www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 3 March 2017, Page No. 20417-20426
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i3.02

Stega Image a Technique to Hide Data within Image File, Using Image Steganography and Encryption

Abdullah Hamid
Student of computer science and engineering
Abacus Institute of Engineering and Management
(Maulana Abul Kalam Azad University Of Technology)
E-Mail: Abdullahhamid7@Gmail.Com

1. ABSTRACT

We propose new algorithm to hide data inside image using Steganography and Encryption. The proposed algorithm uses binary codes and pixels inside an image. The file is converted to binary codes to maximize the storage of data inside the image. By applying the proposed algorithm, a system called STEGA IMAGE is developed. The system is then tested to see the viability of the proposed algorithm. Various sizes of data are stored inside the image, Depends upon the pixels of the Carrier Image.

2. INTRODUCTION

This paper proposes new algorithm to hide the data inside images using Steganography and Encryption. This paper contains two algorithm of hide data inside image. First algorithm Hide only text information while Second Algorithm Hide all type of files within Image File. So, we termed first algorithm as **Text Information Algorithm** and second algorithm as **Information File Algorithm**.

Text Information Algorithm is designed to hide all the data inputted (or extracted from a text file) within the image to protect the privacy of the data. The system is developed in Text Information Tab based on the Text Information algorithm. This proposed system provides an image platform for user to input image, calculate the limit of data possible to hide, and a text box to insert texts. Here Encryption of information works as dual layer of security which is extended by password. Once the proposed algorithm is adapted, user can send the Stega image to other computer user so that the receiver is able to retrieve and read the data which is hidden in the Stega image by using the same proposed system. Thus, the data can be protected without revealing the contents to other people.

Information File Algorithm is designed to hide all type file within the image to protect the privacy of the data. The system is developed in Information File Tab based on the Information File algorithm. This proposed system provides an image platform for user to input image, Read pixel Height, pixel width and Size of Image, Calculate the limit of file size possible to hide, and a text box to browse file. Once the proposed algorithm is adapted, user can send the Stega image to other computer user so that the receiver is able to retrieve and read the data which is hidden in the Stega image by using the same proposed system. Thus, the data can be protected without revealing the contents to other people.

Stega Image is capable of hide all type of data inside the image. The system is using dual layers of security in order to maintain data privacy. Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Privacy, on the other hand, is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively. Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues. Data privacy issues can arise from a wide range of sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, residence and geographic records and ethnicity. Data security or data privacy has become increasingly important as more and more systems are connected to the Internet. There are information privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, hiding the data in a kind of form such as within an image is vital in order to make sure that security or privacy of the important data is protected.

The rest of the paper is organized as follows. Section 3 reviews the related work and section 4 presents the both proposed algorithm. The implementation of the system is discussed in section 5 together with the discussion of various results obtained from testing the system based on the proposed algorithm. Finally, we conclude the paper in section 6.

3. RELATED WORK

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, using steganography.

Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is able to keep others from thinking that the information even exists.

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from seen or discovered.

Due to advances in ICT, most of information kept secure electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can used to secure information.

In cryptography, the message or encrypted message embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can extended to copyright protection for digital media: audio, video and images.

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchange on the internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection.

Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user.

Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

Throughout history, Steganography has been use to secretly communicate information between people.

Some examples of use of Steganography is past times are:

- During World War 2, invisible ink was use to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were use, because when each one of these substances are heated they darken and become visible to the human eye.

- In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message have written, the hair allowed growing back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messenger's hair to see the secrete message.
- Another method in Greece, someone would peel wax off a tablet that was covered by wax, write a message underneath the wax then re-apply the wax. The recipient of the message would simply remove the wax from the tablet to view the message.

The concept used in Stega Image is following. A bitmap (bmp) image will be used to hide the data. Data will be embedded inside the image using the pixels. Then the pixels of stega image can then be accessed back in order to retrieve back the hidden data inside the image. In both Algorithm (Text Information and Information File) two stages are involved. Text Information tab consists of two stage that are encoding and decoding. Information File tab consists of two stage that are Hide File and Extract File. Encoding stage is to come up with Text Information algorithm in order to hide the data inside the image and the Decoding stage is to come up with a decryption algorithm based on Text Information Algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stega image. Hide File stage is to come up with Information File algorithm in order to hide the data inside the image and the Extract File stage is to come up with a decryption algorithm based on Information File Algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stega image.

4. PROPOSED ALGORITHM

Our proposed algorithm is using two layers of security to maintain the privacy, confidentiality and accuracy of the data. Fig. 1 shows the framework for the overall process of the system. The system is able to hide all type of data inside the image as well as to retrieve the data from the image. From Fig. 1, for hiding all type of data, a User Id and password are required prior to use the Stega Image. Once the user has been login into the system, user have to select Tab depends upon type of data to be hide.

