform are stored in a matrix. Then in the second step, DWT is calculated to a single level of decomposition and then deriving Eigen vectors for completing the feature matrix. Then this matrix is lexicographically sorted and by determining the closeness of two vectors, forged area is detected. Because of use of non-overlapping block, complexity of sorting was at $P \cdot \log(P)$. DWT-DCT method is robust to JPEG compression and additive noises.

3. Discrete Cosine Transform (DCT):

Owing to the nature of copy-move forgery, there must be at least a pair of similar regions in a tampered image, which is the basis of all passive detection algorithms. A natural image, on the contrary, is unlikely to have two large similar regions except for the images that have a large area of smooth region, such as blue sky or green grassland in the image. Hence, the task of passive-blind forensics is to determine whether an image contains large similar regions. Since the shape and size of copied regions are unknown, it is definitely computationally impossible to try to compare every possible pairs of regions pixel by pixel. Obviously, it is more effective to divide a forensic image into fixed-sized overlapping blocks and examine whether pairs of blocks are duplicated. The key step is to extract some appropriate and robust features from each block in order to implement an effective detection. Therefore, a good feature can not only represent the whole block, but also has the robustness of common post-processing operations, and what is more, make the detection algorithm have lower computational complexity.

4. Discrete Fourier Transform (DFT):
In this method, 1-D FT of rows of non-overlapping block is calculated and feature vectors are formed by averaging the values of transformed respective columns. DFT method is resistant against Gaussian Blurring or JPEG compression. Overlapping blocks are used to determine 1D and 2D Fourier transform of the block.
5. Singular Value Decomposition (SVD):
In this method small block of dimension $B \times B$ is taken (overlapping blocks are taken over the complete gray scale image giving $(P-B+1)^2$ pixels) and then apply SVD on this block. Output of SVD gives us the feature vector and then forged object could be detected by checking similarity of feature vectors by lexicographically sorting them. SVD is resistant to geometric changes, algebraic changes, scaling rotation, additive noise, Gaussian blurring, lossy JPEG compression.
6. DCT and SVD:
In this tool, overlapping blocks of $B \times B$ dimensions are taken from the input image and then 2D-DWT is applied on these blocks to get coefficient and then SVD is applied on the coefficient matrix to give the final feature vector. Feature vector is sorted lexicographically to detect forged object in the image. This method is Robust against Gaussian blurring, AWGN, JPEG compression and their mixed operation.

FORGERIES INVOLVING IN SINGLE IMAGE

Eliminating undesired objects from an image is one of the most unambiguous methods to alter its meaning. In such circumstances, counterfeiters need to “fill” the neighbourhood of the image from which the object has been detached. A symbolic solution in this case is to copy a fragment of the same image and replace with it the void left from the removal (copy-move technique). To more hide this enterprise to the human eye, the counterfeiter can perform geometrical transforms on the region to be photocopied, such as orbit or scaling. Moreover, to produce an effortless development between the (original) surround and the commodity to be pasted, place mat and blending capacities can be handled. Object removal can be also managed by means of in-painting capabilities. Inspired by real techniques for painting reclamation, in-painting methods fill the pockets left by commodity removal by handling the information secured in the regions enveloping the gaps. In particular, in-painting is depended on an iterative proceeding of smooth instruction propagation from the illustration to the region to be supplied. The gap is gradually filled from the periphery to the centre, resulting in a perceived continuity in the final image. However, the algorithm contends with filling decidedly textured operations. Recently, the joint carving method was shown to be an impressive tool for object eradication. Initially requested for content-aware illustration resizing, the algorithm is based on the impression of seam. A seam is defined to be a monotonic and connected path of pixels including one pixel

per row (column) and traversing the image from the top to the bottom (left to the right). Seams are iterative eliminated based on a minimum efficiency criterion; each seam cancellation corresponds to a horizontal (vertical) resizing of one pixel, dominant to a final result perceptually more rational than what could be obtained by straightforward re-sampling of the thought. When targeting the algorithm on a precise region or object, the same technique becomes a very definitive tool for object removal, which is concluded by iterative wiping out all the seams spanning the selected region. Forgeries can be executed on a specific image also without persisting to object removal. Image semantics can be repaired by applying simple image processing techniques, such as histogram handling or contrast improvement. Also, brightness adjustment and scaling can be of applicable application to better shield copy-move impositions: more in generic, the function of filters or simple geometrical transforms can negotiate the forensics judgment, by protecting or deleting traces of further tampering, as shown in for scientific picture.

