Auto Key Generation and Minimal Image Distortion Mechanism for Image Steganography

Yuvraj Hembade
M.Tech(Computer Engineering)
Pune

Nikita Bhanose
B.E(Computer Engineering)
Pune

Grishma Kulkarni
B.E(Computer Engineering)
Pune

Utkarsha Memane
B.E (Computer Engineering)
Pune

Jayashree Patil
B.E (Computer Engineering)
Pune

ABSTRACT

Nowadays, due to extensive usage of internet for communication, the possibility, threat to data being communicated can't be neglected. Wherever there is a need to have secrecy of the data, there must be a strong technique of encryption.To improve the security features in case of data transfers over the internet, the techniques that have been known till now are like Cryptography, Steganography, etc. Where Cryptography is defined as the method to conceal information by encrypting plaintexts to cipher texts and later transmitting it to the intended recipient using an unknown key, on the other hand Steganography provides or extends security further to a high level by hiding the cipher text into text, image or other formats. For hiding secret information in images, there are many steganography techniques. Each of them has strong and weak points. The methods used before, were having limitations of payload capacity, specific image formats to be used, and more distortion of image quality.

The major advantages of this work are having maximum payload capacity, minimum kind of distortion in actual image quality, negligible change into original covert medium and encrypted file.

General Terms

Image steganography, Auto-generated key

Keywords

Covert image, Plaintext, Payload Capacity

1. INTRODUCTION

Now days, internet security is very important aspect in the world. To improve the security features, in case of data transfers over the internet, the techniques that have been known till now are like Cryptography, Steganography, etc. Steganography, the Greek word "Stegos + grafia" literally means, "Covered + writing" [1]. The idea of steganography mainly circulates around avoiding the use of busy communication channels between the communicating people. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Steganography is a technique which hides information in such a way that, communication occurs as usual and intruder can't even suspect about occurrence of secret communication. An integrated approach to image steganography is to auto-generate the key and send the generated key along with original image to the receiver.

In today's world of internet communication there is possibility of leaking secret information, by the intruders. So, to have a secure communication via network, there must be a strong encryption technique. In vast and deep context of information security, variety of techniques for information hiding; among all those we had been interested in something, which doesn't even, leave doubt of secret communication.

In ancient Greece around 440 B.C. Herodotus is the first Greek historian, who used steganography to convey a message against Persian king. What he has done was he shaved the hair of his messenger than write a message on his head. Later, he waits till that hair growth occurs again and could hide that message. Steganography is thus an art of covered writing that is not seen by any person other than the intended recipient [1].

An image constitute of different pixels having different intensities. This numeric representation forms grid. Every image has its pixel map and it consists of pixels and its color. Bit depth is defined as the number of bits in a color scheme. 8 bits are used to describe the color of each pixel. Thus monochrome and grayscale images use 8 bits to represent each pixel are able to display 265 different color or grayscale. [1]

Digital color images use RGB color model are stored in 24 bit format. Here in RGB model all color variation are derived from primary colors red, green and blue. This result is more than 16 million combinations of different colors. Different types of images can be used for image steganography and the goal is to provide secure communication by minimizing the image distortion after hiding the data in the image.

2. LITERATURE SURVEY

Since the rise of the Internet, that is one of the most important factors of information technology and communication it should be secured. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography involves communication of secret data in appropriate carrier which may be image, audio, video or TCP/IP header file. It hides the very existence of embedded data so as not to arouse an eavesdropper's suspicion. Different techniques of image steganography are available which need thorough understanding and evolution of their existence [2]. Steganography techniques have various features which characterize their weaknesses like embedding capacity, perceptual transparency, robustness, tamper resistance, computational complexity, etc.

Image steganography is further classified into spatial domain and transform domain [2]. In spatial domain the least significant bit (LSB) of the bit planes of covert image are replaced with secret data bits. This results in high embedding capacities and ease of implementation. Whereas in transform domain the covert image is converted to frequency domain and then secret data is embedded in frequency coefficients. This results in higher levels of robustness against simple statistical analysis.

Another important topic in information hiding is steganalysis which is the art of detecting the presence of steganography. Various types of steganalysis schemes are developed [3].Steganalysis has three types of categories 1.Visual Attacks are used to identify the presence of hidden information so that it can separate the image into bit planes. 2. Statistical Attacks is use to suspect the changes in the image behavior. 3. Structural Attacks ,in this file formats may change when data is to be hidden is embedded.

For hiding the data different carrier file formats can be used but digital images are most popular because of their frequency on the internet. And also it is necessary to identify the requirement of a good steganography algorithm. The different applications have different requirements so different steganography techniques are used. Thus it is important to analyze which steganography techniques are more suitable for which application. This can be done by studying the different types of steganography techniques with their pros and cons [4].