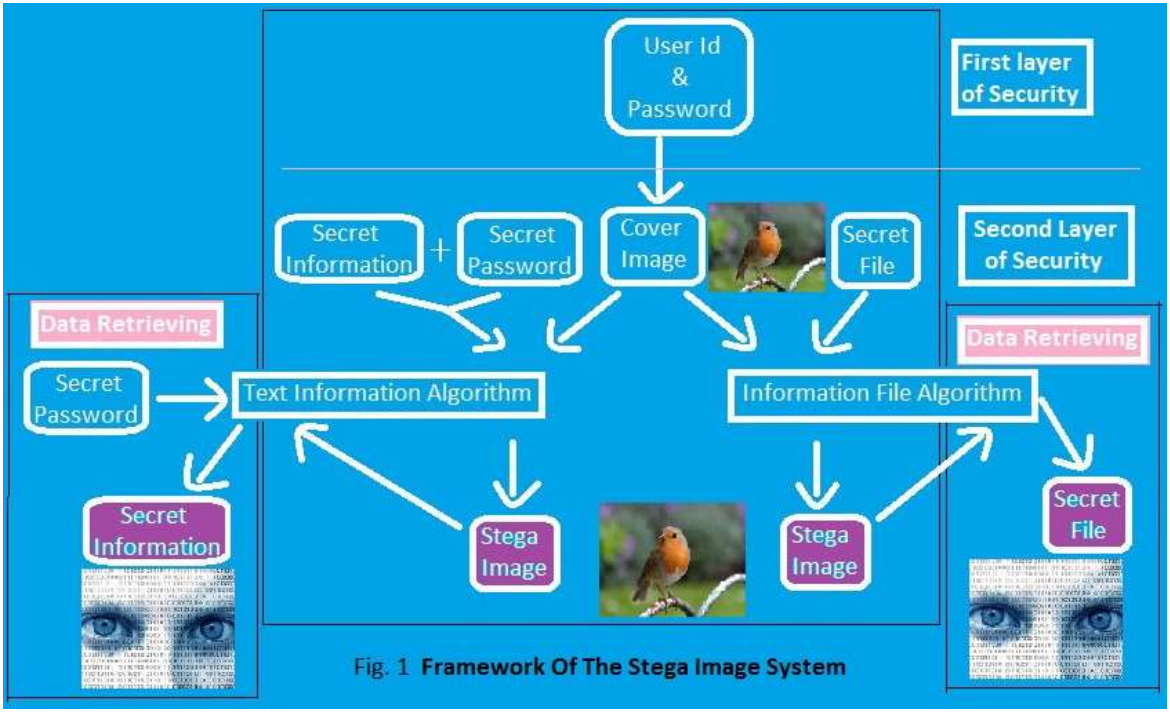
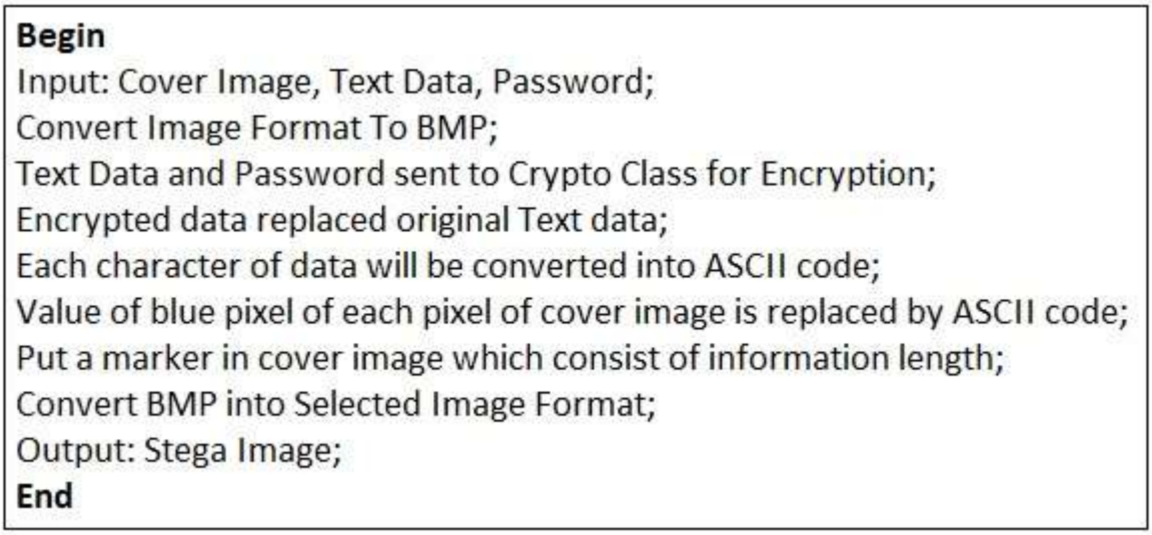


Fig. 1 Framework Of The Stega Image System

In **Text Information Tab**, the user can use the information (data) together with the secret password to hide the data inside the chosen image. Using Text Information algorithm, these data will be embedded and hided inside the image with almost zero distortion of the original image. For retrieving the data, a secret password is required to retrieving back the data that have been embedded inside the image. Without the secret password, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. For the Text Information algorithm, Fig. 2 shows the algorithm for embedding the secret message inside the image. During the process of embedding the message inside the image, a secret password is needed for the purpose of retrieving the message back from the image. From Fig. 2, the secret message that is extracted from the system is transferred into text box.