FORGERIES INVOLVING MULTIPLE IMAGES

Forgeries using various images as source for intruding. The inclusion in an image of material originally materializing from another source is one of the most powerful tools to invalidate the message contained in visual media. Blending and matting facilities are again relevant to mask the borderline of the grafted districts and to give the illustration a more uniform prospect. Also, the creation of image composites might involve geometric conversion. Rotation, scaling and adaptation are often desired to make sure that the grafted object respects the original image prospect and scale. Geometric transforms regularly involve re-sampling, which in turn calls for interpolation (e.g. the nearest neighbour, bilinear, bi cubic). The re-sampling process manufactures artifacts in the image histogram, and hence provides a profitable cue for compositing disclosure. It should be also taken into explanation that inserted element does not unquestionably have to come from innate images. As computer graphics evolves, more and more realistic 3D objects can be designed and delivered to be eventually grafted into an image composite. Furthermore, the eradication of 3D scene structure from images recognizes manipulating objects by transforming them: in this case, the splicing involves reconstruct (i.e. artificial) version of a part of the original photograph. This facility is applied when the counterfeiter aims e.g. to modify a facial explanation as experimented in video rewriting.

CONCLUSION

In this survey, image forensic tools have been reviewed, by classifying them according to the position in the history of the digital image in which the relative footprint. It has been highlighted how image acquisition footprints arise from the

overall combination of individual traces by each single stage in the acquisition process cascade. The technique has been claimed for the virtual reclamation of figures and was found very impressive by reconstruction experts. There are certain prospects of the designed technique that can be further reformed. For example, the crack-detection phase is not very profitable in recognizing cracks located on very dark image areas, since in these areas the vigour of crack components is very close to the power of the enveloping region. Many image processing functions, tools and capabilities helps to derive complex features of an image. Image processing works on single structural image to multidimensional and see what actually in the figure. Image processing is the real core for many perfecting technologies in the real time prospect. This paper examines the examination of an image processing demands, tools and capacities. Despite its success so far, many difficult problems remain open at this stage.. We hope this paper deals with the aspects of image forensics in all ways.

REFERENCES

1. <http://downloads.hindawi.com/archive/2013/496701.pdf>
2. <http://dx.doi.org/10.1080/18756891.2016.1161364>
3. Mushtaq, Saba & Mir, Ajaz. (2014). Digital Image Forgeries and Passive Image Authentication Techniques: A Survey. International Journal of Advanced Science and Technology. 73. 15-32. 10.14257/ijast.2014.73.02.
4. J. Fridrich, "Digital image forensics," in IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 26-37, March 2009.
5. <https://link.springer.com/article/10.1007/s11042-010-0620-1>
6. 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC) Dec 20-22, 2013, Shenyang, China
7. R. S. Khalaf and A. Varol, "Digital Forensics: Focusing on Image Forensics," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-5.
8. V. Murino and A. Trucco, "Three-dimensional image generation and processing in underwater acoustic vision," in Proceedings of the IEEE, vol. 88, no. 12, pp. 1903-1948, Dec. 2000.
9. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1027.7772&rep=rep1&type=pdf>
10. I. Pitas and A. N. Venetsanopoulos, "Order statistics in digital image processing," in Proceedings of the IEEE, vol. 80, no. 12, pp. 1893-1921, Dec. 1992.
11. I. Giakoumis, N. Nikolaidis and I. Pitas, "Digital image processing techniques for the detection and removal of cracks in digitized paintings," in IEEE Transactions on Image Processing, vol. 15, no. 1, pp. 178-188, Jan. 2006.
12. <https://ijict.com/V2I2/V2I2P03.pdf>
13. F. Cheng and A. N. Venetsanopoulos, "An adaptive morphological filter for image processing," in IEEE Transactions on Image Processing, vol. 1, no. 4, pp. 533-539, Oct. 1992.
14. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.217.9580&rep=rep1&type=pdf>

