International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Examination of Tampered Electronic Documents 'Kamalvidya'

Ms. Jaya Giri
M.Sc. Forensic Science, Lok Nayak Jayaprakash Narayan National Institute of Criminology & Forensic Science, PGD Forensic Science, Delhi University, New Delhi, India

ABSTRACT
With the changing scenario of world, towards electronic passage it is important for one to maintain authenticity and move the document "As It Is" from the source to the destination in a defined manner.

Computer reads any e-document in binary language i.e. 0 and 1. The programme so designed is named "**KamalVidya**". Using this programme, it is possible to examine tampered electronic documents and will display the altered text in the allotted space. This programme can be used to investigate tampered e-document as well as can be use to establish a secure passage for e-document transfer. The programme so designed has in-built function to detect and decipher obliteration, addition and deletion in e-documents with capability to locate even a small "dot or space" added or deleted in the e-document. It also includes comparison of two e-documents and finding similarities and differences between them. Today computer forensics is not related to a single domain but it includes various thoughts in various fields which run the whole setup in a defined manner. Today forgery is not limited to civil/criminal cases, it has wide hands in various areas such as banks, MNCs, legal proceedings and many more where electronic document plays major role.

It is the need of time that an application should be made which will identify exact added/deleted/obliterated text in one go.

Any type of electronic document can be tampered by various methods and this research applies to decipher and find out the original document from the forged or tempered one, as per the case.

METHODS OF ALTERATION:-

Addition in genuine e-document	insertion of any clause or sentence may completely change the meaning of a e-document
Obliteration or smeared-over writing	Hiding any written matter by application of various types of clipart or by darken that portion.
Deletion in genuine e-document	Deletion of any clause or sentence may completely change the meaning of any document.

This research will fill the demanding gap in current requirements in examination of e-document and this will also plays an important role in surveillance of any open (but not secure) PCs, laptops and any type of electronic documents. This also ensures secure passage to various departments (banks etc) in a hierarchical unit where passage of information should be secure.

Surprisingly! All these can be done in a single click. This programme has the potential to play a vital role by a forensic expert to summarize his/her evidence in quick and secure manner as well

"**Kamalvidya**" programme is able to examine the tampered electronic documents as follows:-
Added text in the e-document and its exact location in the tampered document

Deleted text in the e-document and its exact location in the tampered document

Comparison of suspected document whether they are similar or not, if only single space is different in the two document then the programme will tell that the two e-documents are not similar

Comparison of suspected PDF files whether they are similar or not.

- if only single space is different in the two documents then the programme will tell that the two e-documents are not similar

Decipherment of obliterated PDF files and displaying the text in another box provided.

It will save the result in the allotted directory and folder with the provided file name by the examiner.

Collection: random collection from various sources. (CD/ SanDisk/Pen drive)

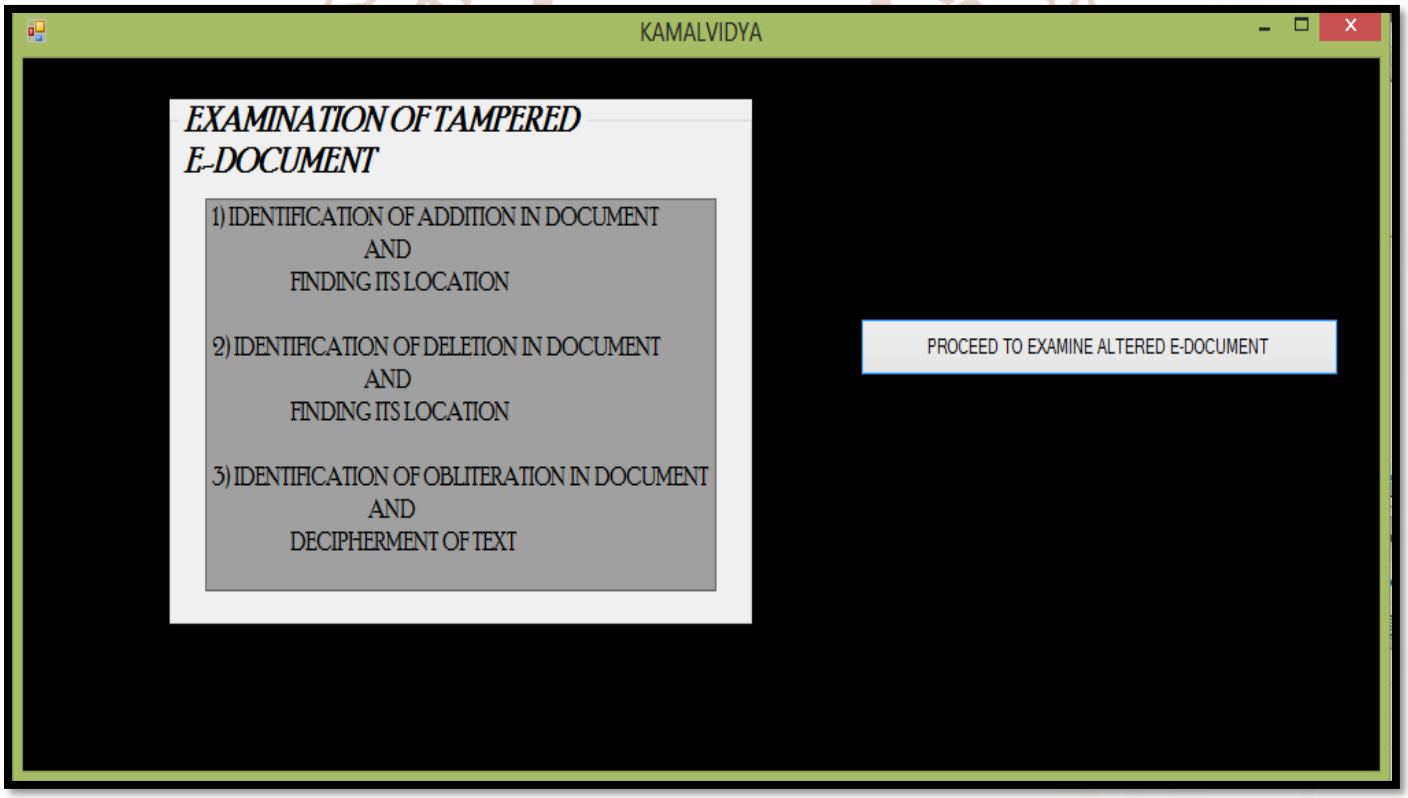
Note: electronic documents used are just hypothetical data and does not pertains to any company or person. All details included are just for demonstration purposes