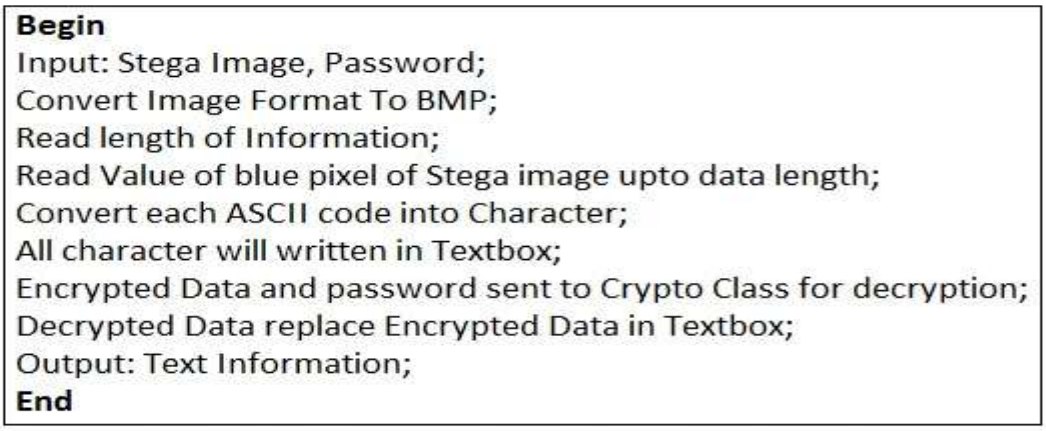


```
Begin
Input: Cover Image, Text Data, Password;
Convert Image Format To BMP;
Text Data and Password sent to Crypto Class for Encryption;
Encrypted data replaced original Text data;
Each character of data will be converted into ASCII code;
Value of blue pixel of each pixel of cover image is replaced by ASCII code;
Put a marker in cover image which consist of information length;
Convert BMP into Selected Image Format;
Output: Stega Image;
End
```

Fig. 2 Algorithm of Embedding Text Data inside Image

The text information is encrypted using **RIJNDAEL Algorithm** of encryption. **RIJNDAEL** is the block cipher algorithm recently chosen by the **National Institute of Science and Technology** (NIST) as the Advanced Encryption Standard (AES). String plaintext and string Secret is need as input where plain text is information and Secret is password. It gives alphanumerical encrypted string as output. Then each character of the encrypted data is converted into the ASCII code and replaced with the value of a blue pixel of cover image, then, next codes are encoded to the next blue pixel in image, the process is repeated until all the ASCII codes are encoded. The purpose of encryption of the text file is because the encryption is more secured if compared with the data that is without the encryption. The Decryption of encrypted data significantly hard to be encrypted without password. Furthermore, this series of binary codes of encrypted and the key is a long random codes in which they only consist of one and zero figures. A data hiding method is applied by using this series of binary codes. The password in this proposed Text Information algorithm is playing an essential role where the key is acts as a locker that used to lock or unlock the secret message. For the data hiding method, each character is encoded into each blue pixel pixel in image. This will ensure the original image will not be tempered with too many changes.

Once the information is hidden inside the image, the information can be extracted back from the stega image. Fig. 3 shows the algorithm for extracting the secret message from the stega image. In order to retrieve a correct message from the image, a secret password is needed for the purpose of verification.



```
Begin
Input: Stega Image, Password;
Convert Image Format To BMP;
Read length of Information;
Read Value of blue pixel of Stega image upto data length;
Convert each ASCII code into Character;
All character will written in Textbox;
Encrypted Data and password sent to Crypto Class for decryption;
Decrypted Data replace Encrypted Data in Textbox;
Output: Text Information;
End
```

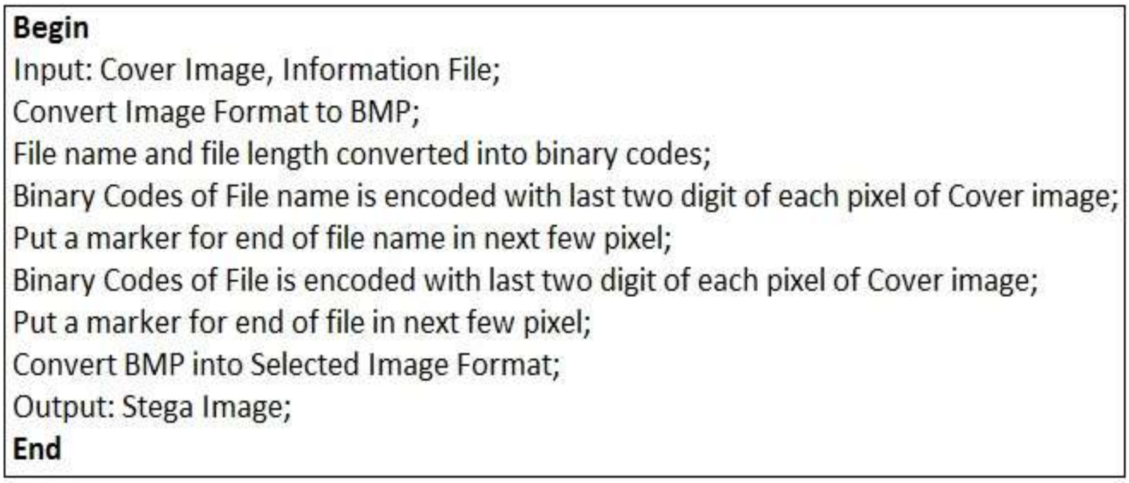
Fig. 3 Algorithm of Extracting Text Data from Stega Image

