MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Forensic Document Examination Using Image Processing Tools

Chourasiya S[1]*, Patel V[1] and Pandey R[2]

[1]Department of Forensic Science Medicaps University, Indore, Madhya Pradesh, India
[2]Guru Ghasidas University, India

***Corresponding author:** Shivam Chourasiya, Department of Forensic Science Medicap's University, Madhya Pradesh, India, Email: shivam.chourasiya@medicaps.ac.in

Research Article
Volume 8 Issue 1
Received Date: January 02, 2023
Published Date: March 09, 2023
DOI: 10.23880/ijfsc-16000292

Abstract

Paper documents have always been our primary means of transmitting and storing information. However, for better storage and processing, the majority of records are currently only available in electronic format. As a result of digitization, the field of forensic document analysis has improved and evolved to keep up with the times, as it has become relatively easy for anyone to change any type of document using various image modification tools. The current study focuses to examine documents that have been manipulated by computers using open-source image processing tools. Forensically beta, FotoForensics, and Adobe Photoshop tools were used to analyze the sample documents that had been altered. The results suggest that these image processing tools can be used to analyze digitally modified documents to detect manipulations and thus can help Forensic document examiners. The present work reveals that some minute characteristics are present in the transplanted documents which can be identified by careful analysis of soft copies of documents with tools present in Forensically beta, FotoForensics, and Adobe Photoshop.

Keywords: Document Examination; Image Processing; Manipulation

Introduction

Handwriting analysis with the purpose of identifying the writer has a lengthy history, maybe reaching back to the beginnings of handwriting itself. Questioned, or Forensic Document Examiners, investigate crimes involving documents, ranging from fraud and anonymous letters to armed robbery and murder [1]. Something that contains information is referred to as a document [2]. An alteration, forging, or creation of any sort of document with the goal to defraud is called forgery. It is the act of adapting, imitating, or creating products, documents, or data with the goal of deceiving others and earning money by selling fabricated items [3]. Whereas it is a crime when it affects a person's rights, whether they are public or private, and it is done in violation of the law. Forgery necessitates deception (4 Nowadays, it's common practise to modify writing and signatures using scanners and computer software. Numerous authentic documents may well be altered using a variety of tactics, including addition, sheet substitution, cut-and-paste manipulation, and photocopies, faxes, and computer-generated documents [4,5]. The essence of a written document has evolved dramatically because of digitization. as well as the nature and perpetration of white-collar crime [6]. These technologies are so readily available to criminals; thus, they are frequently used to create forged photocopies or hard copies created by computers. Similar documents frequently presented in law seem like the only piece of legal evidence available, with the said argument that the authentic records were missing, cleaned, burnt, or otherwise destroyed. Forgery using the aforementioned methods complicates document issues, enabling scientific

detection much more difficult and complex. In today's world, questioned document experts are frequently requested to do signatures as well as other examinations on documents that are not original due to the proliferation of copies [7].

However, technological advancements have made it simple to alter a printed document for nefarious purposes. As a result, document authenticity is critical in forensic science when papers are legally challenged, due to which 'questioned document examination' (QDE) has emerged as an important discipline in the field of forensic science which covers the scientific procedures capable of providing evidence concerning a suspected or doubtful document. Document forensics technology has advanced quickly in recent years, with the majority of applications focusing on tracking the source of a document or detecting forgery. The necessary analyses are performed using common scanners and a computer with this technology [8]. In the field of handwriting analysis and various elements of image forgery, significant work has been done using various Digital Image Processing software and tools, including MATLAB. These strategies have been successful in identifying individuality and extracting traits [9]. The purpose of this research is to investigate how image-processing techniques can be used to examine documents that have been modified by computers. The main aim of the study is to investigate and classify many types of modifications discovered in written documents.

Methods

To study the image processing technique in forensic document examination, the samples collected from google Images. As the original documents cannot be taken due to their authorization and confidentially maintained by the government, with due reason, ten manipulated samples were prepared by copying and transplanting a portion of the document into the other which makes altering the document in such a way that it appears original. The changes made in name, date, place, and number as the sample includes stamp paper, mark sheets, and certificates. Text from these documents added and deleted as part of the alteration. Then these documents scanned in soft copy format by using various software and tools available offline and online. The software and tools used in the present study:

Microsoft paint - It is basic graphics editor which is present with all versions of Microsoft Windows and used for editing the images. With this program, name, date, and place text edited, copied, and pasted into the documents to be forged [10].