SOME IMAGES OF THE DEVELOPED APPLICATION:-

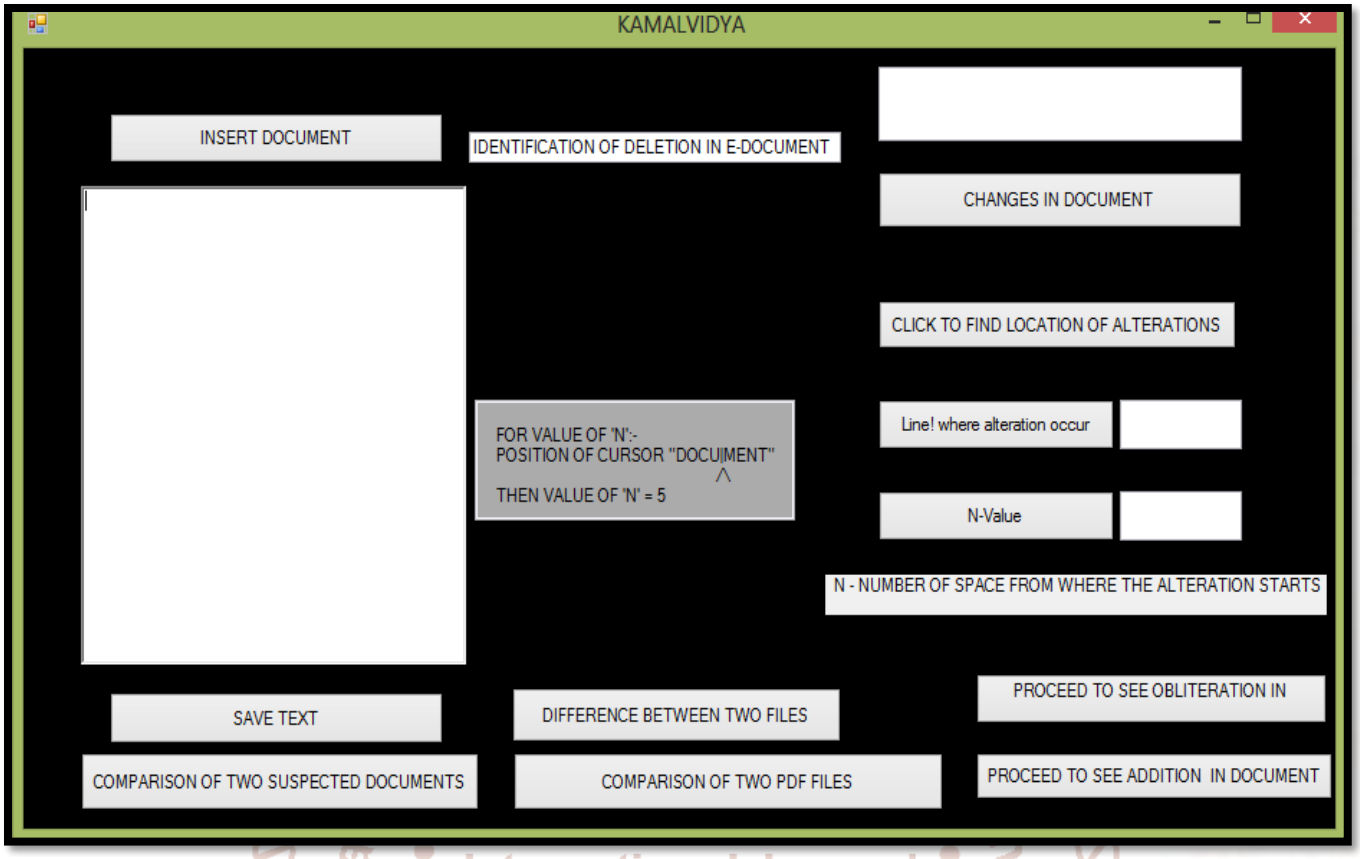
NAME OF PROGRAM: - **KAMALVIDYA**

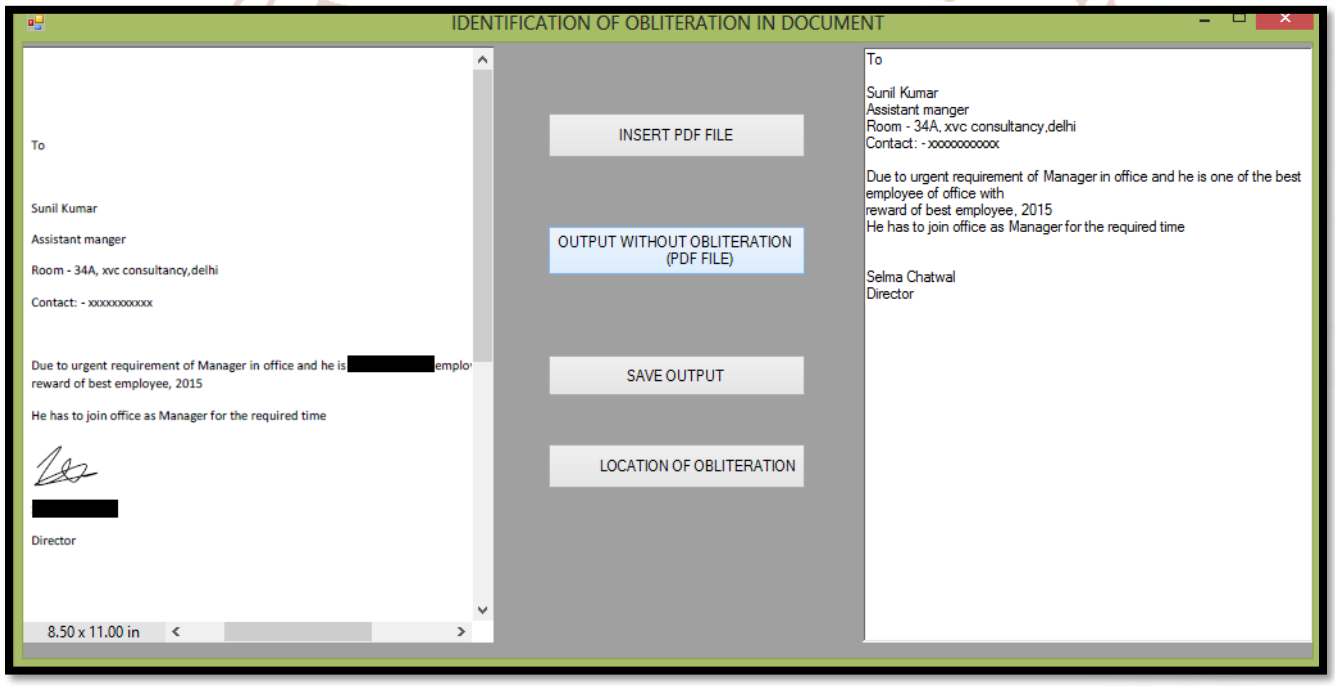
FUNCTION: - IDENTIFICATION OF ALTERATIONS IN E-DOCUMENTS

MAIN SCREEN



Click button “PROCEED TO EXAMINE ALTERED E-DOCUMENT”