From Fig. 3, for the data extracting method, a secret password is needed to detect whether the key is match with the key that decodes from the series of ASCII code. Once the key is matched, the process continues by forming the ASCII code to information text, and show it in specified Textbox.

The main focuses of proposed Text Information algorithm are the use of transferring secret message to encrypted text using password, then converting into a series of ASCII codes, and the use of encoding each ASCII codes into only blue pixels of image. The image quality is still robust where the distortion and colour changes of images are reduced to the minimum or zero-distortion. Secret message, on the other hand, is difficult to be stolen by steganalysis as that was encrypted with password.

Both from Figs. 2-3 show that 2 layers of security are maintain within the system. However, the password is used for verification process in order to decrypt the correct message back from the image. The password is also embedded together with the data inside the encrypted data. Therefore, when a user is transmitting the image via the internet, that image contains the data and the password as well. However, the data can only be retrieved from the image using the STEGA IMAGE system.

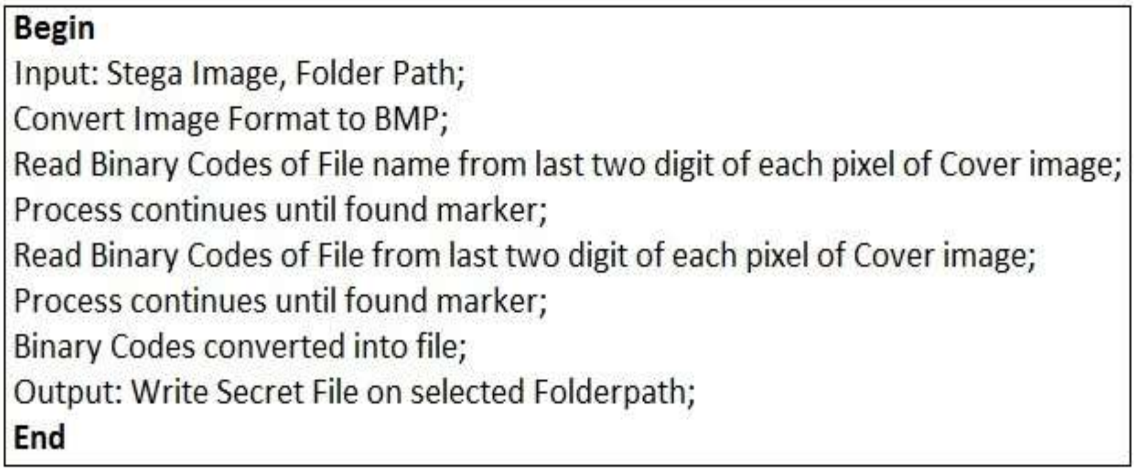
In **Information File Tab**, the user can use the any type of file to hide the data inside the chosen image. Using Information File algorithm, these data will be embedded and hided inside the image with almost zero distortion of the original image. For retrieving the secret file just need stega image, and the extracted file will be stored at selected Folder Path. For the Information File algorithm, Fig. 4 shows the algorithm for embedding the secret file inside the image.



```
Begin
Input: Cover Image, Information File;
Convert Image Format to BMP;
File name and file length converted into binary codes;
Binary Codes of File name is encoded with last two digit of each pixel of Cover image;
Put a marker for end of file name in next few pixel;
Binary Codes of File is encoded with last two digit of each pixel of Cover image;
Put a marker for end of file in next few pixel;
Convert BMP into Selected Image Format;
Output: Stega Image;
End
```

Fig. 4 Algorithm of Embedding File inside Image

The file is converted into the binary codes. A data hiding method is applied by using this series of binary codes. By applying the data hiding method, the last two binary code from the series are encoded into a pixel in image, then, next two binary codes are encoded to the next pixel in image, the process is repeated until all the binary codes are encoded. For the data hiding method, each last two bit is encoded into each pixel in image, this will ensure the original image will not be tempered with too many changes. Once the message is hidden inside the image, this message can be extracted back from the stega image. Fig. 5 shows the algorithm for extracting the secret file from the stega image. From Fig. 5, for the file extracting method, the process continues by forming the binary code to a file and save it to selected Folder path.



```
Begin
Input: Stega Image, Folder Path;
Convert Image Format to BMP;
Read Binary Codes of File name from last two digit of each pixel of Cover image;
Process continues until found marker;
Read Binary Codes of File from last two digit of each pixel of Cover image;
Process continues until found marker;
Binary Codes converted into file;
Output: Write Secret File on selected Folderpath;
End
```

Fig. 5 Algorithm of Extracting File from Stega Image

The main focuses of proposed Information File algorithm are converting into a series of binary codes, and the use of encoding is last two digit of each binary codes into each pixels of image. The image quality is still robust where the distortion and colour changes of images are reduced to the minimum or zero-distortion. The Secret File can only be retrieved from the image using the STEGA IMAGE system. Information File Algorithm is little bit less secure in comparison with Text Information Algorithm.

