ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.7

Information Security through Steganography

Govindraj Chittapur[1], Pooja Kolhar[2]
Assistant Professor[1], Student[2]
Department Of MCA
Basaveshwar Engineering College Bagalkot, India

Abstract:
Information is an essential resource for any individual or association and must be shielded from gatecrashers or programmers. The need to conceal information from programmers has existed since antiquated circumstances, and these days, there are advancements in computerized media, for example, sound, video, pictures, et cetera. To anchor mystery data, diverse media techniques are utilized and steganography is one. Steganography shrouds the information under other information with no differentiable changes. Numerous individual steganography tools can be utilized to exchange information safely and, in this paper, another apparatus is suggested that reductions time and exertion. Utilizing this device, we hide the content in sound, text, pictures in a single place, so there was no need access to multiple tools.

I. Introduction

System Architecture for Proposed System

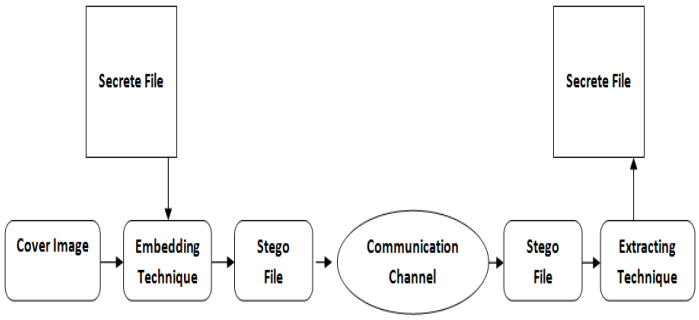


FIGURE 1: SYSTEM ARCHITECTURE FOR "INFORMATION SECURITY THROUGH STEGANOGRAPHY".

Following are the terms used in the steganography system.
Secret File: It's a media which is embedded inside a cover file to hide its existence to the unauthorized users.
Cover File: Cover file is a medium which covers the important data and is encrypted in such a way that it cannot be able to identify easily.
Stego File: Stego File is generated by inserting the secret file into the cover file. After the process of encryption, stego file is available.

The Figure.1 delineates the general steganography framework. A cover file is utilized to convey the secret information. In this cover file, a secret information is implanted utilizing an inserting strategy with a specific end goal to keep up the security of the essential information. The installing procedure is generally called as Data Encryption Process.

After the encryption procedure, a record is produced, that document is called as the Stego File. Stego document is a record which contains the cover record and in addition the mystery information. It is called as stego document in light of the fact that the record is produced by applying the steganography procedure. The created stego record is currently prepared to send to the approved individual.

II. Literature Survey

Steganography is the wide area where research and improvement process is growing vastly. There are various steganography techniques which are proposed to provide the security to the information, here some of the authors mentioned with their algorithms, Xia shuangKui and Jianbin Wu [1] A modification free steganography method based on Image Information Entropy, Saikat Mondal, Rameswar Debnath, Barun Kumar [2] Has proposed Self An improved color image steganography technique in spatial domain, Tapodhir Acharjee, Ashish Konwar [3] XORSTEG: A new model of text steganography, Marwa M Emam, Abdelmgeid Aly, and Fatma A Omara [4] proposed A Modified Image Steganography Method based on LSB Technique, Navneet Kaur, Sunny Behal [5] proposed A Survey on various types of Steganography and Analysis of Hiding Techniques, Prajna Vasudev,Kumar Saurabh [6] proposed Video steganography using 32*32 quantization on DCT, Rongyue, Sachdev, Botnan, K. Hyoung Joong, and H. Jun [7] proposed An Efficient Embedder for BCH Coding for Steganography, Hao, L.Y. Zhao, and W.D. Zhong [8] proposed A novel steganography algorithm based on the motion vector and matrix encoding, Feng, Y. Xiao-Yuan, and G. Yao [9] proposed Video steganography using motion vector and linear block codes, Jafar Mansouri,Morteza Khademi [10] proposed An adaptive scheme for compressed video steganography.

III. Design Issues for "Information Security Through Steganography"

Here the secret data or secret information is embedded in a cover file in order to hide the existence of secret data and encrypted in such a manner that only intended person can retrieve the secret data. The encrypted data is called as stego file, which is used as input to decrypt the secret data by the intended person.

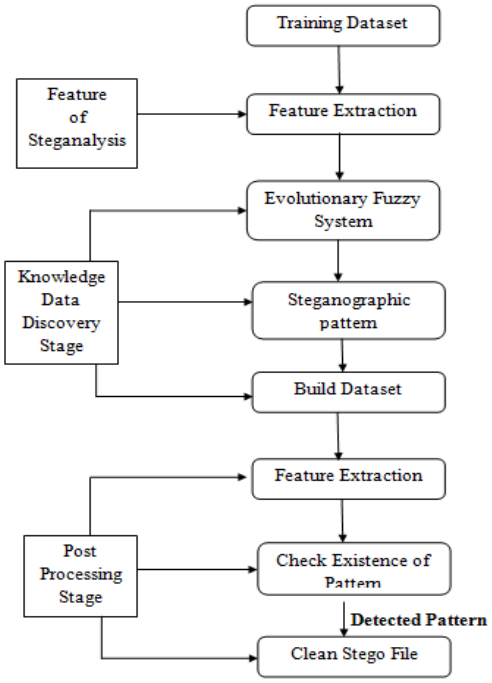


FIGURE 2: DESIGN ARCHITECTURE FOR "INFORMATION SECURITY THROUGH STEGANOGRAPHY".

The Figure 5.2 represents the Architecture design of "Information Security Through Steganography" , It consists data preprocessing , Knowledge data discovery and post processing stages. In first phase from training dataset features are extracted this process termed Steganalysis feature. In KDD method from the fuzzy evolutionary structure, meticulous stego pattern is identified. based on specific generated sample a dataset is built and utilized for implementation of project. Post-Processing segment rechecks the correctness, applied dataset is evaluated and its attributes are extricated, and verified for pattern existence, if it is prevailed clean stego file is ready.

IV. IMPLEMENTATION OF "INFORMATION SECURITY THROUGH STEGANOGRAPHY"

An Ideology for Information Security Through Steganography is a proposed solution where security is provided to the data which is sensitive and only accessible to the intended person without dragging the attention of un authorized persons and it can be performed with Text, Image and Audio in a single platform. In the existing system there is no single platform to perform the Text, Audio and Image steganography, particular steganography tools are used to provide the security. The proposed solution consist several stages like Alteration, Modification, Verification and Reconstruction of Sample to generate the proper input for steganography process.

First there will be registration and login process, user have to perform registration process by providing some personal details and get his/her username and password. Through username and password he/she can be able to access the system. After the authentication stage, user can choose the type of steganography technique he wants to perform such as text steganography, image steganography or image steganography. Now user can choose the cover file and secret file and encrypt to hide the existence of secret information.

Now moving to registration step, in this step the user has to provide the Name, Email id, Contact No, Password and confirm Password and basic validation is done to these fields such as Name cannot be empty, Email id cannot be empty , Contact no cannot be empty then password and confirm password cannot be empty and other validations such as pattern matching for email, Contact No and password and confirm password both should be same are done. validation errors should be displayed if any occurs, if validation is successful then the user is registered to the system.

After the registration step, the next module is login. In this module user needs to submit valid username and password to login to the system. Here also the basic validation is done such as username cannot be empty and password cannot be empty. After the basic validation performed the system checks list of username and if the given username is exist then it will proceed otherwise validation error will be displayed. Next it will check for the valid password for the given username, if it matches it will redirect to the next page else incorrect password error will be displayed. After the successful login process the system provides the other functionalities to the user.

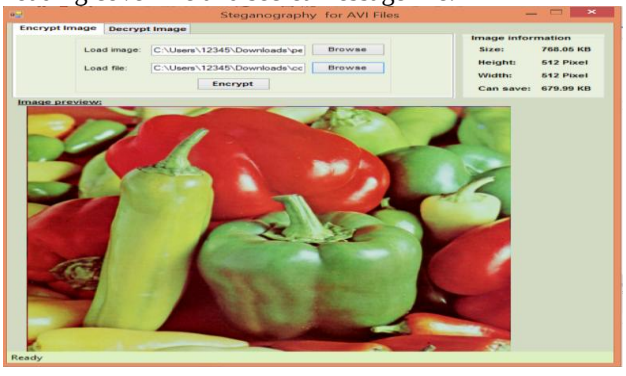
After the successful completion of authentication process, now user can choose text steganography, image steganography or audio steganography to perform the data encryption. After selection, user has to load the cover file and secret message file, if secret message file is large it will display the error as file size is too large, now user has to press the Encrypt button and generate the stego file and displays the message as Encrypted successfully.

After the successful encryption process, stego file is generated and is ready to send it to the intended person, it can be sent via email which is given by the user at the time of registration. After receiving the stego file, receiver need to decrypt that file in order to retrieve the secret message. Now the receiver has to load the stego file as input and should provide the path to save the secret message, it can be a file or new folder. Later user has to press the button decrypt, decryption process is carried out. After the completion of decryption, message will be displayed as successful decryption and file is saved.

V RESULT AND DISCUSSION

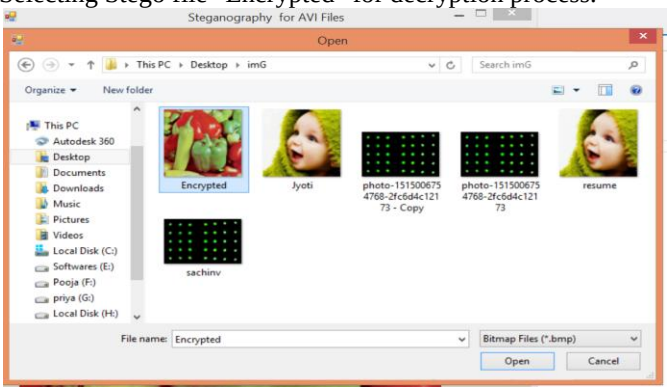
The following screenshots are usefull to understand the interface and the method of the process.The tables contain the Image dataset and audio dataset used during the process. another tablecontains the result after encryption and decryption process and the screenshots helps to understand the flow of the system.

Loading cover file and secret message file.



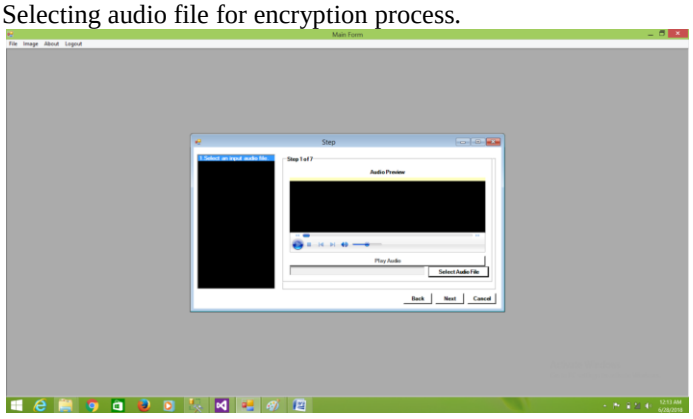
After Encryption message displayed as Encrypted message has been successfully saved.

Selecting Stego file "Encrypted" for decryption process.

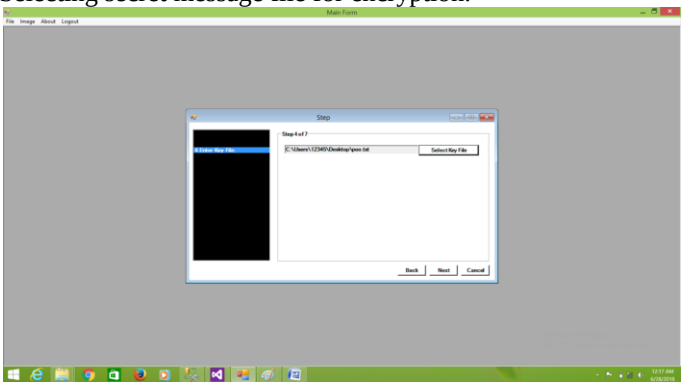


Loading stego file and providing path to save the secret file and decrypting stego file.

Selecting audio file for encryption process.



Selecting secret message file for encryption.



Extraction of secret message from audio file.

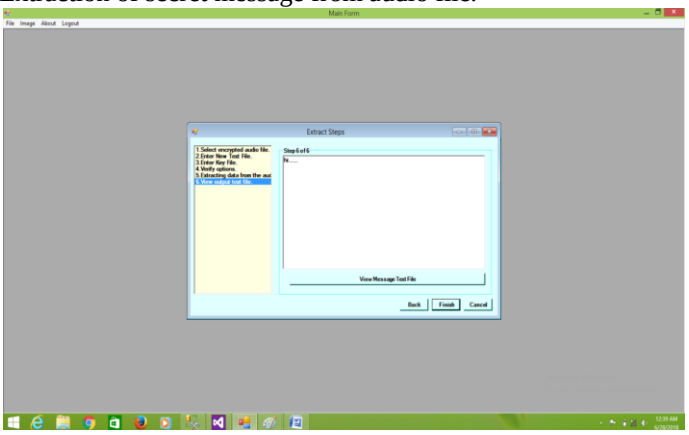


TABLE I. IMAGE DATA SET USED IN "INFORMATION SECURITY THROUGH STEGANOGRAPHY"

SI. No	File Name	File Type	File Size	Dimension	Resolution	Bit Depth
1	Image_00001	.jpg	47.9 Kb	591*500 Pixel	96*96 dpi	24
2	Image_00018	.jpg	67.3 Kb	751*500 Pixel	96*96 dpi	24
3	Image_00003	.jpg	56.4 Kb	500*667 Pixel	96*96 dpi	24
4	Lena	.bmp	768 Kb	512*512 Pixel	72*72 dpi	24
5	Kodim24	.png	689 Kb	768*512 Pixel	96*96 dpi	24
6	Peppers	.bmp	768 Kb	512*512 Pixel	96*96 dpi	24
7	Renoir4-512	.bmp	588 Kb	512*392 Pixel	96*96 dpi	24
8	First-day-of-spring	.gif	136 Kb	546*215 Pixel	96*96 dpi	8
9	Kodim15	.png	598 Kb	768*512 Pixel	96*96 dpi	24
10	Roses	.jpg	349 Kb	2024*1724 Pixel	72*72 dpi	24
11	Vase512	.bmp	967 Kb	512*645 Pixel	96*96 dpi	24
12	Baboon	.jpg	11.5 Kb	225*225 Pixel	96*96 dpi	24
13	Image_00014	.jpg	107Kb	500*500Pixel	96*96 dpi	24
14	Image_00099	.jpg	64.2Kb	670*500 Pixel	96*96 dpi	24
15	Image_00330	.jpg	40.4 Kb	500*564 Pixel	72*72 dpi	24
16	Image_00856	.jpg	30.1 Kb	667*500 Pixel	96*96 dpi	24
17	Image_00954	.jpg	39.7 Kb	752*500 Pixel	96*96 dpi	24
18	Image_01124	.jpg	39.7 Kb	667*500 Pixel	72*72 dpi	24
19	Image_03946	.jpg	41.8Kb	667*500 Pixel	96*96 dpi	24
20	Image_03951	.jpg	44.5 Kb	725*500 Pixel	72*72 dpi	24

TABLE II. AUDIO DATA SET USED IN "INFORMATION SECURITY THROUGH STEGANOGRAPHY"

Sl.No	Name	File Type	Size	Length	Bit Rate
1	Atmospace_jungle	.wav	918 Kb	00:00:05	1411 Kbps
2	Board	.wav	94.6 Kb	00:00:01	705 Kbps
3	Film	.wav	94.6 Kb	00:00:01	705 Kbps
4	Industry_mad	.wav	8.10 Kb	00:01:36	705 Kbps
5	King_pin	.wav	459 Kb	00:00:02	705 Kbps
6	Sa1	.wav	297 Kb	00:00:04	512 Kbps
7	Si649	.wav	540 Kb	00:00:08	512 Kbps
8	Song	.wav	94.6 Kb	00:00:01	705 Kbps
9	Upward_jungle	.wav	459 Kb	00:00:02	1411 Kbps
10	Notify	.wav	94.6 Kb	00:00:01	705 Kbps

TABLE III. DATASET FILE SIZE BEFORE ENCRYPTION AND AFTER ENCRYPTION.

Sl.No	Cover File	Cover File Size	Resolution	Secret Message File	Cover File Size after Encryption
1	Lena.jpg	768.05 KB	512*512 Pixel	Cover.docx	784.93 KB
2	Vase512.jpg	967.55 KB	645*512 Pixel	gk.docx	847.59 KB
3	renoir4.jpg	588.05 KB	392*512 Pixel	First-day-of-spring.gif	590.61 KB
4	Hide.bmp	2605.52 KB	667*1000 Pixel	Extract.jpg	590.61 KB
5	Kodim23.jpg	544.52 KB	512*768 Pixel	lab_output.docx	1216.88 KB
6	Roses.jpg	349.10 KB	1724*2024 Pixel	Pepper.bmp	9652.52 KB
7	Baboon.jpg	11.59 KB	225*225 Pixel	Doc_intro.doc	146.54 KB
8	Kodim15.jpg	598.22KB	512*768 Pixel	Li-Fi.Pdf	1023.99KB
9	Image_0001.bmp	47.90KB	500*591 Pixel	Image_01441.jpg	769.52 KB
10	Image_03163.jpg	32.88KB	500*570 Pixel	Gull.wav	742.17KB
11	Industry_mad.wav	8304MB	-	Outputfiletest.wav	662KB
12	003-003-Trone.wav	8304 KB	-	Output.txt	8 Bytes

ACKNOWLEDGMENTS

I would like to acknowledge my sincere thanks to Basaveshwar Engineering College Department of MCA for giving support, resources for doing this research paper.

REFERENCES

[1] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Volume 2, No. 4, April 2011 Journal of Global Research in Computer Science.

[2] C.S. Lu," Multimedia security: steganography and digital watermarking techniques for protection of intellectual property" Artech House, Inc (2003).

[3] H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes," in Image and Signal Processing (CISP), 2011 4th International Congress on, 2011, pp. 1784-1787.

[4] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "An Adaptive Matrix Embedding for Image Steganography," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 642-646.

BIOGRAPHIES

Prof. GOVINDRAJ CHITTAPUR received the B.Sc. degree in Computer Science from the University of KUD, Dharwad, Karnataka, in 2002, the M.C.A degree from VTU, Belgaum, Karnataka, in 2005 and awarded M.sc Technology by Research from Mysore University in 2011. Has published 17 international journal and national journal has also served as Reviewer and Editorial Board Member of various international journal and conferences. His major research area includes Image and Video forensics, Machine learning and Data Mining.

Miss. POOJA KOLHAR received the BCA degree from the Karnataka University Dharwad, Dharwad, Karnataka, in 2015, and pursuing MCA degree under VTU, Belgaum, Karnataka.