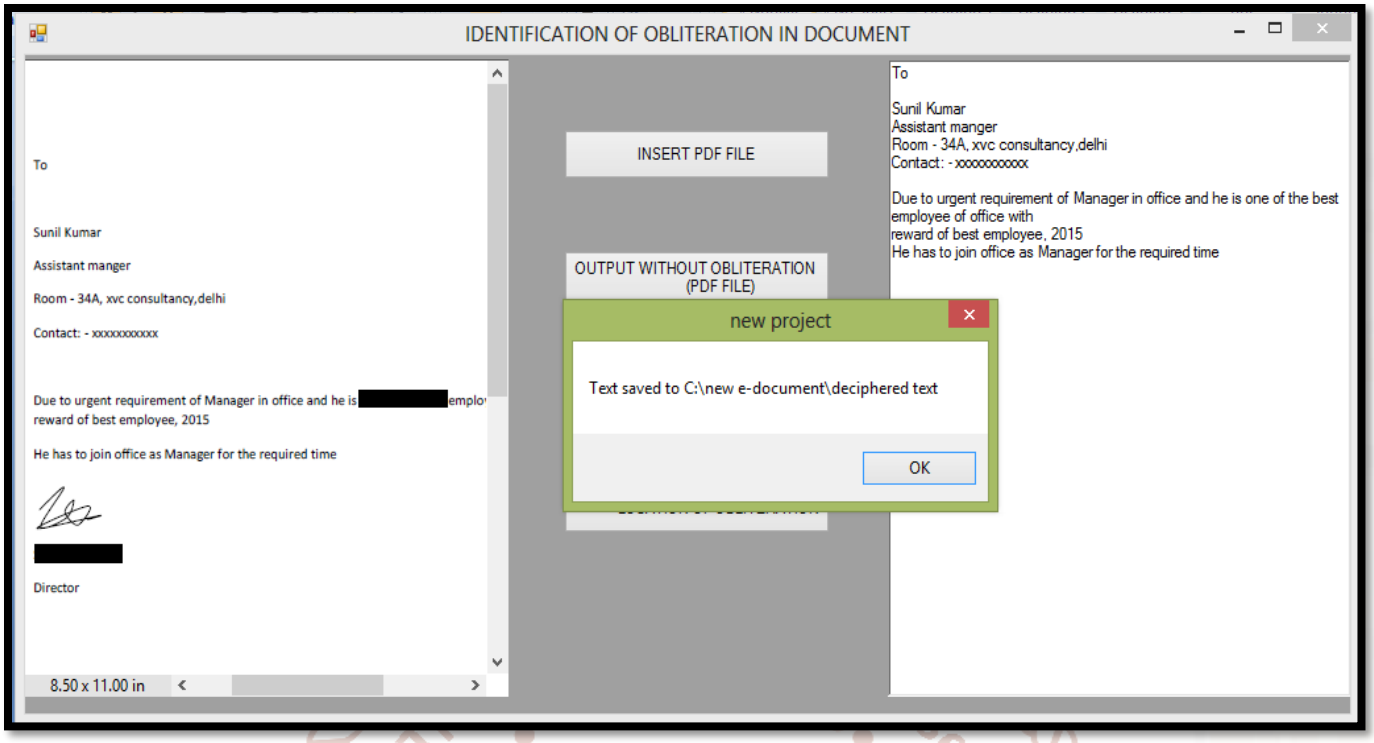
Result:-

After clicking the button, obliteration which was done by blackening that area has been completely deciphered as:-

First obliterated area read as ‘one of the best’

Second obliterated area read as ‘Selma Chatwal’

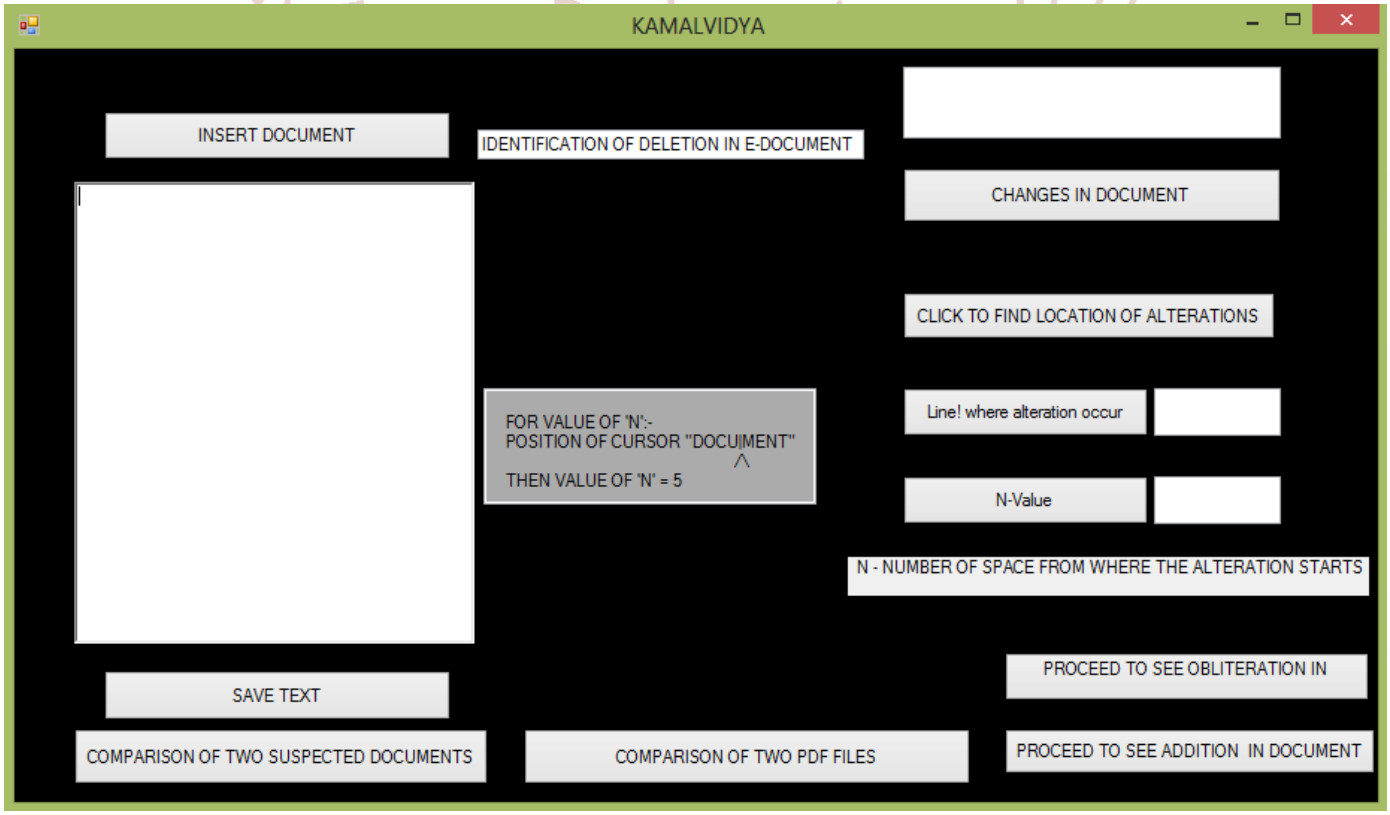
Directory and file where the deciphered text has been saved will be displayed in the message box above the window:-



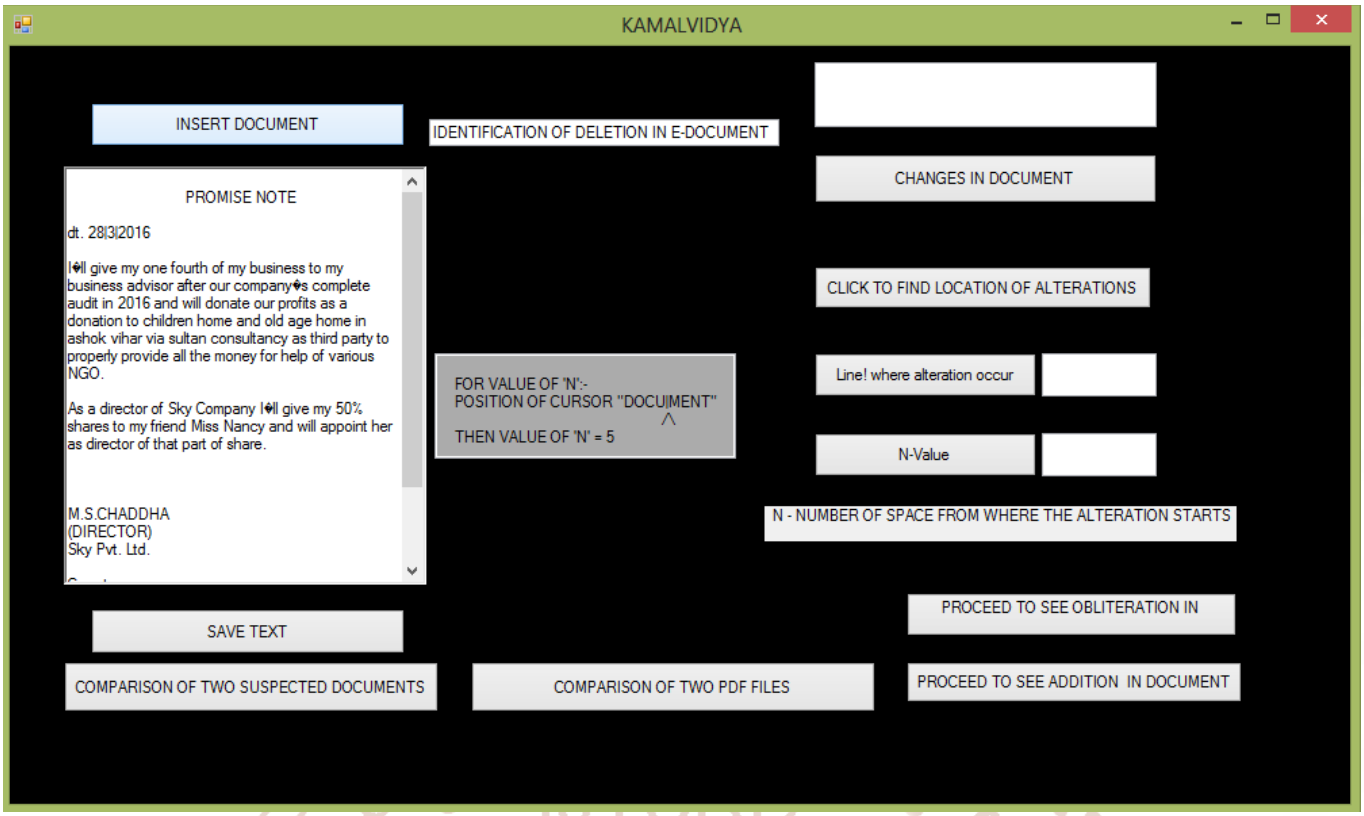
Deciphered text of the above case has been saved in dir. C: / in folder – new e-document with a file name- deciphered text.

