# An Image Steganography Technique for Files and Messages

Rutvij H. Jhaveri SVM Institute of Technology Old N.H.-8 Bharuch, Gujrat Kruti J. Dangarwala SVM Institute of Technology Old N.H.-8 Bharuch, Gujrat Ashish D. Patel SVM Institute of Technology Old N.H.-8 Bharuch, Gujrat

# ABSTRACT

Digital Steganography is a process of hiding confidential digital information into a file of any kind. Digital Information is a resource which holds a lot of value in the modern world. In this paper we propose Steganography with SMS alert which is an approach to send secure digital information over a network in a secure way. The proposed algorithm secures files and messages and targets enterprise level security to hide and deploy digital information without the risk of network attacks or data theft.

#### **General Terms**

Security, Steganography, Files, Messages.

#### **Keywords**

Information security, Digital steganography, Proposed algorithm.

# 1. INTRODUCTION

Steganography is a technique to hide messages or files into another file so that one does not recognize major changes in the contents of the original file. In this technique messages and files can be embedded and made password protected in the first phase and being made as steganos file. Embedded file will be uploaded to a web server and link of the file and password will be sent as an SMS to the specified recipient through gateway. Embedded file can be downloaded and then extracted with our software application by providing the specified password.

# 2. PROPOSED ALGORITHM

Our Algorithmic concept in our application is as follows as shown in Fig. 1:

- 1. Input source file 1, target File 2 and password.
- 2. Then both the files are converted into binary files.
- 3. Both binary files are stored in byte array according to the input sequence of the file (First file 1 and then file 2).
- 4. The password is encrypted and it is stored in the byte array at the end after file 2.
- 5. The merged file will be stored as the extension of first file, File 1.



Fig. 1: Embedding a File

Sending and receiving the steganos file is shown in Fig. 2

- 6. The merged new steganos file is uploaded on Internet.
- 7. File link is uploaded and password is sent to receiver's mobile via SMS.
- 8. Receiver downloads and opens file with the given password.

stego file Upload to net Send upload link and pessword through sms	reciver recieved link and paa\sword and download file and open	
--	---	--

Fig. 2: Sending and Receiving the Steganos File

# 3. APPLICATION DESCRIPTION

We carry out our implementation by using Microsoft DOT NET Framework 2.0 as front-end and MS-SQL 2005 as back-end.

# 3.1 Embedding and Retrieving File

The complete flow of the application is as follows:

- 9. First choose any options as shown in Fig. 3.
- 10. On selecting option embed file, as shown in Fig. 4, input source file, target file, and target location where embedded file is to be stored. After successfully embedding files as shown in Fig. 5, enter secret password and mobile number of recipient as shown in Fig. 6.
- 11. Click OK to embed file for specific path.
- 12. If the choice is to retrieve file then input embedded file and target location where to store the file, using a password.



Fig. 3: Options in Application Software

National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012 Proceedings published by International Journal of Computer Applications® (IJCA)

Embed_File		
	EMBED FILE	
Source File	D:\Photos\101CAN Browse Sour	ce
Target File	D:\Photos\101CAN Browse Targ	jet
Embed File	D:\Photos\101CAN Browse Emb	ed
Mobile No. (+91)	9427834368	
Password	Z	
	Ok Ext	

#### Fig. 4: Embedding File

Embed_File		
Ŀ	EMBED FI	LE
Source File	D:\Photos\101CAN	Browse Source
Target File		se Target
Embed File	Successfully Embeddeded	se Embed
Mobile No. (+91)	ОК	
Password	v	
	Ok	Exit

#### Fig. 5: File Embedded Successfully

Embed_File	
	EMBED FILE
Source File	D:\Photos\101CAN Browse Source
Target File	Send arget
Embed File	Do you want to send pass to Mobile?
Mobile No. (+9	Yes No
Password	☑
	Ok Exit

Fig. 6: Send Password via SMS

# 3.2 Embedding and Retrieving Message

- 13. First select the source file, target location, message and optional passowrd as shown in Fig. 7.
- 14. Mobile number of user is to be entered by the user for sending password as shown in Fig. 8.
- 15. If the choice is to retrieve message then input embedded file and target location where to store the file, using the password as shown in Fig. 9
- 16. If message is retrieved successfully, a message is shown as shown in Fig. 10.