The image formats used for image steganography are more suitable which have high degree of redundancy. Redundancy is defined as the bits of an object that provide greater accuracy. The redundant bits of object are those which can be altered and this alteration is not been detected easily. Also to avoid possibility of suspicious, image files being transmitted must be of smaller size and there must not be too much change in quality of original and stego image. In some steganography techniques 8-bit random key is used for encrypting the secret message and also the same key will be used for choosing the pixel in cover image where the encrypted data is hidden [5].Least significant bit is one of the most popular steganography techniques [6]. Image steganography provides high security purpose and it can be used for legal and illegal purpose.

The performance of image steganography methods can be evaluated by many parameters. Some of them are capacity ,security, imperceptibiltity, tamper resistence and computational complexity,etc[8].Based on these parameters the types of image steganography are differenciated. One of the simple technique is LSB(Least significant bit) substitution method. In this technique the data hiding is done by replacing the LSB of the image with the actual data[9].Various extensive experiments show the effectiveness of this technique.

Another method more effective than LSB method is Pixel-value differencing. In this technique the data hidden in the image can be obtained without referencing the original cover image. A pseudo-random mechanism can be used to achieve secrecy protection. Dual statistic attacks were conducted to show the security of the method[10].A technique Triple M method (Matrix Matching Method) makes the steganalyst harder because this method is not performed on same specific bits. Experimental result also shows that stego images visually indistinguishable from the original image[11].

3. METHODOLOGIES

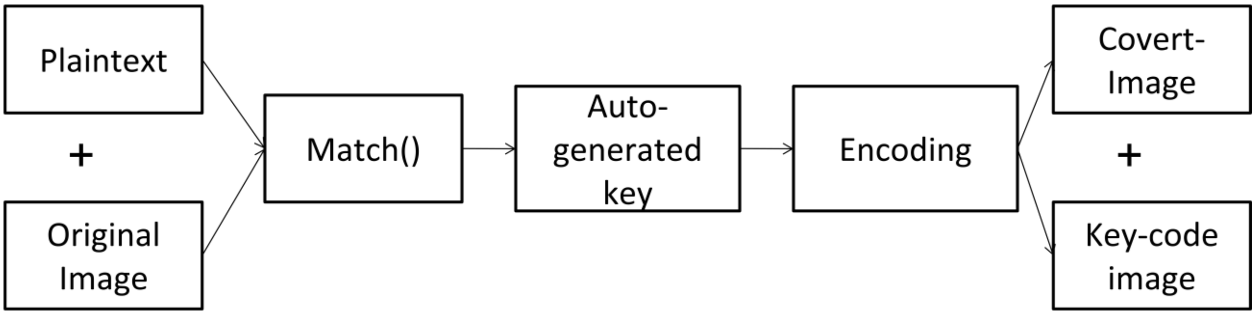


Fig 5: Sender side operation

On the sender side user uploads the covert image in which the secret message is to be hidden along with the secret message. Then using match( ) the system matches the data bits of image with the data bits of message and the mark the position which matched. This positions form the auto-generated key which will be further used to retrieve the original message on the receiver side.

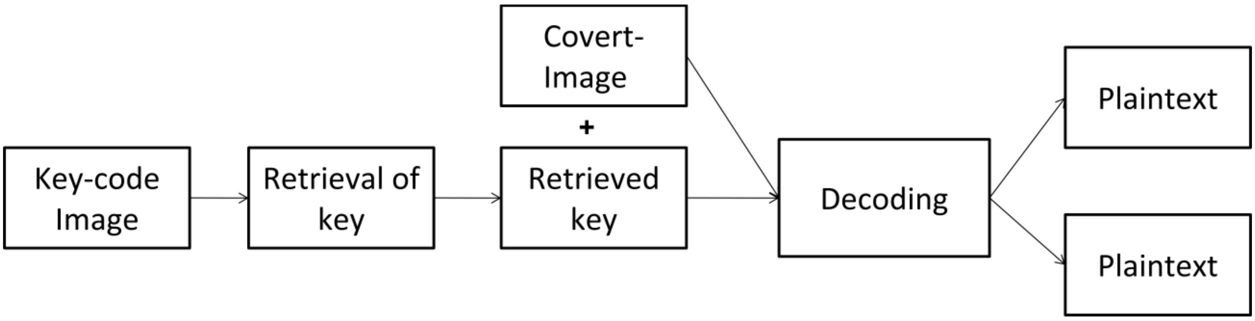


Fig 6: Receiver side operation

On the receiver side to retrieve the original message the user has to upload the original image along with the key code image. Then the system again uses the match( ) to match the data bits of key code image with the data bits of original image and get the positions. This will retrieve the message in the binary format and finally this binary format of text is converted to plaintext i.e. the original secrete message.