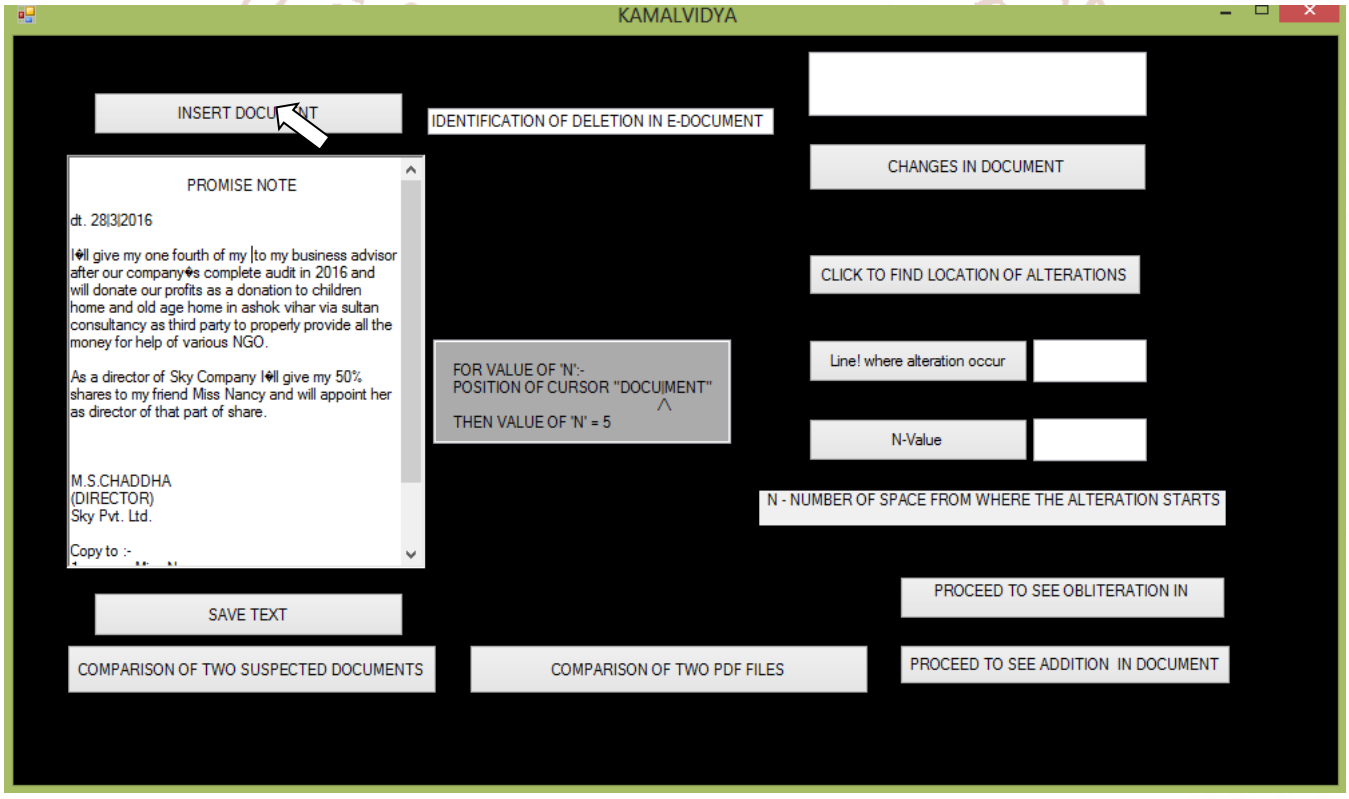
- Selection of the path of result is user friendly which can be change as per the examiner wish.

IDENTIFICATION OF DELETED PORTION IN E-DOCUMENT AND FIND ITS EXACT LOCATION



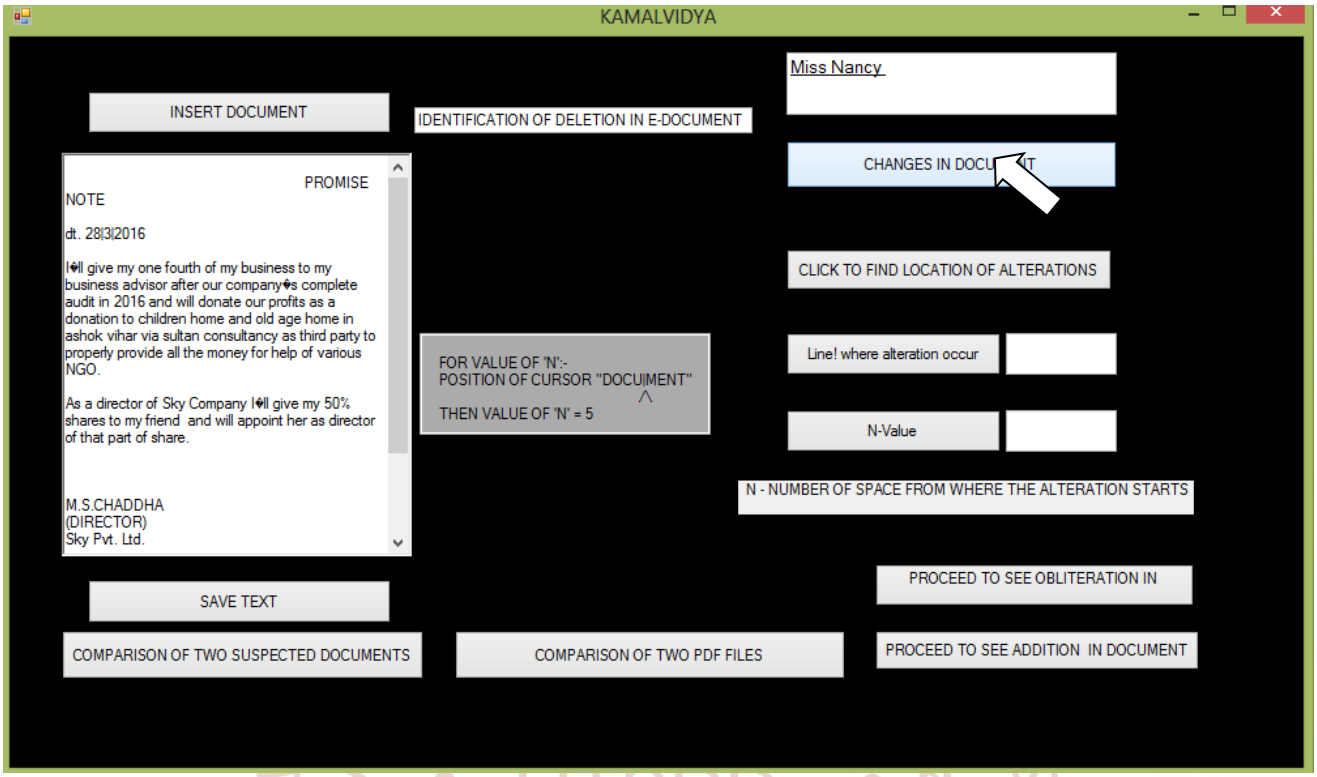
NOW INSERT E-DOCUMENT BY CLICKING BUTTON “INSERT E-DOCUMENT”