5. RESULT AND DISCUSSION

Based on the proposed algorithm, we develop a simple system, which implements both algorithm. We name the system as STEGA IMAGE. Based on the framework for the system as seen in Fig. 1, Stega Image imposed on 2 layers of security. The first layer is for the login purpose and the second layer is for the hiding and retrieving purposes. The system is introduced in Fig. 6 shows the login interface for the system, Fig. 7 shows the main interface of Text Information Tab of the system and Fig. 8 shows the main interface of Information File Tab of the system.

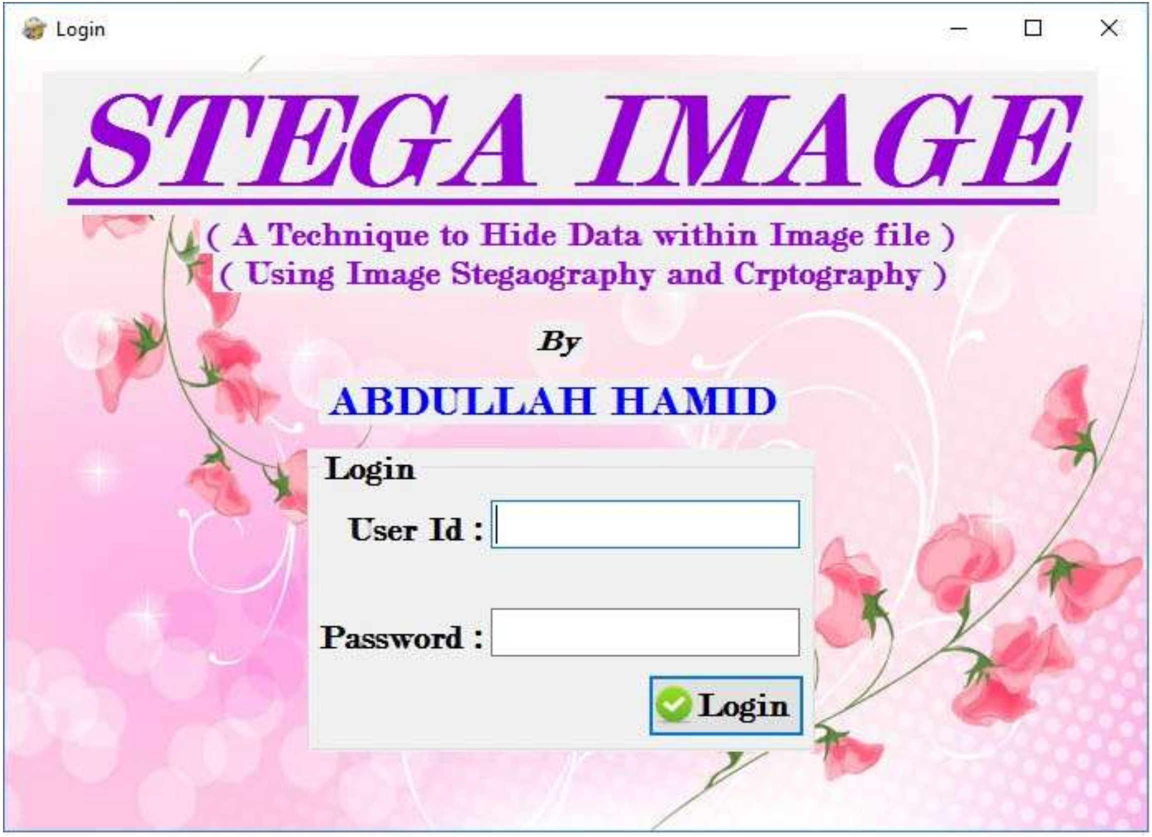

Login
STEGA IMAGE
(A Technique to Hide Data within Image file)
(Using Image Stegaography and Crptography)
By
ABDULLAH HAMID
Login
User Id :
Password :
Login

