Data Minder using Steganography : Technology of Data Encryption

[1]Bhushan Walke, [2] Riddhi Naik, [3] Dhara Desai

[1]Computer Engineering, GHRCEM, Pune University
Pune. Maharashtra, INDIA

[2, 3] Computer Engineering, CGPIT, Uka Tarsadia University,
Bardoli, surat. Gujarat, INDIA

Abstract - The internet and the World Wide Web have revolutionized the way in which digital data is distributed. The growing possibilities of modern communication need special means of security especially on computer network. In this paper a new randomized secure data hiding algorithm using file hybridization is proposed for strengthening the security of information through a combination of cryptography and steganography with random transformation and file hybridization. Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganlysis is process to detect of presence of steganography. Steganography hides the message so it cannot be seen. A message is a cipher text for instance, might arouse suspicious on the part of the recipient while an "invisible" message created with steganography. This approach includes a high degree of security and data protection implemented by the concept "Message Sending" and "Secrete Communication" at large scale. This System includes three main parts Administrator, Encryption and Decryption. The Administrator creates the monitor accounts. Encryption uses the service of the system & authenticates the user. Decryption is used to decrypt data.

Keywords- *Datahiding, Steganography, Unique ID , Pattern Detection*

1. Introduction

In our proposed system we are using an efficient carrier media, digital image for steganography. The basic unit of the composition of an image is called pixel. The size of an image can be given in pixels. Pixels are indexed by x and y coordinates with x and y having integer values. Each pixel is generally stored as 24 bit or 8 bit. A 24- bit image are spread over three bytes and each bytes represents red, green, and blue Colors are obtained by mixing red, green, and blue light in different proportions. In our proposed system we are combining cryptography and steganography mechanisms with random transformation, to have better security. Random transformation makes the tasks of steganolysis difficult. And the unique ID provided to each file while Encryption makes it difficult to the analyzer to infer where in the image actually contains the secret message.

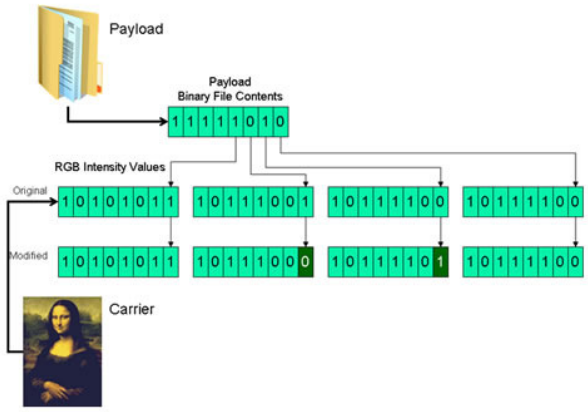

Fig.1 Basic Steganography

2. Objectives

The primary objective of data minder is to provide a highly secure environment to the data the user would provide. This security will include not just the encryption of the sensitive data, but also to provide a valid authentication process while decryption to see if the user is authorized to decrypt the data. Flexibility to the user to provide portability of the encrypted data file and decryption process made easy by access to the system irrespective of the location of the user or the system.

3. Existing System

There is a system available for encryption of the data using steganography, but it encrypts the data into the image serially and if random encryption is used it does not provide any type of authentication during decryption. Due to this reasons the existing system does not provide adequate level of secuity and confirmation that the data will be decrypted by the authenticated user only. Also by several means the data can be sniffed and manipulated over the network while transmission. Another system works in a way by providing a user generated password which will be required during decryption. This is a painstaking process for the user to remember the passwords.

4. Proposed System

The system targets the secure data transfer requirements of a user. Using the basic principles of steganography, the random pixel steganographic algorithm, and the unique key combination we promise to secure the data more efficiently. The user has to provide the system with the image file and the data that he has to hide. The system accepts these parameters and processes the image file with the developed algorithm and secures the data by generating a unique key and embedding it to the image. This key will be hidden from the users too. Another copy of this key will be stored into the database which will be used for further decryption. This key will be mapped to the respective user only. Further while decrypting the data user have to just provide the file to the system, which will then be authenticated if the file is authorized to decrypt the file or not, if true the data will be decrypted using the algorithm and the data will be provided to the user without and manipulation and loss of the original content. Another major advantage provided by us is using steganography while communication between the user and the system. All the communication that will be taking place between the system and the user will be totally secured, eliminating the threats of data sniffing over the network.