Forensically beta – Forensically beta is a set of free tools which is used for the analysis of documents or images. Tools such as error level analysis, level sweep, and noise analysis are included for analysis [11]. FotoForensics- FotoForensics is a website with free tools such as color adjustment, file digest, error level analysis, hidden pixels, estimate JPEG quality, lens effects, metadata analysis, and strings [12]. Adobe Photoshop 7 - Adobe Photoshop is the software that is used for the editing and retouching of images. In other words, this software is used for the magnification of documents or images through which we can observe the minute changes such as color and font size differences present in the documents. It allows users to create and edit raster images in multiple layers [13].

The background details of the document are recorded and examined back and forth precisely under a good source of light.

Results

All 10 forged samples were examined using online tools available in Forensically beta, FotoForensics website and adobe photoshop software. The following observations recorded:

- All samples examined in error level analysis and level sweep tool in Forensically beta and FotoForensics website. The segment of the document which was transplanted is highlighted more than other parts of the document indicating the changes made in the document (Figures 1-8).
- SHA1 hash value of all the original documents and forged documents was calculated using the digest tool available on the FotoForensics website and compared in (Table 2). The hash value of all original documents differs from the forged documents.
- All forged documents were analysed in 250% and 1200% magnification using Adobe Photoshop software. The minute differences like pixelate, font size, and color differences are clearly observed in (Figures 7 & 8).
- Comparison of the software Forensically beta, FotoForensics, and Adobe Photoshop is shown in Table 4.

Figure 1: Enlarged view of sample 1 showing the colour, font size and pixelate differences at 800% magnification.

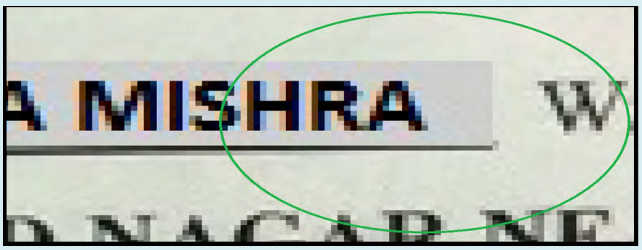


Figure 2: Enlarge view of sample2 showing colour, font size and pixelate differences at 800% magnification.

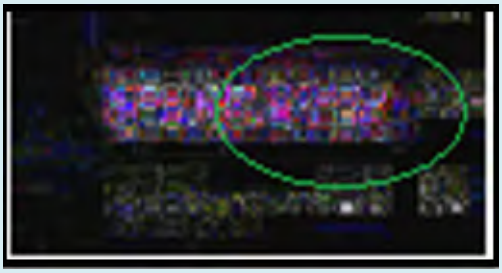


Figure 4: Error level analysis of S1 in Forensically beta.

Figure 3: S1 Forged Sample.

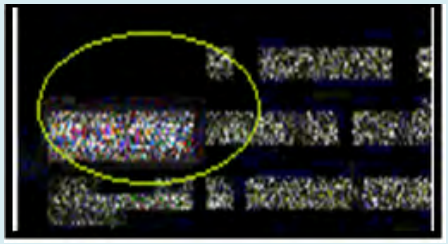
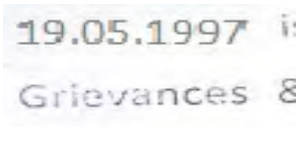
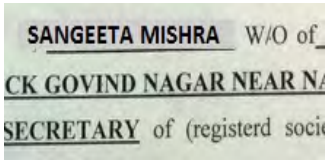
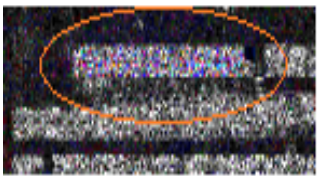
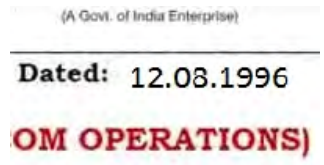
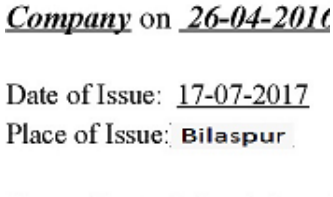


Figure 5: Error level analysis of S1 in FotoForensics.