Fig. 6 Login Interface of Stega Image

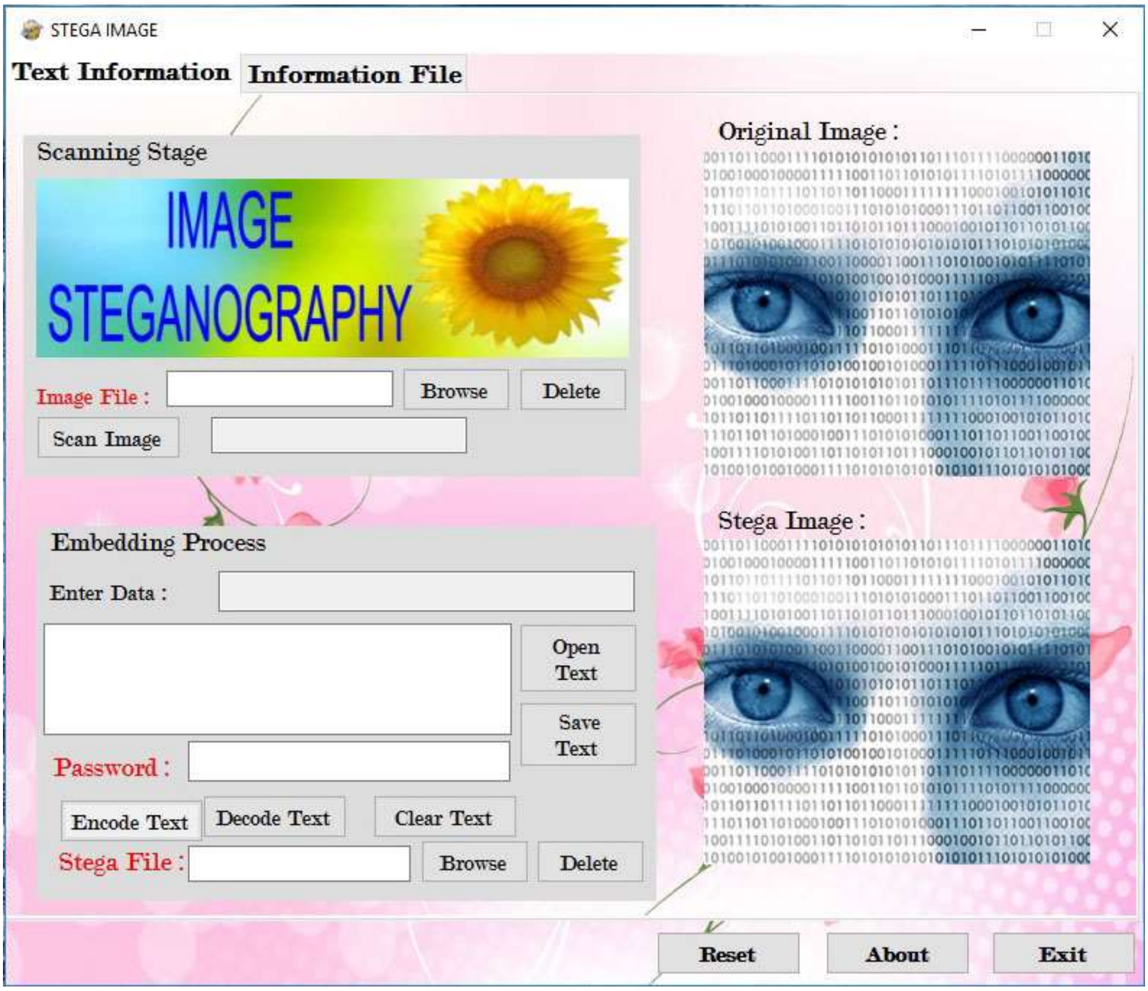


Fig. 7 Interface of Text Information Tab of the system

From Fig. 6, system has two Textbox, one box for the User Id and another box for the Password that the user needs to login to use the system. From Fig. 7, Text Information Tab has two group, one group is scanning Stage and another group is Embedded Process. Scanning Stage consists of three button that are Browse, Delete and Scan Image. Browse button used to browse the Cover Image, after browsing original image will be shown in Original Image Picture Box. Delete Button used for Reset the scanning stage, and Scan Image button used for Scan the selected image and show how many characters can possible to hide in cover image. Embedded Process is the main part of this Tab. There is a Textbox named as Enter Data in which we have to type the secret information or we can extract from any Text File using Open Text Button. There is also a Textbox named as Password in which we have type secret password. Encode button is used for embedding the secret information in image, while Decode button is used for Extracting information from stega Image. In order to extract the data from the stega image, same secret password is required which was used at the time of encoding. The system accept minimum 6 characters password. Once the information has been encoded in image, the new stega image can be saved to a different image file. This new stega image can then be used by user to send it via internet or email to other parties without revealing the secret data inside the image. If the other parties want to reveal the secret data hidden inside the image, the new stega image file can then be upload again using the system to retrieve the data that have been locked inside the image using the password.