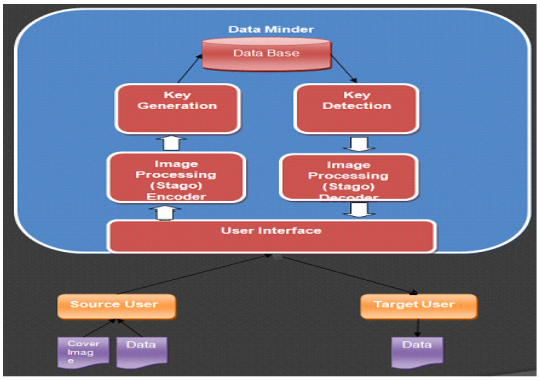

Fig.2 Product Perspective

5. Applications of Steganography

- Communication and secret data storing.
- Protection of data alteration.
- Access control system for digital content distribution.
- Media Database systems.
- The knowledge of the technology is still limited to mainly the research individuals and academia. In future, we would extend the system to be more robust and efficient. The research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. We will also reduce the chances of corruption, inconvenience and bureaucratic delays. Analysis the processing time to generate the random number and introduce method to minimize the time.
- Industries like music, film, publishing and organization like ministry and military will definitely be highly benefited by the use of such techniques.

6. Risks in Implementation of Steganography

- We cannot Steganograph a file which is larger in size. The data and the file cannot be too large as that would take much time for encryption as well as decryption. A subsequent large file can be broken up into small files and then processed. But data with Gigs of bytes will be an overhead.
- Due to bandwidth limitations, restrictions come on the file size that we are going to upload and download.

.

7. Characteristics

7.1 Administrator

- Create, and monitor accounts of authorities.
- The created user should be assigned with a Primary Unique-ID.
- Authorize the user to perform various operations as provided by the system.
- Should properly handle Encryption and Decryption phases.
- For every individual encrypted file a encryption stegnographed pattern should be assigned, which further will be used to Decrypt the data.

7.2 Encryption

- Users should be able to create new account, log-in to their existing accounts which will give them the authority to use the services provided by the system.
- Authenticated users should be able to encrypt the important and essential data.
- While encryption phase user should provide a Carrier image and the data that is to be encrypted.
- User will be able to then download the stegnographed file, and will be able to carry it. User can share the encrypted file with other users of their choice by selecting the users from the list or just by providing the user name.

7.3 Decryption

- Users can log-in to their accounts as created by administrator.
- Authenticated users should be able to decrypt the important essential data.
- Upload the encrypted file for further decryption.

8. Methodology

Firstly user need to login into the system if not existing user, then register for a new user. This is essential step because a Unique-Id will be assigned to every user which is a primary factor of encryption and decryption process of our system. Even while this communication we use steganography. The client application has a default image with it, this image is used to store the user credentials using steganography and then send over the network to the server system. Here the file is then decrypted and the data is validated.

8.1 Encryption Side

- After the user is authenticated he will now be able to access the services of the application of encryption or decryption. The user can as well share a encrypted file to another user.
- For encryption the user now has to provide the system with a image file and the data that he has to hide. This image is called the cover image.
- The system accepts the file and the data. Then the system embeds the data into the image file using the image bits i.e. using the basic principle of steganography, here the system modifies the embedding process by storing the data into image bits but not into contiguous order. A random pattern of the image's pixel bit selection is done by the system to store the data. This pattern will only be known to the system. The user will be unaware of this random pattern.
- After the data is being stored into the image file, the system them embeds the users Unique-Id into the image file with the same process as the data is stored. If the user selects to share the encrypted file with other user the system embeds the Unique-Id of the other user as well.
- A file Id is generated by the system and is then stored into the database which is mapped to the respective user who created the encrypted file and also if there is any file sharing User-Id.
- If the data size exceeds the image size, the system breaks the data and then stores the data into multiple image files, and all the files are then compressed into a single file.
- Finally the system then allows the user to download the encrypted file and can be carried by the user into portable media.

8.2 Decoding Side

- User needs to be logged in to the system, this is essential as the users parameters will be checked for authorization.
- When the user wants its data back then user needs to upload the encrypted file.
- Here the system will check the Unique-Id embedded into the file with the Unique-Id that is mapped to the file id from the database.
- If the credentials are authorized then and then only the data is decrypted and the original data is provided to the user without any distortion and manipulation.
- While decryption the system detects the pattern of data storage into the image pixels and the decrypts the file.
- If the encrypted file consists of number of files which are compressed, then the system decompresses the compressed file and then arranges the image files sequentially and then decrypts the file one by.
- Finally the decrypted data is arranged sequentially and then the original file is created and provided to the user.

