

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- This research will fill the demanding gap in current 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 which will identify made 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	insertion of any clause or
genuine e-	sentence may completely change
document	the meaning of a e-document
Obliteration	Hiding any written matter by
or smeared-	application of various types of
over writing	clipart or by darken that portion.
Deletion in	Deletion of any clause or
genuine e-	sentence may completely change
document	the meaning of any document.

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

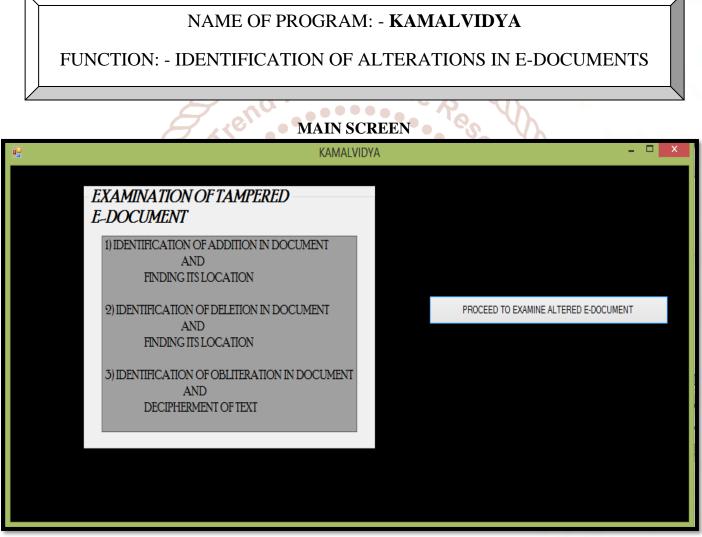
Decipherment of obliterated PDF files and displaying the text in another box provided.

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:-



Click button "PROCEED TO EXAMINE ALTERED E-DOCUMENT"

12	KAMALVIDYA	- • • • • • • • • • • • • • • • • • • •
INSERT DOCUMENT	IDENTIFICATION OF DELETION IN E-DOCUMENT	
		CHANGES IN DOCUMENT
		CLICK TO FIND LOCATION OF ALTERATIONS
	FOR VALUE OF 'N':- POSITION OF CURSOR "DOCUIMENT"	Line! where alteration occur
	THEN VALUE OF 'N' = 5	N-Value
	N - 1	NUMBER OF SPACE FROM WHERE THE ALTERATION STARTS
SAVE TEXT	DIFFERENCE BETWEEN TWO FILES	PROCEED TO SEE OBLITERATION IN
COMPARISON OF TWO SUSPECTED DOCUMENTS	COMPARISON OF TWO PDF FILES	PROCEED TO SEE ADDITION IN DOCUMENT
lia ••	International Journ	nal 🖌 🖌
	IDENTIFICATION OF OBLITERATION IN DOCUM	ENT – 🗆 💌
То	INSERT PDF FILE	To Sunii Kumar Assistant manger Room - 34A, xvc consultancy,delhi Contact: - x0000000000
Sunil Kumar		Due to urgent requirement of Manager in office and he is one of the best employee of office with reward of best employee, 2015 He has to join office as Manager for the required time
Assistant manger Room - 34A, xvc consultancy,delhi	OUTPUT WITHOUT OBLITERATION (PDF FILE)	Selma Chatwal
Contact: - x0000000000		Director
Due to urgent requirement of Manager in office and he is reward of best employee, 2015 He has to join office as Manager for the required time	SAVE OUTPUT	
100	LOCATION OF OBLITERATION	
Director		
8.50 x 11.00 in <	× >	

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:-

P IDENTIFICAT	TION OF OBLITERATION IN DOCUM	1ENT – 🗆 🗙
То	INSERT PDF FILE	To Sunii Kumar Assistant manger Room - 34A, xvc consultancy,delhi Contact: - x0000000000
Sunil Kumar Assistant manger Room - 34A, xvc consultancy,delhi	OUTPUT WITHOUT OBLITERATION (PDF FILE)	Due to urgent requirement of Manager in office and he is one of the best employee of office with reward of best employee, 2015 He has to join office as Manager for the required time
Contact: - xxxxxxxxxxxx Due to urgent requirement of Manager in office and he is employement of Manager in office and he is	new project Text saved to C:\new e-document\decipt	× hered text
He has to join office as Manager for the required time		ОК
Director		
8.50 x 11.00 in K		