Sample	Forged sample	Error level analysis	Sha1 hash value	
			Original document	Forged document
S1			8aa18519ce2ecc9f406a93964bed58577d72a615	ebade69f22835d43427022f13f69c447313f2ae8
S2			50cb3fa165e9b856716b846d7259efd042e23693	8175df484d9a27a20f3a3986ff22423d8132cdb7
S3			a3dda9c5723624705c712e5c3f0840bbc39b1a6e	55263f8152d460368d07d86cc903011709d340b3
S4			155ef504df7fbf2077432fc96bded6d86dc9b341	7835f5ffde938c02072c6d54e78aac64286e28f6

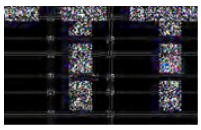
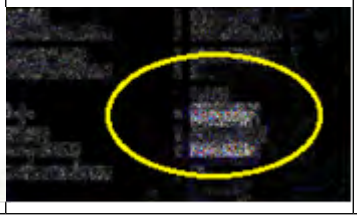
S5	Department of Industrial Policy ATE LIMITED incorporated/ regis of Health and environment		0ae327a76196be8d692 643b498af78ef455b00ee	58c3d8a682 10f3460ecbe 788b6af0ccc21ef3573
S6	(Zero) : UMESHWAR KURREY : Not Applicable : UMESHWAR KURREY : 10 (Ten only)		f4681e6034412e1f646 02f4c5ce4ccd3524782a6	cdeffeef0509a b55ec1a8a93 1a50816d42dda535
S7	A1 10 A1 10 A2 08 A1 10 A1 10		1eb75d885bad2eea076 2d244e3ebb45caa69d6ba	2a9fe9fbf761 925546866 cb47b5de8ea39b4ebe2
S8	ximum: 35 ye)2.09.1990 an		4717543893812b2e1c 29a1f4b1b4 d263993bbcf7	2c1150fb2958121bc327a f5cf05ce08c7339b814
S9	Dated Guwahati 14th Mar nt Dates Last Date & Time rts from 19.03.2017 02:00 PM pplication 31/03/2018, 04:30 PM 3/4/2018. Till bank		569bfca983937cfe516 b1ae5fae4 2f9b84d4a9ce	43002dfd5 fb79320daebfa f4fb760dc15d3d629e
S10	(Rs.) : 0 (Zero) : NEHA SAHU : Not Applicable y : NEHA SAHU t(Rs.) : 10		1a43fb2eaf35838b4d 528dc 569ea7c0e3905f3ea	74651f9a e1cf0ca37d8b 7351a739ecfd4a2da9fe

Table 2: Analysis of sample using error level analysis and comparing hash value of original and forged document using FotoForensics.

Figure 6: Level sweep S1 in Forensically beta.

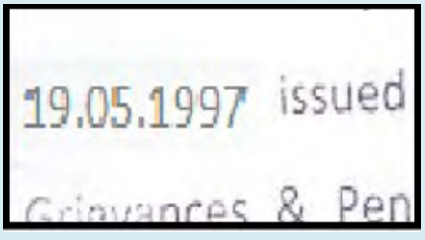


Figure 7: Magnification of S1 in 250% in Adobe Photoshop.

Figure 8: Magnification of S1 in 1200%.

Tools	Forensically beta	Foto forensics	Adobe photoshop
Magnification	Good	Not available	Best
Error level analysis	Best	Good	Not available
Level sweep	Not available	Good	Not available
Hash value	Not available	Present	Not available

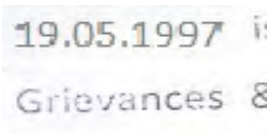
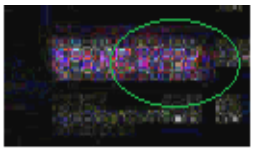
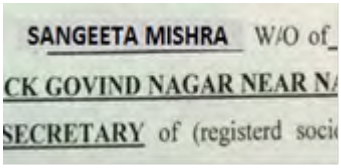
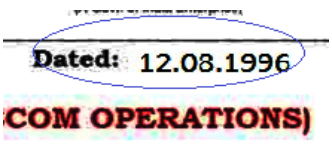
Table 4: Comparison of tools used in forensically beta, FotoForensics, and Adobe Photoshop.

Discussion

According to the study, free software also yields superior outcomes when used to examine documents that have been altered by computers, and programs like FotoForensics offer tools for computing the document's hash value. Examination reveals that there are differences in the letters' Color Level, Pixelate, and Font Size (Figures 1-8). The Software is simple to use and doesn't take much time, money, or effort to analyze or find the changes in the altered text. Table 4 compares the software, although there is no one best program because each software has its own qualities, thus this makes the analysis easier for the examiner and saves the effort, cost, and time of the Forensic Examiner.