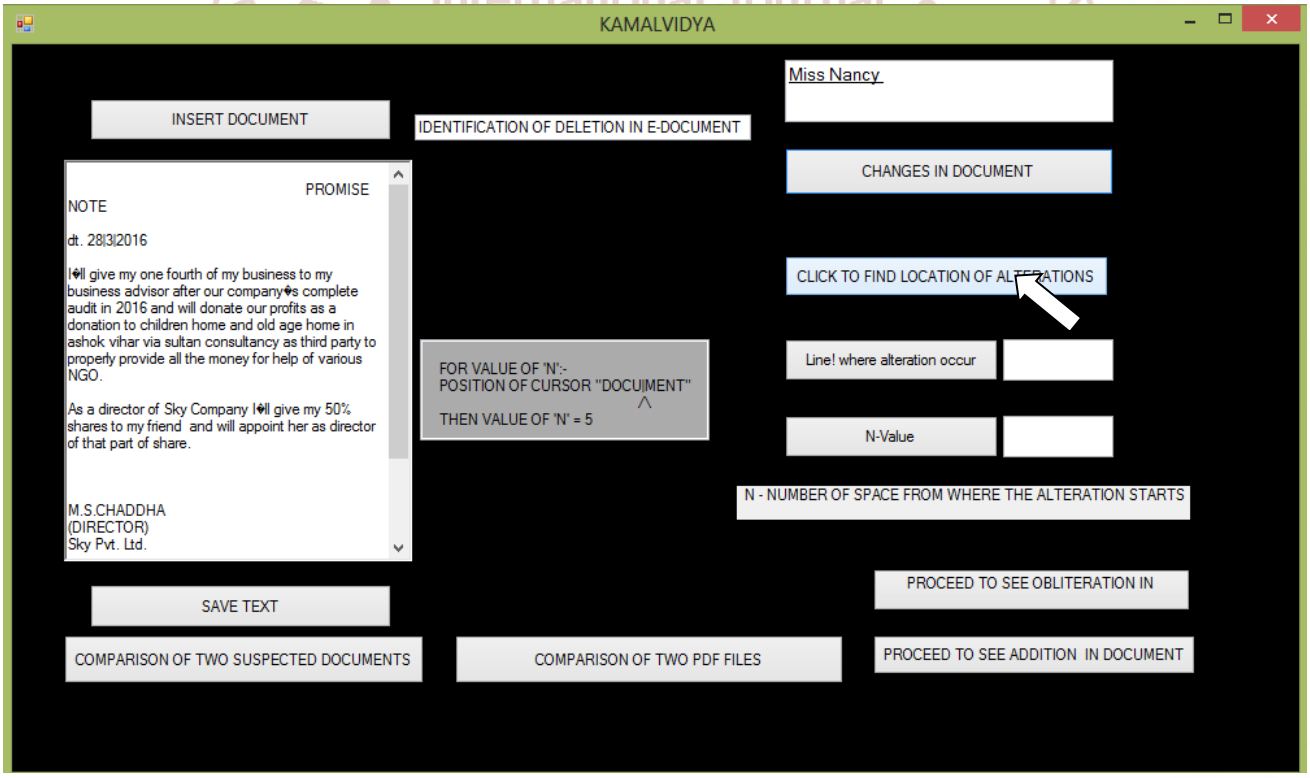


"Miss Nancy" has been deleted from the inserted e-document.

Now, to find the word which was deleted click on button 'CHANGES IN E-DOCUMENT?'
SEE BOX ABOVE THE BUTTON "CHANGES IN E-DOCUMENT".....deleted word from the e-document has been displayed.



To find location of deleted text click on button ‘click to find location of alteration’



Method of finding location of text in e-document:-
Whole text with blank space has been divided into number of rows and columns for example:
Text – “questioned e-document or suspected
E-document”

q	u	e	s	t	i	o	n	e	d		d	o	c	u	m	e	n	t		o	r		s	u	s	p	e	c	t	e	d
d	o	c	u	m	e	n	t																							

Division of text in above program

If word ‘e-document’ has been deleted than its location can be located as follow:-

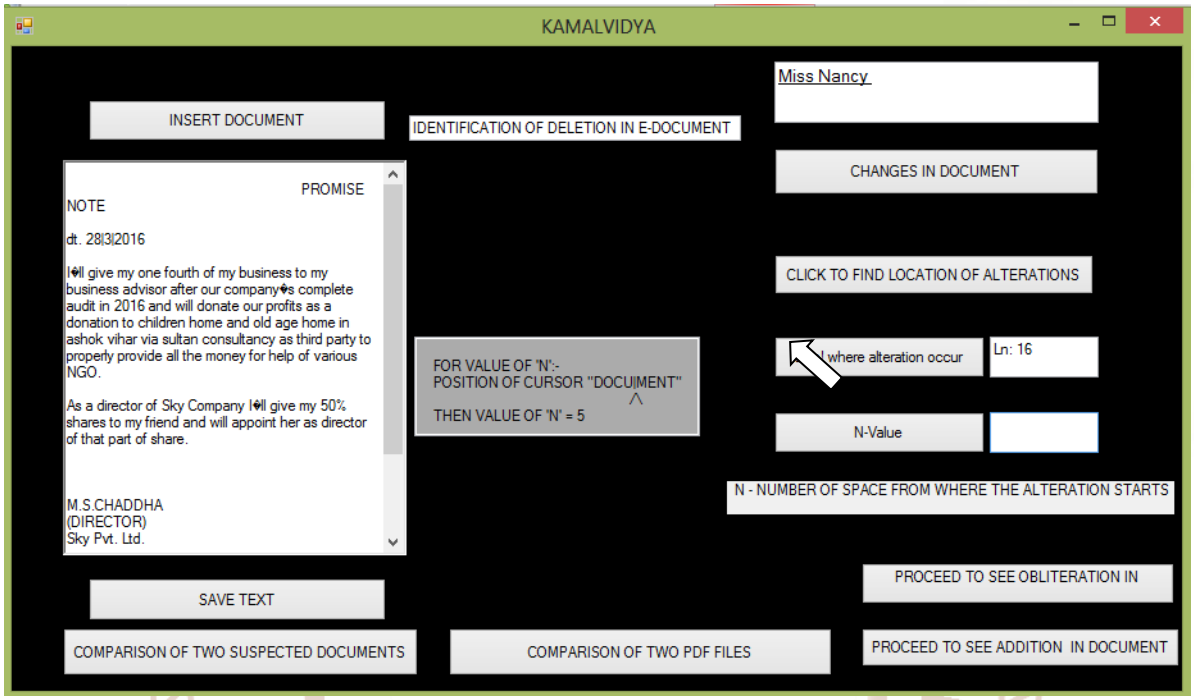
q	u	e	s	t	i	o	n	e	d									o	r		s	u	s	p	e	c	t	e	d
d	o	c	u	m	e	n	t																						