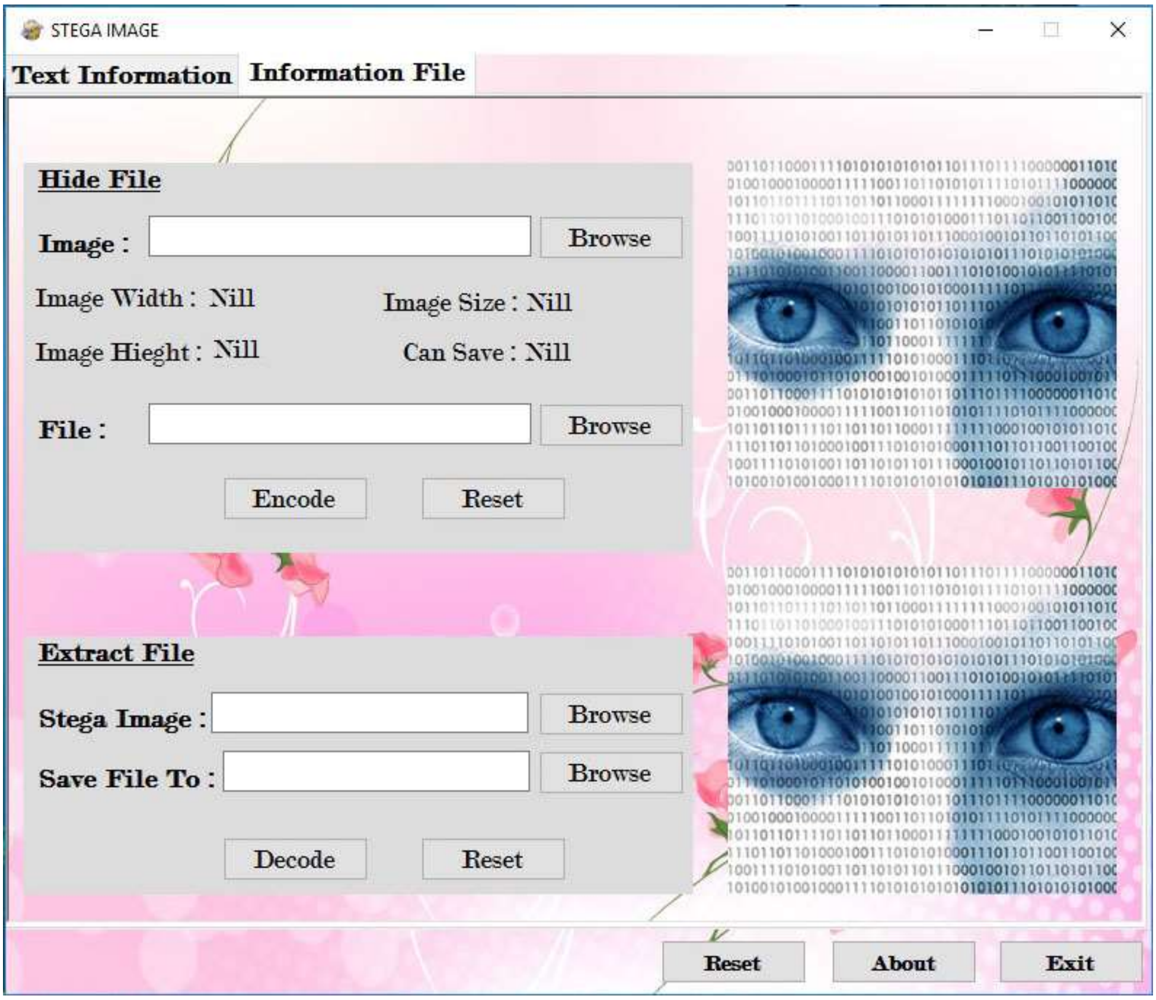


Image Width : Nill

Image Size : Nill

Image Hieght : Nill

Can Save : Nill

Fig. 8 Interface of Information File Tab of the system

From Fig. 8, Information File Tab has two group, one group is Hide File and another group is Extract File. Hide File consists of four button that are Browse (Image), Browse (File), Encode and Reset. Browse (Image) button used to browse the Cover Image, after browsing original image will be shown in Original Image Picture Box, also shows height, width, image size along with how larger file possible to hide in cover image. Browse (File) Button used for browse the file, after browsing system checks the size of file and if size of file was not possible to hide in selected cover image, it shows a warning. Reset button uses to reset Hide File section and Encode button used for embedding the file in cover image. Once the information has been encoded in image, the new stega image can be saved to a different image file. Extract File is the part where we can extract the file from Stega Image. In this section we have to browse Stega image using Browse (image) button and browse the folder path where extracted file will be saved.