Conclusion

In the modern world of cybercrime, computers often are commonly utilised to perpetrate specific crimes, including manipulating the meaning of documents. The present work reveals that some minute characteristics are present in the transplanted documents which can be identified by carefully analyzing a soft copy of the document with tools present in forensically beta, FotoForensics, and Adobe Photoshop. The authenticity of the document can also be checked using these tools. The minute pixelates, font size and color differences were present in the document that were clear when analyzed in large magnification. The range of magnification was between 250% to 1200%. The changes in the transplanted segment of the document were highlighted more when analyzed in error level analysis and level sweep tool available in Forensically beta and FotoForensics website (Tables 1-3). SHA1 Hash values of all original and forged documents were calculated to determine the difference between original and simulated documents to verify the integrity of the document and to support the findings of the Software used in the analysis. the results of this study suggest that image processing tools may be used to analyse digitally modified documents to detect manipulations, and which can help document examiners.

Sample	Forged Sample	Error Level Analysis	Level Sweep
S1			
S2			
S3			

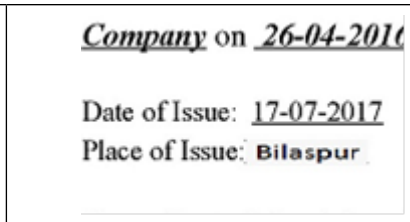
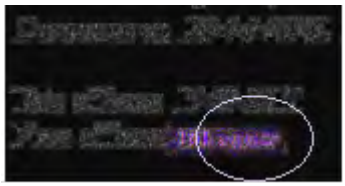
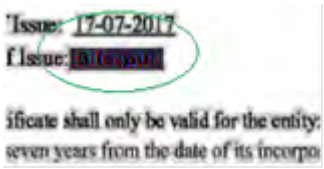
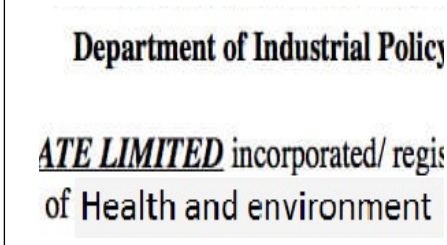
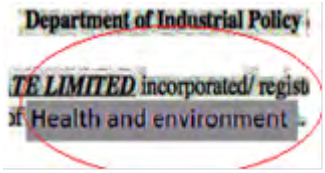
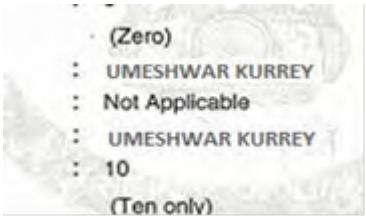
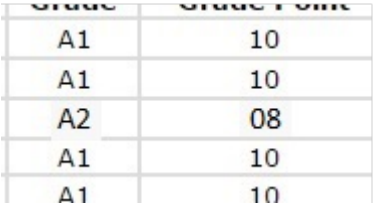
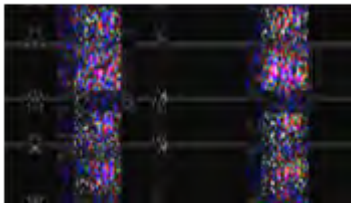
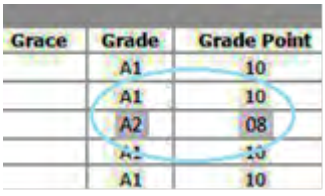
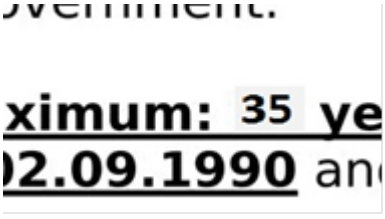
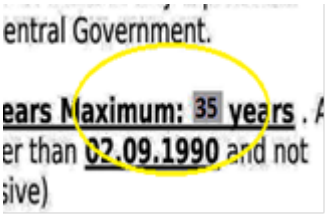
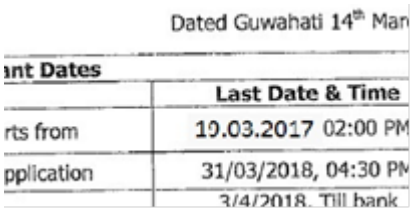
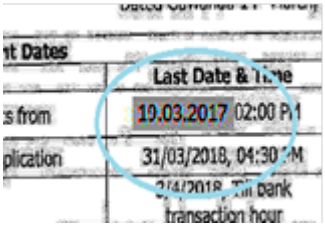
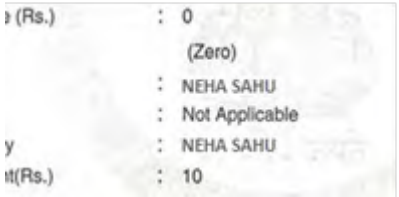
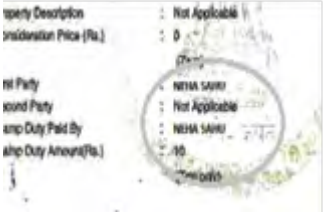
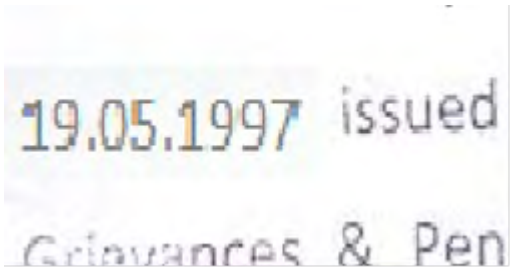
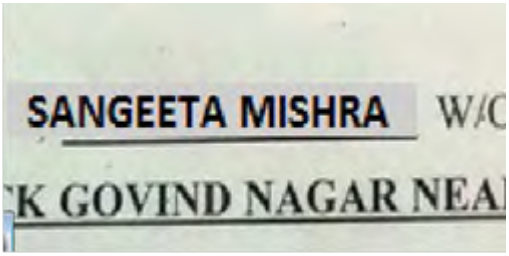
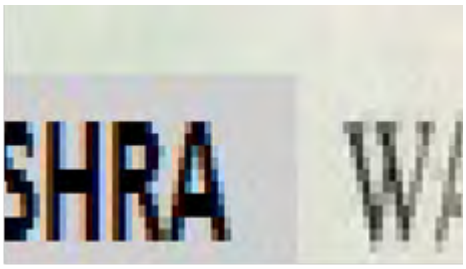
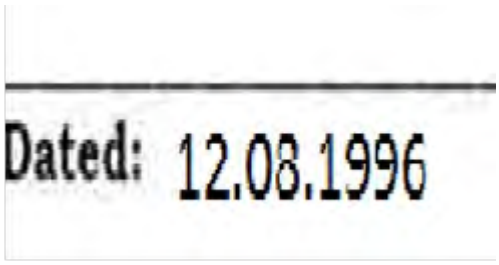
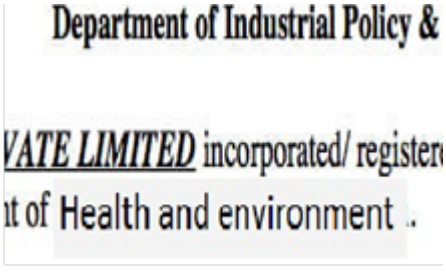
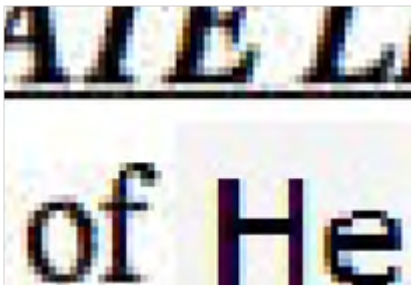
S4			
S5			
S6			
S7			
S8			
S9			
S10			

Table1: Analysis of sample using error level analysis and level sweep tool using Forensically Beta.