Embed_Message		
Emt	oed Mess	sage
Source File	D:\Photos\101CAN	Browse Source
Embed File	D:\Photos\101CAN	Browse Save
Message	Hi.Howru?	
Mobile No. (+91) 🛛	9925366666	
Password 🗸		
Ok	Exit	

#### Fig. 7: Embedding Message

Source	File	D/) Rhotes) 10	ICAN		1
Jource	Send	D. (Photos (Tu	Br	owse Source	
Embed			В	rowse Save	
Messag	Do you want	to send pass to Mo	obile?		
		Yes	No		
Mobile	NO. (+31)	3325366666			
Passwo	ord 🗸	••••••			

Fig. 8: Send Password via SMS

National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012 Proceedings published by International Journal of Computer Applications® (IJCA)

Retrieve_Message		
Retriev	ve Mess	age
Browse Embedded File	D:\Photos\101CAN	Browse Embedded File
Save Retrieve File	D:\Photos\101CAN	Save Embedded File
Password		
Retrieve Message	Ext	

Fig. 9: Retrieve Message

Retrieve_Message	And a local division of the same	
Ret	rieve Mes	ssage
Browse Embedded	File D:\Photos\101C/	AN Browse Embedded File
ſ		x
Save Retrieve F		Save Embedded File
Password	Successfully Retrieve File	
	ОК	
Retrieve		

Fig. 10: Message Retrieved Successfully

# 4. EMBEDDING FILE/MESSAGE AND RETRIEVING FILE/MESSAGE

# 4.1 Image to Image Embedding and Retrieving

We carry out practical implementation on the described software. Fig. 11 shows a source image file and Fig. 12 shows the target image file. The resulting embedded file is shown in Fig. 13 which looks almost similar to Fig. 11, though it contains hidden file in it. The resulting file size is nearly the addition of size of source file and size of target file. Fig. 14 shows the retrieved image file at the destination.



Fig. 11: Source File with Size 92.7 kb



Fig. 12: Target File with Size 78.6 kb



Fig. 13: Embedded File with Size 171.3 kb



Fig.14: Retrieved Target File with size 78.6kb

4.2 Image to Doc/Text File Embedding and Retrieving

We also carry out implementation for hiding a Microsoft Word document in the same image as Fig. 11. Fig. 15 shows the target document file. The resulting embedded file is shown in Fig. 16 which looks almost similar to Fig. 11, though it contains hidden document file in it. The resulting file size is nearly the addition of size of the source file and size of the target file. Fig. 17 shows the retrieved document file at the destination.

Home Insert	Page Layout Refe	erences Mailing	s Review Vie	w				
Anal Sterior B Z U - 1	- 12 - A'	х' (ூ) ⊟ - 1 2 - <u>А</u> - ) <b>≡ ≡</b>	= · /示/ 律 律   = = [1=   ♪	21 ¶ AaBbi	CCDC AaBbCcDc mai T No Spaci	AaBbCe Heading 1 Heading 2	A A rind - Change Styles - Uz Select -	
ooard 🧐	Font		Paragraph			Styles	G Editing	
	SHRIS'A College Cam B.E.(SEV	D VIDYA pus, Old Nation 'ENTH SEMES I	MANDAL I nal Highway No TER) OF THE A NFORMATION	N S T I T U T 8, BHARUCI ACADEMIC YE -TECHNOLOG	E_Q F T E C H H - 392001 TIM EAR 2009-2010 GY	H N O L O G Y E TABLE FOR BRANCH		
	Time	Monday	Tuesday	Wednesday	Thursday	Friday		
	10:30 to 11:25	SE (PMT)	DBMS (MT)	PROJECT	PROJECT	ISA (C,D)-TUT		
	11:25 to 12:20	ISA (RRS)	OS (N)	DBMS (V)	GUI TUTORIAL (SUJ)	ISA		
	12:20 to 01:15	GUI (GP)	SE (JJP)	OS	OS (RRS)	SE		
	01:15 to 01:45							
	01:45 to 02:40	SE DBMS LAB-2 LAB-3 (C,D) (A,B)	OS ISA Lab-2 (A,B) (C,D)	GUI (S)	DBMS (V)	GUI SE LAB-3 LAB-2 (C.D) (A.B)		
	02:40 to 03:35		200	SE (J) TUTORIAL		440 440		
	03:35 to 03:45							
	03:45 to 04:40	Seminar		DBMS OS LAB-3 LAB-2		Seminar		