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

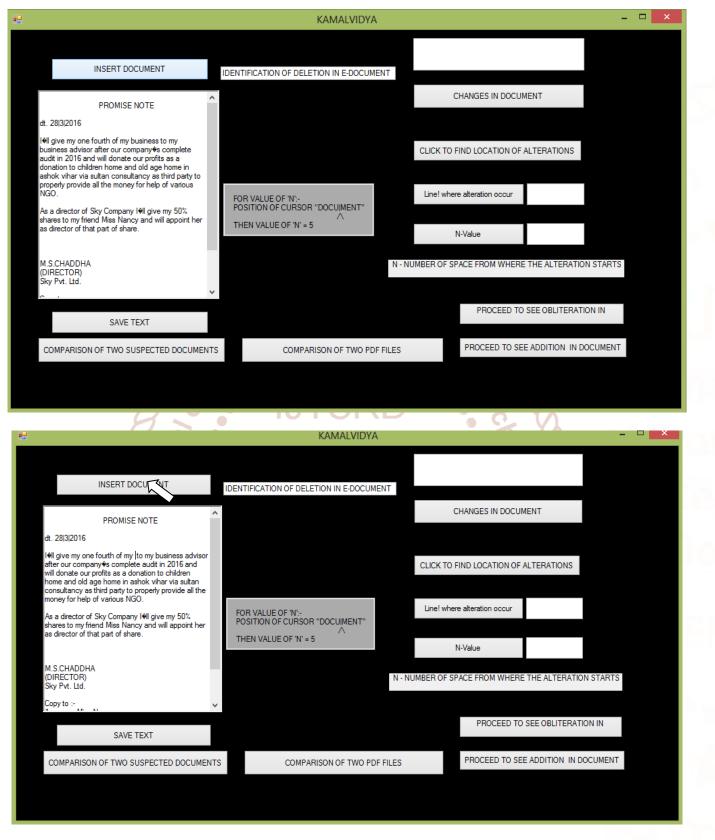
International Journal

> 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

•	KAMALVIDYA	- 🗆 🗙
INSERT DOCUMENT	IDENTIFICATION OF DELETION IN E-DOCUMENT	
l I		CHANGES IN DOCUMENT
		CLICK TO FIND LOCATION OF ALTERATIONS
	FOR VALUE OF 'N':- POSITION OF CURSOR "DOCUIMENT"	Line! where alteration occur
	THEN VALUE OF 'N' = 5	N-Value
	N - NU	JMBER OF SPACE FROM WHERE THE ALTERATION STARTS
SAVE TEXT		PROCEED TO SEE OBLITERATION IN
COMPARISON OF TWO SUSPECTED DOCUMENTS	COMPARISON OF TWO PDF FILES	PROCEED TO SEE ADDITION IN DOCUMENT

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.

	KAMALVIDYA	-
INSERT DOCUMENT	Miss Nancy	
PROMISE	CHANGES IN DOCU	
dt. 28 3 2016 I till give my one fourth of my business to my business advisor after our company tills complete audit in 2016 and will donate our profits as a donation to children home and old age home in ashok wihar via sultan consultancy as third party to property provide all the money for help of various NGO. As a director of Sky Company I till give my 50% shares to my friend and will appoint her as director of that part of share.	FOR VALUE OF 'N':- CLICK TO FIND LOCATION OF ALTERATIONS POSITION OF CURSOR "DOCUIMENT" Line! where alteration occur THEN VALUE OF 'N' = 5 N-Value	
M.S.CHADDHA (DIRECTOR) Sky Pvt. Ltd.	N - NUMBER OF SPACE FROM WHERE THE ALTERAT	
SAVE TEXT	PROCEED TO SEE OBLITERA	ATION IN
COMPARISON OF TWO SUSPECTED DOCUME	COMPARISON OF TWO PDF FILES PROCEED TO SEE ADDITION IN	DOCUMENT

To find location of deleted text click on button 'click to find location of alteration'

	International Journal 👗 🍊	Y A
9 <u>9</u>	KAMALVIDYA	- 🗆 🗙
INSERT DOCUMENT	Miss Nancy	
PROMISE NOTE dt. 28/3/2016	CHANGES IN DOCU	MENT
Ive give my one fourth of my business to my business advisor after our company vs complete audit in 2016 and will donate our profits as a donation to children home and old age home in ashok vihar via sultan consultancy as third party to	CLICK TO FIND LOCATION OF	ALTRATIONS
property provide all the money for help of various NGO. NGO. As a director of Sky Company I till give my 50% shares to my friend and will appoint her as director	FOR VALUE OF 'N':- POSITION OF CURSOR "DOCUMENT" THEN VALUE OF 'N' = 5 N-Value	
of that part of share. M.S.CHADDHA (DIRECTOR)	N - NUMBER OF SPACE FROM WHER	E THE ALTERATION STARTS
Sky Pvt. Ltd.	Y PROCEED TO	D SEE OBLITERATION IN
COMPARISON OF TWO SUSPECTED DOCUME	NTS COMPARISON OF TWO PDF FILES PROCEED TO SE	E ADDITION IN DOCUMENT

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	0	n	e	d	d	0	с	u	m	e	n	t	0	r	S	u	S	р	e	с	t	e	d
d	lo	2	u	m	e	n	t																					

Division of text in above program

If word '	e-document'	has been	deleted that	in its location	can be lo	cated as follow:-
-----------	-------------	----------	--------------	-----------------	-----------	-------------------

(q	u	e	S	t	i	0	n	e	d						0	r	S	u	S	р	e	c	t	e	d
(d	0	с	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



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)

		SUSPECTED DOCUMENT)
To sunil kumar assistant manger room - 34A, xvc consultancy, delhi contact :-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	To sunil kumar assistant manger room - 34A, xvc consultancy,delhi contact - xxxxxxxxxxxxxxx Due to urgent requirement of Manager in office and he is one of the best employee of office with reward of best employee, 2015 he have to join office as Manager for the required time jan-jun,2016 until consultancy will get another candidate with required qualifiaction and experience.	DIFFERENCE BETWEEN TWO DOCUMENTS(ADDITIC SUSPECTED DOCUMENT)
Seema Chatwal Director	Seema Chatwal Director	jan-jun,2016

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.