Above text has:-

Number of lines – 2

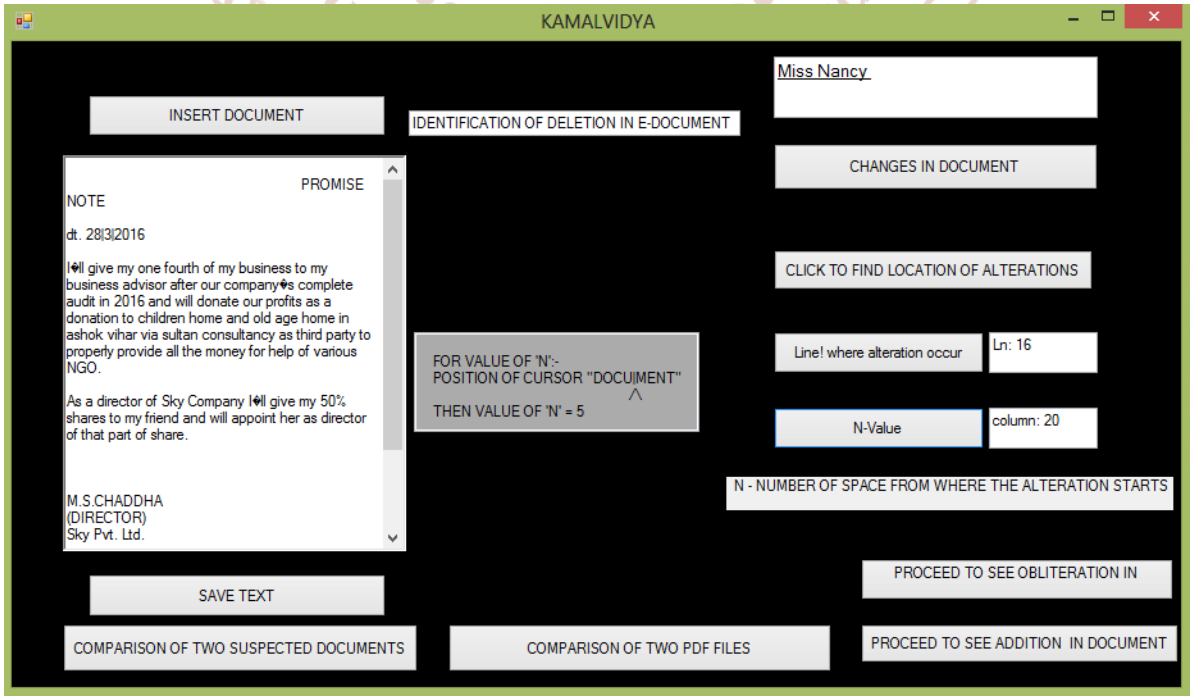
Note: - N-value is the number of alphabets and spaces in a particular line, N-value of line 1 is 32

N-value – 12



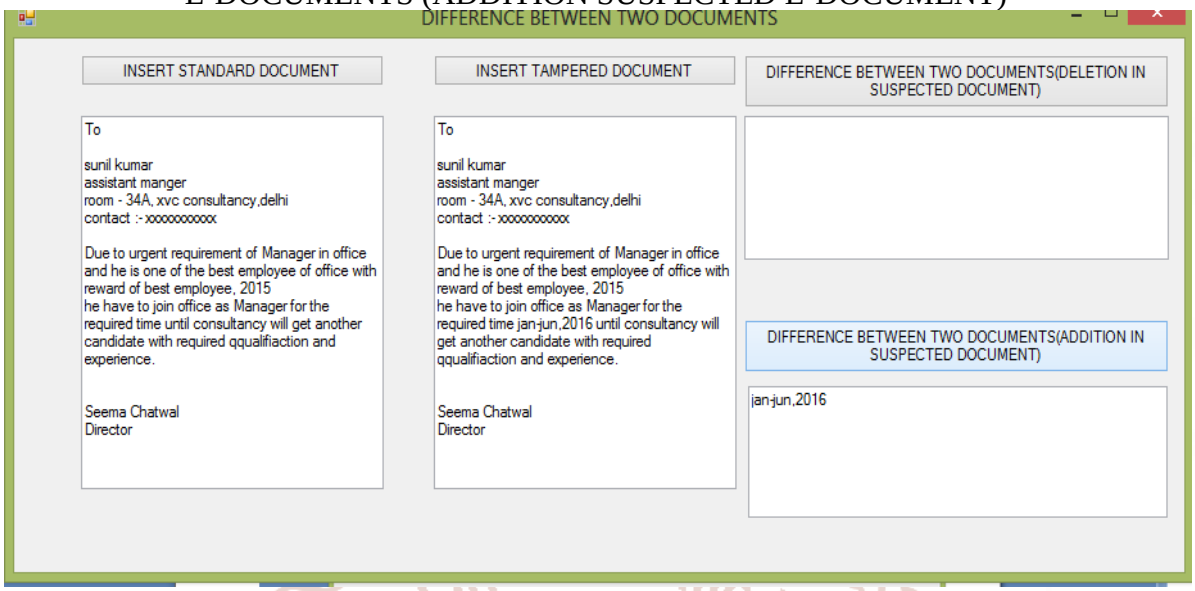
“Miss Nancy” is in 16th line of the inserted text.

To locate the place from where the deletion starts:-



N-value of text “Miss Nancy” in inserted text is 20

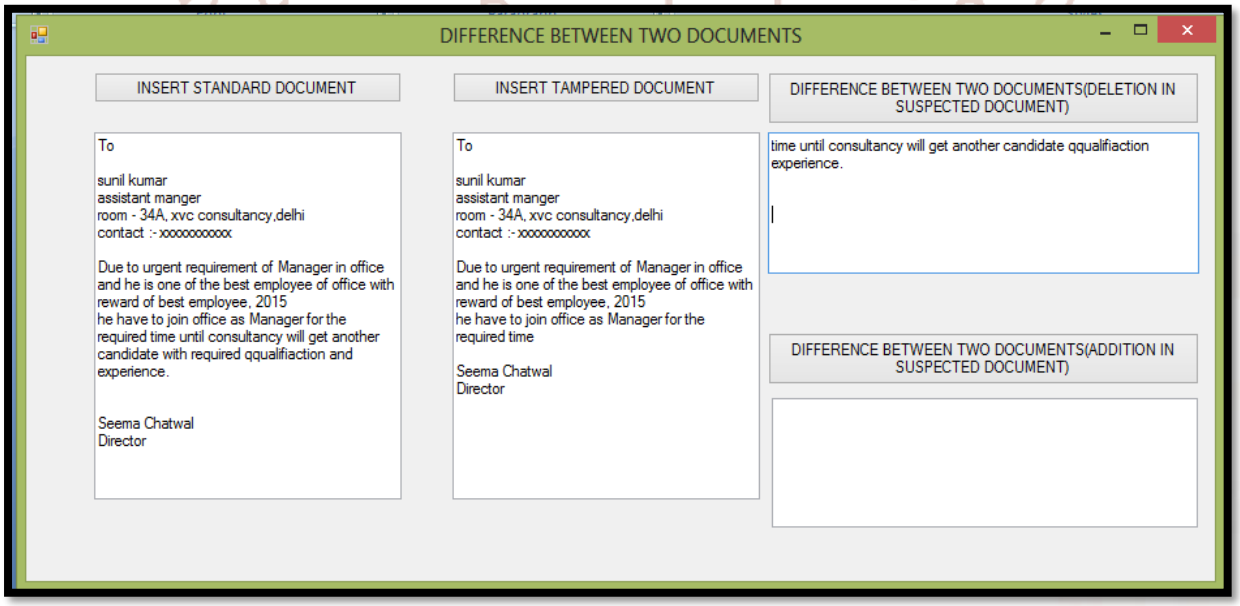
To identify the added text in the tampered e-document click on button ‘DIFFERENCE BETWEEN TWO E-DOCUMENTS (ADDITION SUSPECTED E-DOCUMENT)



In the above window added text in the tampered e-document has been identified i.e. ‘jan-jun, 2016’ has been added

So, added text will be displayed in the space present below the clicked button.