Fig. 15: Target File with size 50 kb



Fig. 16: Embedded File with size 142.7 kb

a 7.0 .			Time.docx -	Microsoft Word				5
Home Insert	Page Layout Ref	erences Mailing	Review Vie	w				
Anal Ste J B Z U - I	* 12 * A*	x' (=) (= • ) 2 • Δ • (≡ =	= · · · · · · · · · · · · · · · · · · ·	AaBbo	CCDC AaBbCcDc nal 1 No Spaci	AaBbC AaBbCc Heading 1 Heading 2	Change Le Select	* *
ioard 🧐	Font	14	Paragraph			Styles	G Editing	
	SHRIS'A College Cam B.E-∦SEV	D VIDYA ppus, Old Nation /ENTH SEMES I	MANDAL I nal Highway No TER) OF THE A NFORMATION -	N S T I T U T I 8, BHARUCH CADEMIC YE -TECHNOLOG	E_Q F T E C H 1 - 392001 TIM AR 2009-2010 SY	IN O L O G Y E TABLE FOR BRANCH		
	Time	Monday	Tuesday	Wednesday	Thursday	Friday		
	10:30 to 11:25	SE (PMT)	DBMS (MT)	PROJECT	PROJECT	ISA (C,D)-TUT		
	11:25 to 12:20	ISA (RRS)	OS (N)	DBMS (V)	GUI TUTORIAL (SUJ)	ISA		
	12:20 to 01:15	GUI (GP)	SE (911)	OS	OS (RRS)	SE		
	01:15 to 01:45							
	01:45 to 02:40	SE DBMS LAB-2 LAB-3 (C,D) (A,B)	OS ISA Lab-2 (A,B) (C,D)	GUI (S)	DBMS (V)	GUI SE LAB-3 LAB-2 (C,D) (A,B)		
	02:40 to 03:35	40		SE (J) TUTORIAL		AW AW		
	03:35 to 03:45							
	03:45 to 04:40	Seminar		DBMS OS LAB-3 LAB-2		Seminar		
1						Ala ala ala	100%	

Fig. 17: Retrieved .doc File with Size 50 kb

# 5. APPLICATIONS

- 17. It provides one of the most secured File/Data transfer over Internet/Intranet.
- 18. AFiles can be embedded with the algorithm.
- 19. The password and other details are being encrypted by AES (Advanced Encryption Standard) which is considered as a standard in the encryption in the current digital world.
- 20. Location and password of the project will be sent only to the recipient through SMS which shortlists the possibility of any third party indulging in the file.
- 21. Even if any third party downloads the file directly from FTP, still he requires the password to open it which is only delivered to the recipient by SMS.
- 22. There is no database which keeps the record of the file details and password. Therefore no one can see the hidden information.
- 23. There is no information stored for password on the server so user has to manually request for the password if he has lost or misplaced.
- 24. If the recipient has lost the embedded file there is no way to generate it back rather than requesting the owner to make the steganos file again and upload it again.

# 6. CONCLUSION

As the world is going digital and information is transferred in the digital form, it is imperative to increase security to avoid any kind of loss or modification in the digital information by a adversaries. We developed algorithm that can prove its usefulness in enterprise level security. We successfully implemented the new steganographic algorithm that can hide a file or a message into a file and can be securely sent to the recipient.

# 7. REFERENCES

- [1] József Lenti,"Steganographic Methods", Periodica Polytechnica Ser. El. Eng. Vol. 44, No. 3-4, pp. 249–258, 2000.
- [2] M. Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza, "Steganography in Persian and Arabic Unicode Texts using Pseudo-Space and Pseudo Connection Characters", Journal of Theoretical and Applied Information Technology, pp. 682-687.
- [3] Bryan Clair, "Steganography: How to Send a Secret Message", 2001. http://www.strangehorizons.com /2001/20011008/steganography.shtml
- [4] Shen Wang, Bian Yang and Xiamu Niu, "A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing, Vol. 1, No. 1, pp. 28-35, 2010.
- [5] Adnan Abdul-Aziz Gutub, and Manal Mohammad Fattani, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", World Academy of Science, Engineering and Technology, pp.28-31, 2007.
- [6] Faird, Hany. "Detecting Steganographic Messages in Digital Images", 2000.
- [7] Shawn D. Dickman, "An Overview of Steganography", 2007.
- [8] Amanpreet Kaur, Renu Dhir and Geeta Sikka, "A New Image Steganography Based On First Component Alteration Technique", International Journal of Computer Science and Information Security, Vol.6, No.3, pp. 53-56, 2009.