Sample	Magnification (250%)	Magnification (1200%)
S1		
S2		
S3		
S4		
S5		

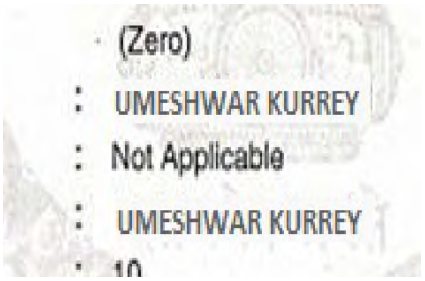
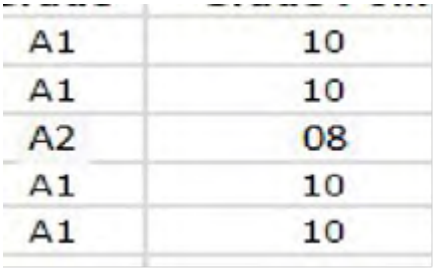
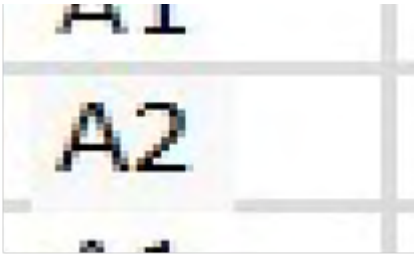
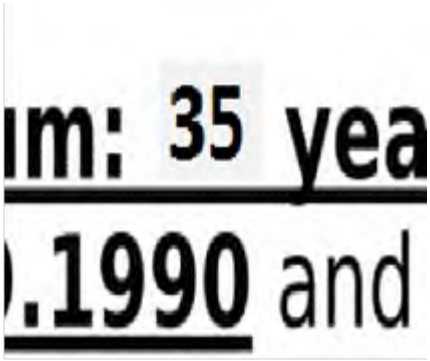
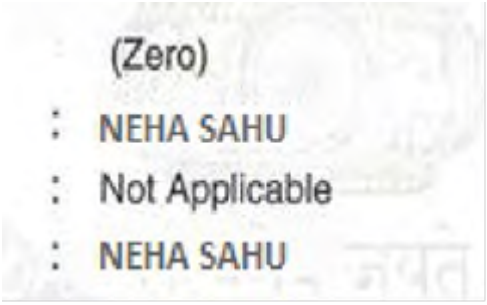
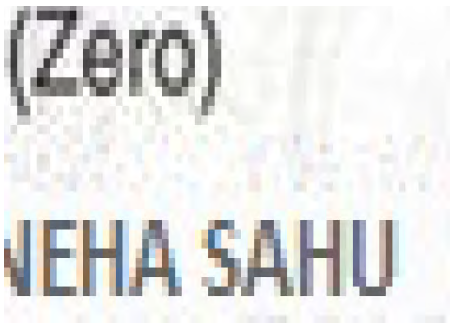
S6		
S7		
S8		
S9		
S10		

Table 3: Examination of samples at 250% and 1200% magnification using Adobe Photoshop.

Author Contribution

- **Varsha Rani Patel:** The author arranged the Figures and Tables as per the format of the Journal.
- **Ritesh Pandey:** The author helped in selecting the software for analysis by performing the trial and analysis on various fake images.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article**.**

Acknowledgments

The authors would like to thank the Department of Forensic Science Medicap's University for providing access to Medicap's library research Journals.

Conflict of Interest

The authors declare that they have no competing interests.

References

1. Shrihari S, Leedham G (2003) A Survey of Computer Methods in Forensic Handwritten Examination. Proceedings Eleventh International Graphonomics Society Conference, Scottsdale, AZ, pp: 278-281.
2. Bradford RR, Ralph B (1992) Introduction to Handwriting and Identification, Nelson-Hall.
3. Huber RA, Headrick AM (1999) Handwriting Identification: Facts and Fundamentals, CRC Press, Boca Raton, New York, USA.
4. Singh A, Mishra MK, Kesharwani L (2018) Detection of Alteration in Suspected Documents – A Case Study. Malaysian Journal of Forensic Sciences 8(1): 21-23.
5. Kelly JS, Lindblom BS (2006) Scientific examination of questioned documents, CRC Press, Bocca Ratton, London, New York, USA.
6. Saini K, Kaur S (2016) Forensic examination of computer-manipulated documents using image processing tools. Egyptian Journal of Forensic Sciences 6(3): 317-322.
7. Joshi MC, Kumar A, Thakur S (2011) Examination of a digitally manipulated-machine generated document. A Case study elucidating the issue of such unwanted progenies of modern technology. Problems of Forensic Sciences 86: 162-173.
8. Shang S, Memon N, Kong X (2014) Detecting documents forged by printing and copying. EURASIP Journal on Advances in Signal Processing.
9. Sameria S, Saran V, Gupta AK (2015) A review of trends in digital image processing for forensic consideration. International Journal of Software & Hardware Research in Engineering 3(8): 8-13.
10. Microsoft Paint.
11. Forensically Beta.
12. FotoForensic.
13. Techopedia.