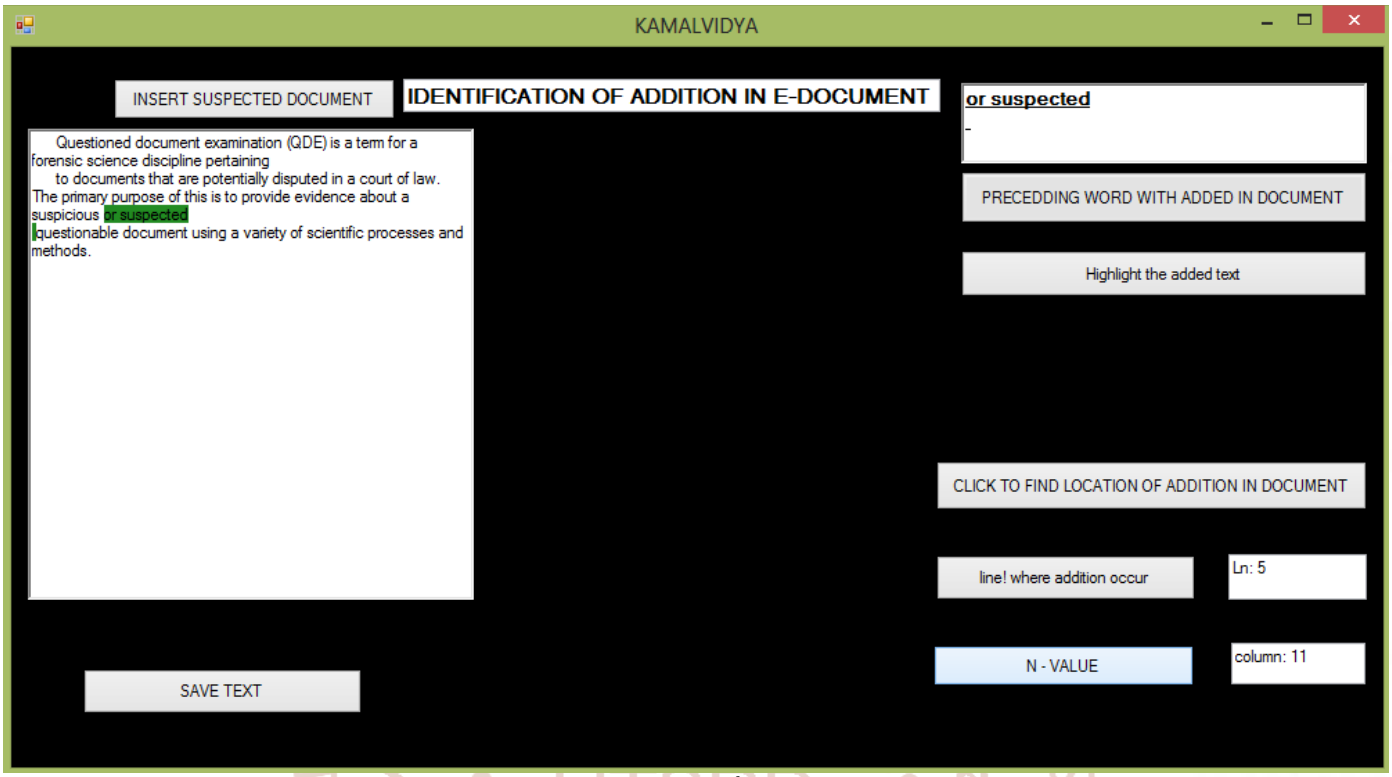
Note: - in this case there is no preceding word as there is difference of one space between preceding and the added text.



After successfully inserting the text of the standard and tampered e-document in the space provided, examiner will proceed to identified the deleted text in the tampered e-document by clicking button ‘DIFFERENCE BETWEEN TWO E-DOCUMENTS (DELETION IN SUSPECTED E-DOCUMENT)

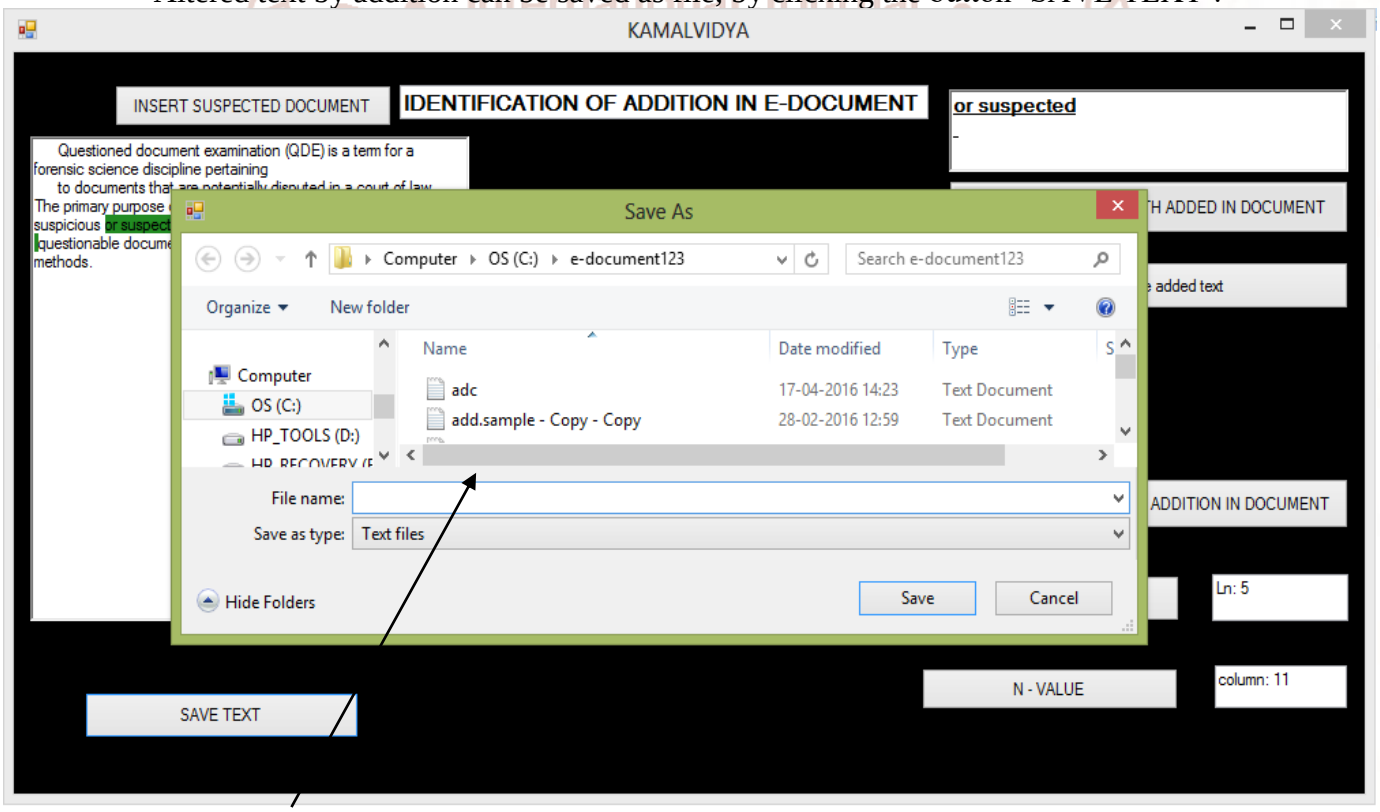
In the above case by clicking the respective button the deleted text of the tampered e-document has been displayed in the space provided

Deleted text is ‘time until consultancy will get another candidate qualification experience.’