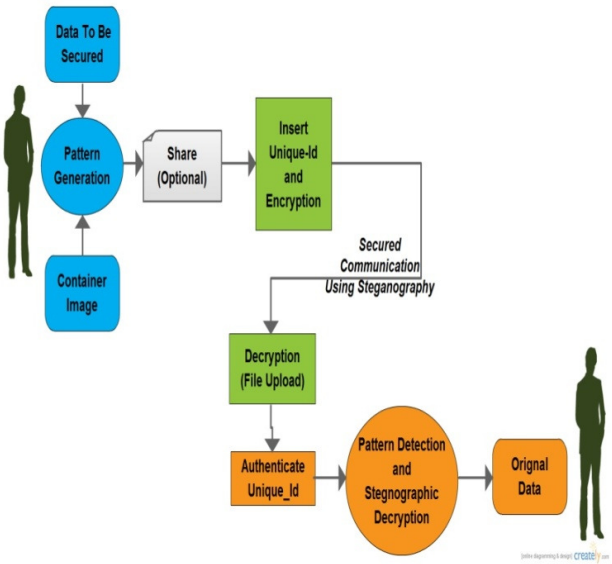

Fig.3 Method

8.3 Project Role

- At first the data to be hidden and a file through which it is to be send are encoded using software.
- The secret data is embedded by random pixel pattern and a unique key generated by the system for the particular user.
- When the system receives the data it decrypt's the data by the use of unique key which is only known to the system itself.
- The Hiding of the data in a coloured image with better security.
- Image containing encrypted data can be transmitted to anybody any where across the world in a complete secured form.
- Combination of both Steganography and cryptography can provide us a double layer of protection.
- Secure Communication.
- Digital Signature Authentication.
- Digital linkage Storage.
- Strong security schema
- Scalable, speedy & high level of accuracy is document is intended for users of particular group and community and will be helpful to users to fulfil their requirement, complaints, suggestion and needs.
- This project help to Municipal authority to manage all the works effectively which users will desire.

9. Existing vs Proposed

Table 1: Comparison between existing and proposed system

S.N.	EXISTING	*Proposed*
1.	Mostly data stored in consequent pixel bits of the cover image.	Data stored in random pixel bits of the cover image.
2.	If at all random pixels used data can be decrypted by any unauthorized user by the using same application.	Only authorized personals by using his Unique-ID can upload the particular encrypted file and decrypt the data.
3.	High risk of data loss or data sniffing while communication over the network.	Use of seteganography while communicating with the server over the network, eliminating the risk of sniffing and data loss.
4.	Restriction of file size of the data as compared to the cover image, data size should be smaller than the cover image.	Large data can be encrypted irrespective of the cover image. As data file will be sub-divided into parts to fit into the cover image forming multiple parts of the encrypted data and then compressing all into one single file.
5.	Encrypted data cannot be shared by the user, if he wants to share with his workgroup or community.	User can very well share his encrypted data with and only with a desired user or the workgroup he wants to share, without worrying about the security.
6.	Cannot manage his files and data that were previously encrypted by the particular user.	User can easily manage, modify and access the data that he has previously used or encrypted.

10. Conclusion

Our goal in this paper is to propose a new steganography mechanism that allows the hiding and communication of a data in a colored image with better security, also eliminating the restriction of six to some extent. The suitability of steganography as a tool to conceal highly sensitive information has been discussed by using a new methodology sharing the concept of hybridization and a multilevel of security of data is achieved.

References

[1] A Randomized Secure Data Hiding Algorithm Using File Hybridization for Information Security.
[2] European Journal of Scientific Research ISSN 1450-216X Vol.40 No.2 (2010), pp.223-231 © EuroJournals Publishing, Inc. 2010 http://www.eurojournals.com/ejsr.htm.
[3] Public–Key Steganography Based on Matching Method.
[4] Exploring Steganography: Seeing the Unseen.
[5] Neil F. Johnson Sushil Jajodia George Mason University.
[6] Modern Steganography.
[7] Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Karlovo n´am_est´_ 13, 121 35 Prague 2, Czech Republic dobsicm@fel.cvut.cz
[8] UNCHS, 2001.

Bhushan Walke perceived and completed B.E. in Computer Engineering in 2012 from G.H. Raisoni college of Engineering and Management under Pune University. Research interest includes Computer Networks, Network Security, Data Communication, wireless Networking.

Riddhi Naik perceived and completed B.E. in Computer Engineering in 2012 from G.H. Raisoni college of Engineering and Management under Pune University. Research interest includes Computer Networks, Wireless Networking. Currently pursing M.Tech in Computer Science from CGPIT, Uka Tarsadia University, Surat. Published a paper named Touch and Dine a multi-touchable restaurant system in UACEE international journal of computer science and its applications volume 2 issue1.

Dhara Desai perceived and completed B.E. in Computer Engineering in 2012 from G.H. Raisoni college of Engineering and Technology under Pune University. Research interest includes Computer Networks, Wireless Networking. Currently Pursing M.Tech in Computer Science from CGPIT, Uka Tarsadia University, Surat.