•	DIFFERENCE BETWEEN TWO DOCUM	ents – 🗆 🗙
INSERT STANDARD DOCUMENT	INSERT TAMPERED DOCUMENT	DIFFERENCE BETWEEN TWO DOCUMENTS(DELETION IN SUSPECTED DOCUMENT)
To sunil kumar assistant manger room - 34A, xvc consultancy,delhi contact :- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	To sunil kumar assistant manger room - 34A, xvc consultancy,delhi contact : xxxx consultancy,delhi Due to urgent requirement of Manager in office and he is one of the best employee of office with reward of best employee, 2015 he have to join office as Manager for the required time Seema Chatwal Director	time until consultancy will get another candidate qqualifiaction experience. DIFFERENCE BETWEEN TWO DOCUMENTS(ADDITION IN SUSPECTED DOCUMENT)

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.'

-	KAMALVIDYA		- 🗆 🗙
INSERT SUSPECTED DOCUMENT Questioned document examination (QDE) is a term f forensic science discipline pertaining	IDENTIFICATION OF ADDITION IN E-DOCUMENT	or suspected -	
to documents that are potentially disputed in a court The primary purpose of this is to provide evidence abou suspicious preuspected questionable document using a variety of scientific proc methods.	ta and a second se	PRECEDDING WORD WITH ADD	DED IN DOCUMENT
		Highlight the added	l text
		CLICK TO FIND LOCATION OF ADDIT	ION IN DOCUMENT
		line! where addition occur	Ln: 5
SAVE TEXT		N - VALUE	column: 11
Re	N-value is 11 th place.	N N	

N-value is 11th place.

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

		KAMALVIE		o mon on	1-2/4	_ 🗆 🗙
Questione	INSERT SUSPECTED DOCUMENT	ENTIFICATION OF ADDITION	N IN E-DOCUMENT	or suspected		
forensic scien	ce discipline pertaining ents that are potentially disputed in a court of law urpose (Save As			×	H ADDED IN DOCUMENT
questionable methods.	docume ⓒ ⋺ → ↑ 퉱 ≻ Comp Organize → New folder	e 🕞 🦻 🔻 🖡 k Computer k OS (C:) k e-document123			م added text	added text
	INCOMPUTER INCOM	Name adc add.sample - Copy - Copy	Date modified 17-04-2016 14:23 28-02-2016 12:59	Type Text Document Text Document	s ^ >	
L	File name: Save as type: Text files		Sav	e Cancel	× •	ADDITION IN DOCUMENT
	SAVE TEXT			N - VALUI	E	column: 11

Enter file name

	COMPARISION OF TWO E-DOCUMENTS – 🗆 🗙						
INSERT SUSPECTED DOCUMENT PROMISE NOTE dt. 28[3]2016 I el give my one fourth of my business to my business advisor after our company es compl audit in 2016 and will donate our profits as a donation to children home and old age home ashok whar via sultan consultancy as third p proper whar via sultan consultancy as third p	INSERT SUSPECTED DOCUMENT-1 INSERT SUSPECTED DOCUMENT-2 PROMISE NOTE dt. 28/3/2016 IMI give my one fourth of my business to my business advisor after our company the complete audit in 2016 and will donate our profits as a donation to children home and old age home in ashok vihar via sultan consultancy as third party to properly provide all the money for help of various						
NGO. As a director of Sky Company III give my 50 shares to my friend Miss Nancy and will app as director of that part of share. M.S.CHADDHA (DIRECTOR) Sky Pvt. Ltd. Conv.to		donation to children home and old age home in ashok vihar via sultan consultancy as third party to properly provide all the money for help of various NGO. As a director of Sky Company I II give my 50% shares to my friend Miss Nancy and will appoint her as director of that part of share. M.S.CHADDHA DIRECTOR) Sky Pvt. Ltd.					

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'

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.

Advantage: - if the original copy has been extracted All the result has been saved in the selected directory from somewhere else then the altered file that was and files by the user.

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 edocument:- 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.

References

- 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
 - 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)

- Claus Vielhauer, Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, Springer; 2011 edition (7 March 2011)
- 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
- 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)

- Dr. A. Murugan, Dr. K. Shyamala, Visual Basic Programming, Margham Publications; 2 edition (2012)
- 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)

International Journal of Trend in Scientific Research and Development

SSN: 2456-6470