PLAGIARISM REPORT:

- ABSTRACT AND INTRODUCTION

100%

Completed: 100% Checked

0%

Plagiarism

100%

UNIQUE

Sentence Wise Result

Matched Sources

Document View

UNIQUE	The increasing rate of Cyber Crime has drawn spotlight toward Digital Forensics and cyber security.
UNIQUE	It is a branch of forensic science which trades with cybercrime.
UNIQUE	It necessarily includes the detection, recovery and investigation of material found in digital hardware.
UNIQUE	Digital images and recordings take most key part in digital crime scene investigation.
UNIQUE	They are the prime assertions of any cyber-crime scene.
UNIQUE	Digital Photography is having a rapid and steadily evolving scattering as of late, since it certifies anyo...
UNIQUE	no cost, and to store them effortlessly on a symbolic number of digital assistance, or share them on t...
UNIQUE	At the same time, with the broad availability of advanced tools for editing image like (e.g.
UNIQUE	Adobe Photoshop, Gimp), rework a digital photo, with little or no evident signs of tampering have bec...
UNIQUE	A digitally corrected image can be uncertain from a bona fide image.
UNIQUE	The altering, be that as it may, may hinder some fundamental precise properties of the image.
UNIQUE	Under this presumption there are many distinct techniques are proposed that quantify and reveal stat...
UNIQUE	Images and videos have become the major instruction carriers in the digital era.
UNIQUE	The thoughtful potential of visual tools and the ease in their acquisition, transportation and storage is...

- LITERATURE SURVEY:

RESULTS

100%


Completed: 100% Checked


0%


Plagiarism

100%

UNIQUE

 Sentence Wise Result

 Matched Sources

 Document View

UNIQUE	The years from 1999-2007 were a sort of "Golden Age" for digital forensics.
UNIQUE	During this period digital forensics became a sort of magic window that could see into the yesteryear...
UNIQUE	Network and image forensics made it possible to hold up time and monitor crimes as they were being...
UNIQUE	Forensics became so comprehensive and reliable that it evaded from the lab and onto the TV screen, ...
UNIQUE	comprehensive use of Microsoft Windows, and specially Windows XP.
UNIQUE	• Relatively scanty file formats of forensic involve mostly Microsoft Office for evidences, JPEG for digi...
UNIQUE	• Examinations largely restrained to a single computer organization belonging to the case of the inve...
UNIQUE	• Storage devices provided with standard interfaces, fixed using removable cables and connectors, a...
UNIQUE	• Multiple merchants selling tools that were reasonably satisfying at recovering allotted and deleted f...
UNIQUE	The broad failure of the market to accept encryption technology for dataat-rest built it relatively secur...
UNIQUE	These means allowed someone with almost limited training to hunt for email messages, restore delet...
UNIQUE	Today much of the previous decade's development is quickly becoming inappropriate.
UNIQUE	Hard-won powers are in jeopardy of being diminished or even dropped as the consequence of advan...

- WHAT IS DIGITAL IMAGE AND WHAT IT IS COMPOSED OF?