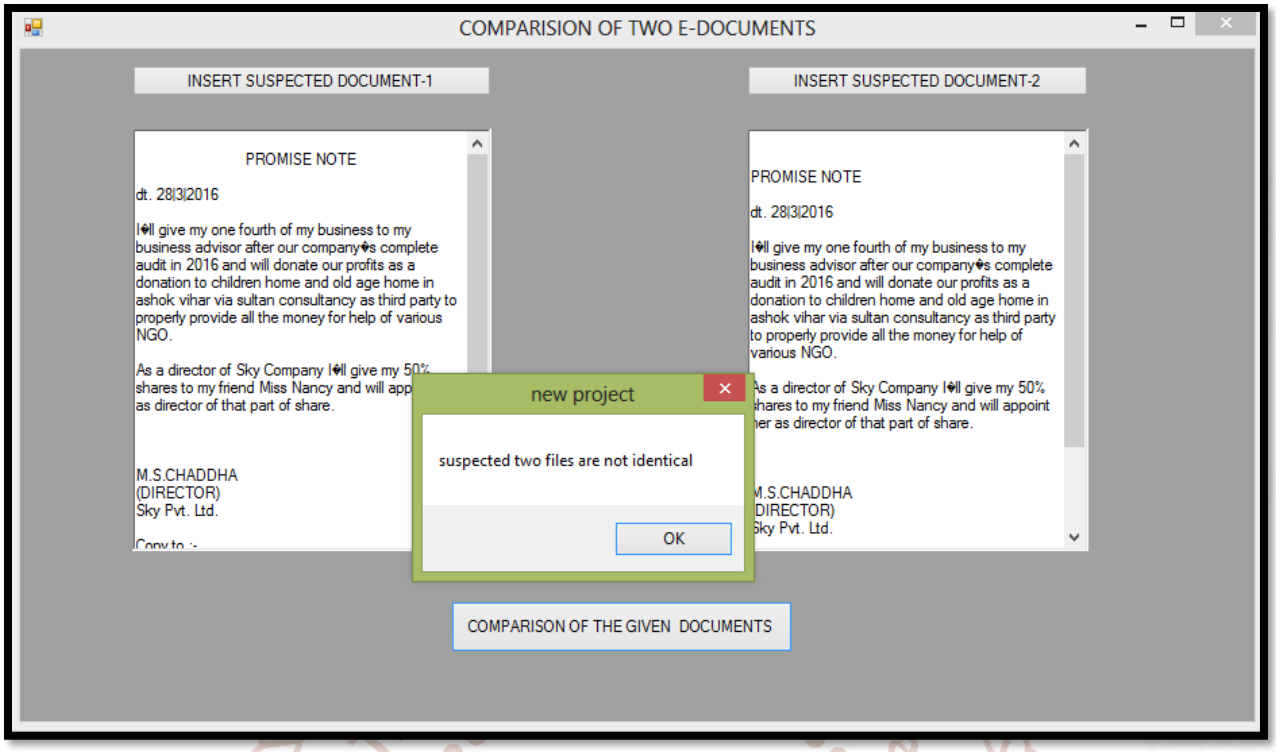


N-value is 11th place.

Altered text by addition can be saved as file, by clicking the button 'SAVE TEXT'.



Enter file name



In the above case the text of two suspected files are identical, but because of different spacing and alignment output will be 'the given files are not identical'

Advantage: - if the original copy has been extracted from somewhere else then the altered file that was supposed to be the genuine copy with exact details as that of original copy can be examine authentically

Conclusion: the application can deal with tampered document as follows:

- Comparison of suspected PDF files: - two suspected files were identical and two suspected files were different.
- Comparison of two suspected text files and display the difference between them:-the standard and tampered e-document has been compared and the difference has been displayed in the space allotted for result.
- Decipherment of obliteration in e-document:- the obliterated part has been successfully deciphered and the text has been displayed in the space allotted
- Identification of added text in the suspected e-document:- the added text has been identified and the result has been displayed in the space allotted
- Identification of deleted text in the suspected file: - the deleted text has been successfully identified and displayed in the space allotted.
- Comparison of suspected two files: - comparison of two suspected files has been done and whether the files are identical or not has been displayed in the message box above the window.

All the result has been saved in the selected directory and files by the user.

References

1. **Albert Marcella, Jr.**, **Doug Menendez**, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Second Edition (Information Security), CRC Press, 19 Dec 2007
2. Santanam, Raghu, **Cyber Security, *Cyber Crime and Cyber Forensics: Applications and Perspectives***, IGI Global, 1 Oct 2010
3. **Albert J. Marcella, Jr., Frederic Guillossou, *Cyber Forensics: from Data to Digital Evidence***, Wiley; 1 edition (27 March 2012)
4. **Syngress, *Scene of the Cybercrime: Computer Forensics Handbook,*** Syngress Media, U.S. (12 August 2002)
5. **Jack Wiles, Anthony Reyes, *The Best Damn Cybercrime and Digital Forensics Book Period,*** Syngress Media, U.S. (7 December 2007)
6. **Steve Bunting**, ,.*EnCase Computer Forensics -- The Official EnCE: EnCase Certified Examiner*

Study Guide, Sybex; 3rd Edition edition (7 September 2012)

7. Claus Vielhauer, *Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates*, Springer; 2011 edition (7 March 2011)
8. **Albert Marcella, Jr.**, **Doug Menendez**, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* Auerbach Publications; 2 edition (19 December 2007) – 19 Dec 2007
9. **Albert J. Marcella, Jr., Frederic Guillossou,** ***Cyber Forensics: From Data to Digital Evidence,*** Wiley; 1 edition (27 March 2012)
10. **Debra Littlejohn Shinde,** ***Scene of the Cybercrime: Computer Forensics Handbook,*** Syngress Media, U.S. (12 August 2002)
11. **Steven Holzner,** *Visual Basic .NET Programming* , Dreamtech Press (27 June 2005)
12. **Dr. A. Murugan, Dr. K. Shyamala,** *Visual Basic Programming* , Margham Publications; 2 edition (2012)
13. **Jeremy Shapiro** *Visual Basic(R).Net: The Complete Reference*, McGraw Hill Education India Private Limited; 1 edition (24 September 2002)
14. **Sanjeev Sharma, Nandan Tripathi,** *Visual Basic 6*, Excel Books (1 January 2009)
15. **Soma Dasgupta**, *Visual Basic Projects*, Bpb (1 November 2002)
16. Eoghan casy, *Digital evidence and computer crime: forensic science, computers and the internet* second edition, academic press(2004)
17. John r. vacca, *computer forensics: computer crime scene investigation*, Charles river media inc.,(2004)