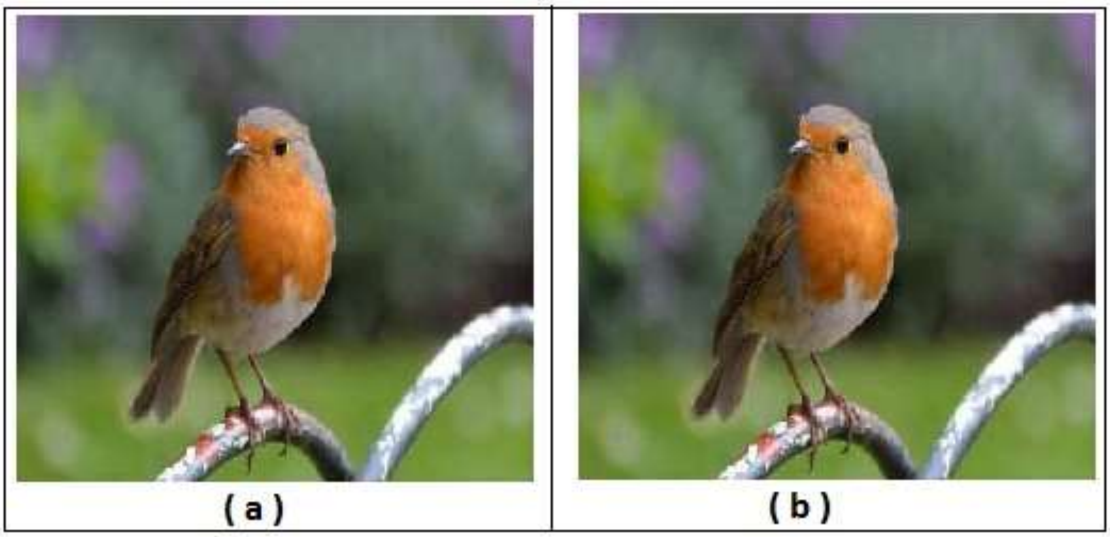


Fig. 9 (a) Original Image (b) Stega Image

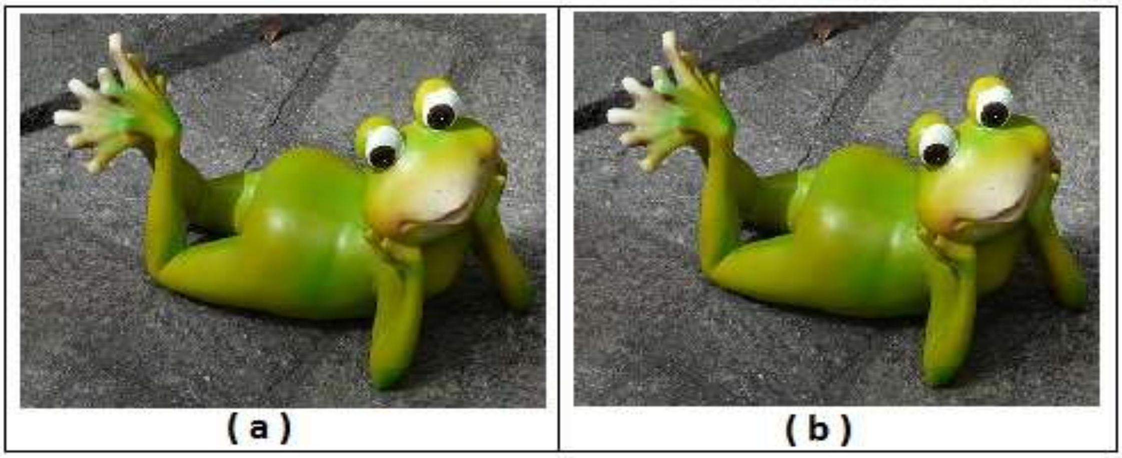


Fig. 10 (a) Original Image (b) Stega Image

The system is tested using the images as showed in Figs. 9-10. Fig. 9 (a) shows the original image before the message is stored inside the image and Fig. 9 (b) shows the stega image after the message is stored inside the image. We found that the stega image does not have a noticeable distortion on it (as seen by the naked eyes). Fig. 10 shows another example of image with data hidden inside the image. From Fig. 10, it shows that the comparison of distortion by naked eyes between cover image and stega image is almost zero. The surfaces of between both images show no difference by using naked eyes even though the size of stega image has a slightly higher than the cover image.

6. CONCLUSIONS

This paper proposed a new steganography algorithm with 2 layers of security. A system named Stega Image has been developed using the proposed algorithm. We tested few images with various sizes of data to be hidden. With the proposed algorithm, we found that the stega image does not have a noticeable distortion on it (as seen by the naked eyes). Hence this new steganography algorithm is very efficient to hide the data inside the image. Stega Image can be used by various users who want to hide the data inside the image without revealing the data to other parties. Stega Image maintains privacy, confidentiality and accuracy of the data. The message is highly secure since it has double-layer protection: encryption and steganography, and has wide range of applications in various sectors.

Special features of STEGA IMAGE are follows:

- It supports all Format of image as input and output while other steganography tools only supports BMP.
- It is capable to hide all type of data or file while other steganography tools only supports either text information or file.

- Encryption works like additional layer of privacy.
- Its algorithm give much more size or information to hide in comparison with other steganography tools.

Acknowledgement

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.

I am highly indebted to our technical guide Miss SOHINI BANERJEE for her guidance and constant supervision as well as for providing necessary information regarding the project and also for her support in the Project.

I would also extend our gratitude to faculties and other members of our esteemed institution for their kind co-operation and encouragement which helped us in this project.

Also my thanks and appreciation also goes to our friends who have willingly helped in our project in best of their abilities.

Lastly, thanks to my parents (Especially to my father MOHAMMAD NEAR KHAN) for all type of support and amazing chances they've given me over the years.

REFERENCES

Websites

- http://www.google.com
- http://msdn.microsoft.com
- http://www.wikipedia.org
- http://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html

Books and E-Books

- Mastering C#
- Professional C#, 2nd Edition
- Professional ASP.NET
- MCAD/MCSD Self-Paced Training Kit: Developing Web Applications with Microsoft® Visual Basic® .NET and Microsoft Visual C#® .NET, Second Edition