100%

Completed: 100% Checked

2%

Plagiarism

98%

UNIQUE



Sentence Wise Result



Matched Sources



Document View

UNIQUE	WHAT IS DIGITAL IMAGE AND WHAT IT IS COMPOSED OF?
UNIQUE	A digital image is a pattern of pixels arranged in an organized way, showing a precise image.
UNIQUE	We accumulate images or shift them from one position to another inside the pc or transport them to ...
UNIQUE	A. Pixel images (bitmap images) — We handle with these every day (normal digital images).
UNIQUE	PNG, JPEG, TIFF, and GIF are different pixel images.
UNIQUE	Each category is defined by its own procedures and devices.
UNIQUE	They are pixel-based; capacity is linked to its particulars; they are best for editing and manipulating a...
UNIQUE	B. Vector images — These photographs are used for cartoons, logos, descriptions, etc.
UNIQUE	and are controlled by special courses like Corel=draw with a mathematical calculation.
UNIQUE	When we do services like enlarging or stretching, the resolution of the photograph will stay constant.
UNIQUE	Types of vector images are AI, CDR, SVG, and EPS.
UNIQUE	An image is an array of picture elements, as mentioned above, but there are several image types:
UNIQUE	A. Binary image is an array of two dimensions of bits.
UNIQUE	It has dual colors, typically white and black — 0s represent white-colored pixels, and 1s represent bla...

- METHODS AND TOOLS IN DETECTION PROCESS:

100%


Completed: 100% Checked

0%


Plagiarism

100%


UNIQUE



Sentence Wise Result



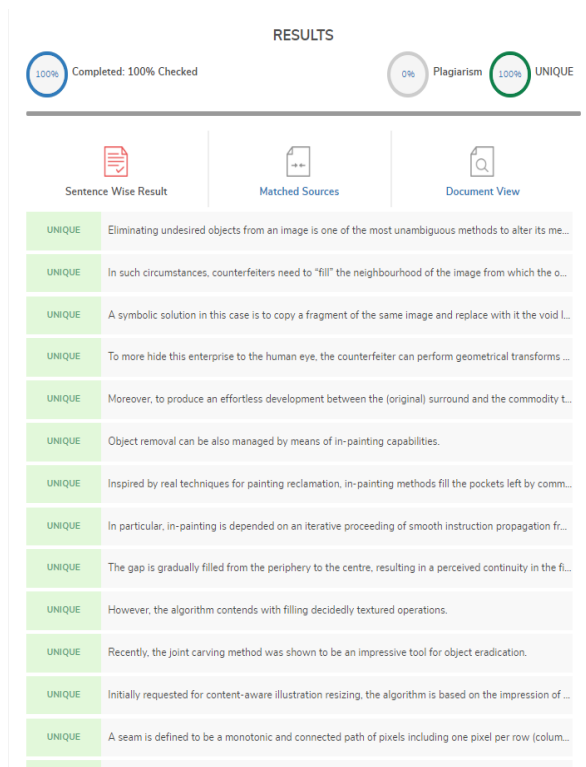
Matched Sources



Document View

UNIQUE	Initially Principal Component Analysis (PCA) is applied on small fixed-size blocks to yield a reduced di...
UNIQUE	In a grayscale image consisting of $P \times 2$ number of pixels, PCA is applied on small blocks of $B \times 2$ pixels...
UNIQUE	PCA provides robustness and good sensitivity in detecting additive noise and lossy JPEG compressio...
UNIQUE	In this method, out of total $P \times 2$ pixels, DWT and DCT features of blocks of $B \times 2$ non overlapping pixel...
UNIQUE	In the first step, DCT of all the $B \times 2$ pixels are calculated and coefficients of cosine transform are store...
UNIQUE	Then in the second step, DWT is calculated to a single level of decomposition and then deriving Eige...
UNIQUE	Then this matrix is lexicographically sorted and by determining the closeness of two vectors, forged a...
UNIQUE	Because of use of non-overlapping block, complexity of sorting was at $P^2 \log(P)$.
UNIQUE	DWT-DCT method is robust to JPEG compression and additive noises.
UNIQUE	Owing to the nature of copy-move forgery, there must be at least a pair of similar regions in a tamper...
UNIQUE	A natural image, on the contrary, is unlikely to have two large similar regions except for the images th...
UNIQUE	Hence, the task of passive-blind forensics is to determine whether an image contains large similar re...
UNIQUE	Since the shape and size of copied regions are unknown, it is definitely computationally impossible to...

- FORGERIES INVOLVING IN SINGLE IMAGE & MULTIPLE IMAGES:



- CONCLUSION & REFERENCES:

