Research Journal of Applied Sciences, Engineering and Technology 4(24): 5410-5415, 2012
ISSN: 2040-7467

Submitted: March 18, 2012 Accepted: April 23, 2012 Published: December 15, 2012

Secure Image Steganography

C. Bharathi, A. Divya Bhagya, N.R. Lakshmi and J. Kalai Selvi
Department of Information Technology, University Departments of Anna University of Technology, Jothipuram, Coimbatore -641047, Tamilnadu, India

Abstract: The aim of this study is to study the requirements of hiding information digitally while maintaining the integrity of hidden information. So that the stego of object remains unchanged or almost unchange the human eyes. If stego object changes significantly a third party may see that information is being hidden and therefore could attempt to extract or destroy it. Steganography is used to convert historical documents into 1 and 0's that is digital format. This digital conversion gives more advantages for document preparation, maintenance, storage etc and reduces complexity as well as space occupied by the historical documents. In addition to this, it supports the point of digital data recoding based on system design. In this digital data processing, like analysis, filter, conversions, reproduction and rematch the number of times synchronizing the digital data with a help of stream action. These are all processed with the help of the digital to analog conversions. These above processes are taking place with the help of some standard as well as non standard interfacing of processors with an order of protocols. With a help of above techniques the captured data is studied, regurgitated, number of times played back with synched data stream. It has been developed for the purpose of making several security-based transactions. The confidential or important information, which if sent in normal format, may be misused. This can be avoided by making use of this system. The mechanism, which is used to hide the digital file in the image files, is known as Steganography.

Keywords: Digital format, image files, security, steganography, transaction

INTRODUCTION

Secure Image Steganography is an approach through which most secured documents, like paper documents, historical documents are all converted into digital format. It is called an electronic image or digital image and it can be easily viewed in a system. Compared to historical method of document protection (Petitcolas, 2011), this digital document have the following advantages like avoiding paper works, easy to send as well as receive. Multiple copies are easily and quickly generated, storage area and maintenance are also simple. In this digital image not only documents but also manuals, catalogues, brochures, banners can be included. As a final face of this conversion helps for data processing with digital data processing and digital image processing, like analyzes, filter, conversions, reproduction and rematch the number of times synchronizing the digital data with a help of stream action. These are all processed with the help of digital to analog conversions (Ramachandran, 2003). These above process are taking place with a help of some standard as well as non standard interfacing of processors with an order of protocols. With the help of above techniques the captured data is studied, regurgitated, number of times played back with synched data stream, it has been developed for the purpose of making several security-based transactions (Artz, 2001). The confidential or important information, which sent with normal format, there might, may be a chance of happening misuse cases. This can be avoided by making use of this system. The mechanism, which is used to hide the digital file in the image files, is known as Steganography (Trithemius, 1621).

Objective: This project has the following objectives while design the tool. The tool should support various platform, easy to use like GUI mode, should hide a 24 bit color image inside and should have effective hide a message in the form of image degradation and original image should be retrieved while reprocessing it (Hrytskiv *et al*., 1998). Not only that but also effectiveness of the hiding as well as Secret Key Steganography approach [also should be supported.

Scope: There is a wide scope for future development of the software. The world of computer fields is not static it is always subject to change. The technology which is famous today will become outdated very next day. To

Corresponding Author: C. Bharathi, Department of Information Technology, University Departments of Anna University of Technology, Jothipuram, Coimbatore -641047, Tamilnadu, India

keep abstract of technical improvements, the system may be refinement. So it is not concluded. Yet it will improve with further enhancements. It is essential to change the software when new software arrives with more advanced feathers. So it is much necessary for further development. Further enhancements can be done in an efficient manner with disruption to the system.

LITERATURE SURVEY

Existing system: The data hiding behind an image is the general goal of this steganography. The current techniques can provide reasonable security for the hidden message, but often leave marks that suggest the cover has been tampered with. Most of these marks are caused by the message being embedded into the cover without any regard to the cover's original content (Richard, 1997). Therefore, it is likely that if the original content was taken into account it would become significantly more difficult to discover whether steganography has been used.

Proposed system: This project will be an investigation into the effectiveness of taking into account the original content of the cover and will result in a cross platform tool that can evaluate the effectiveness of its hiding mechanism. The tool will work on colour images and should be able to hide a message of any type inside the image. The security of stego-images depends entirely on their ability to go unnoticed, so being able to evaluate characteristics of an image using water marking detection is a clear advantage.

Module description: It Contains following Modules, Convert into digital format:

- Hide File
- Extract File

Convert into digital format: Digital documentation is in the form of binary, which has more advantages hence all historical documents are converted into digital format and is easily viewed in a system.

Hide file: This module is used to hide picture in data file. It has the following process like, image location, save file location, encryption key is provided by the user to hide picture file in the saved data file location.

Image location: The image file exists in the system is used by the user to open the file from the open dialogue box.

Save location: This is also image file that is generated by the user. User has to save this new file in any location according to their wish, this file is used to embed the picture file in the data file.

Encryption key: This key is the public key and is confidential key between sender and receiver. This is also embedding the picture file with data file.

Validation key: This is actual file size of the image location in bytes. The picture file is added to the saved image location after this last byte.

Fig. 1: Login screen

Fig. 2: Main screen

Fig. 3: Digital convertion

Hide: It is used to hide the data file into saved picture file. Picture file encrypted is unknown format and then embed in the saved data file.

Send: The user to another user uses this button to send the saved image file, which contains the picture hidden.

View file: This module is used to display the picture files that can be embed with the data file. Forms, file name, validation code are displayed in the list. The receiver can download the selected file by right clicking the list view box. The downloaded file is stored in c:\download folder in the client machine from server.

Fig. 4: Encrypted file

Fig. 5: Hiding the data

Extract file: This module is used to extract files.

Image location: Downloaded images by the user are given as the input in this text box.

Encryption key: The key used to extract the file is the secret key. Receiver should know this key to retrieve message.

Fig. 6: Extraction of the file

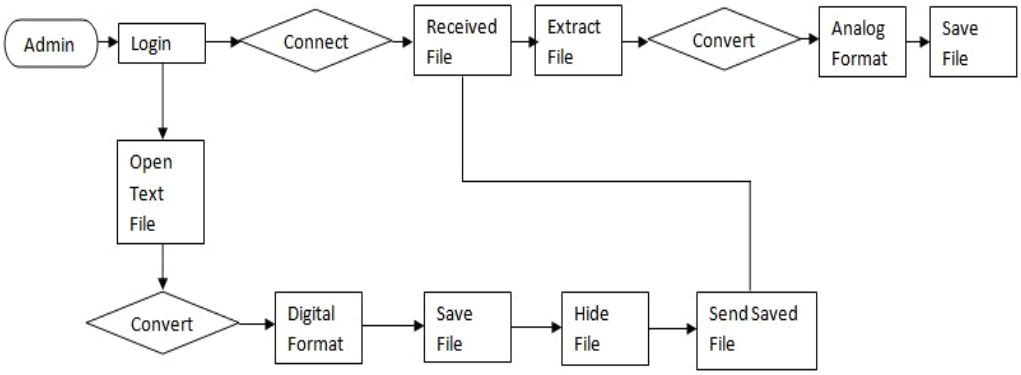

Fig. 7: System flow diagram

Validation code: This is the offset of the file where actually the picture file is resided.

Extract file: When receiver clicks this button the picture file is shown to the receiver. Encrypted files are decrypted and then shown in the text box.

DESIGN DIAGRAM

Snapshots:

Details about snapshot: Figure 1 depicts the login form where user name and password authentication is done. Figure 2 shows the home screen obtained upon successful verification. Figure 3 corresponds to the module-Convert into digital format. Figure 4 is the extension of this module where the encrypted file is stored on to a different location, whereas Fig. 5 and 6 represents hiding and extraction of file respectively. Figure 7 shows th diagram of system flow.

CONCLUSION

The "Secure Image Steganography" has been developed to satisfy all proposed requirements. The system is highly scalable and user friendly. Almost all the system objectives have been met. The system has been tested under all criteria. The system minimizes the problem arising in the existing manual system and it

eliminates the human errors to zero level. Figure 7 shows diagram of system flow.

The software executes successfully by fulfilling the objectives of the project. Further extensions to this system can be made required with minor modifications. The excogitation can be used digital electronic circuitry, or designed as hardware in VLSI, firmware, soft core as System on Chip into FPGA. As a result of fact, by using some technology it can convert into machine-readable format. While designing as a processor, which can execute the instructions to perform functions with a help of input parameters and related output can be generated.

REFERENCES

Artz, D., 2001. Digital Steganography: Hiding Data within Data. IEEE Internet Comput., 5(3): 75-80.

Hrytskiv, Z., S. Voloshynovskiy and Y. Rytsar, 1998. Cryptography of video information in modern communications. Electr. Energet., 11: 115-125.

Petitcolas, F.A.P., 2011. History of Steganography and Cryptography. Retrieved from: www.cl.cam.ac.uk/~fapp2/steganography/history.html, (Accessed on: 07 January, 2011).

Ramachandran, S., 2003. Computer Aided Design. 3rd Edn., Air Walk Publication.

Richard, F., 1997. Software Engineering Concepts. 2nd Edn., Tata Mc Graw Hill Publication.

Trithemius, J., 1621. Steganographia this is the Art of Secret Writing of his Mind will be opened in the Absence of Certain. Retrieved from: www.esotericarchives.com /tritheim/stegano.htm.