3.1 Algorithm

1. Upload the cover image.
2. Type the secret message or upload the text file to be embedded.
3. Convert the text to binary format.
4. Convert the image to binary format.
5. On the sender side use match ().
6. Using match (), match the data bits of secret message with the data bits of image and store the matched positions into the position file.
7. Convert the position file into image which will be the key-code image.
8. The key-code image along with the original image will be saved at the given location.
9. On the receiver end again convert the key-code image and original image into binary format and use the match function to retrieve the positions of image bits to get the secret message in binary format.
10. Finally, convert the secret message in binary format into text and display that converted secret message in the text box or create a text file of it in the location given by the user.

3.2 Modules to Sender side

1. Take Plaintext and Image which is to be used as cover object, as input.
2. Modules for hiding text

3.2.1 Text to binary

This module converts the secret text message into binary format, for this we use StringBuilder class from .NET. The StringBuilder class is found in the System.Text namespace. The StringBuilder class is used when you want to modify a string without creating a new object. In the StringBuilder class we use the append function for conversion. The arguments to this function are the Convert.ToByte ().

3.2.2 Image to binary

This module converts the image into binary format using MemoryStream class. In this class, the Image object has a save function which saves an image to a file in any image format supported by the .NET Framework, *save* function is applied on the MemoryStream object, while specifying an image format. Since the object is in memory, it can be easily converted into a byte array with the ToArray function in the MemoryStream object.

3.2.3 Match Function

This module matches the data bits of secret message with the data bits of image, and will mark the positions which match and form a position file of it. This position file will be the auto generated key and will be converted into a image called as the key-code image.

3.2.4 Generating and storing the key-code image and original image

Match function creates key-code image which is to be transmitted to the receiver along with original image and saved at specific location .This key-code image will be useful in retrieving the message at receiver end.

3.3 Modules to Receiver side:

1. Take original image and key-code image asa input from user.
2. **Modules for unhiding the text:**

3.3.1 Key-code image and original image to binary

This module converts the original image and key-code image into binary format using FileStream class. The object of FileStream class is used. Since, it can be easily converted into a byte array from the FileStream object.

3.3.2 Retrieving of positions from key-code image

Using match() matched positions are retrieved from the key-code image.

3.3.3 Retrieving of text message in binary format

This module retrieves the message from the matched positions in binary format.

3.3.4 Binary to text

This module converts the secret message data bits into text and generate text file which can be saved at any given alterable path by user. In addition plaintext will be displayed textbox.

4. IMPLEMENTATION

4.1 User Interface

The proposed system used C-sharp .NET as a framework for the implementation because it provides the quality front end design.It also contains almost all functions to deal with the images and conversion functions which are required during implementation of all the modules of the system.

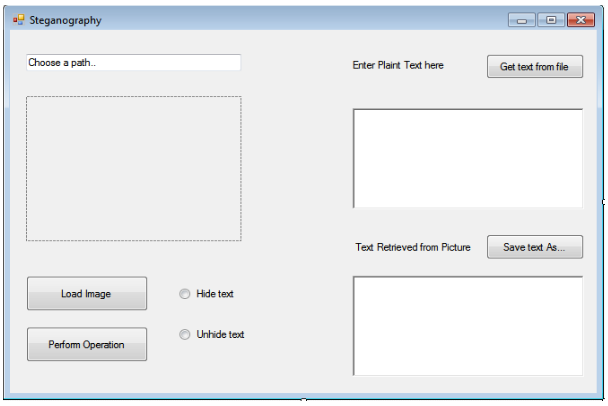

Choose a path..

Fig 1: Basic User Interface

Standard Buttons:

Load image: This button will upload the covert image for hiding text.

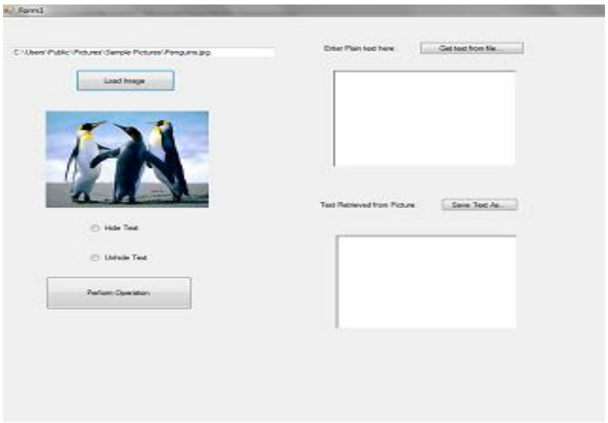

C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg

Fig 2: Load Image

Hide text: This will enable the sender side where the text will be hidden.

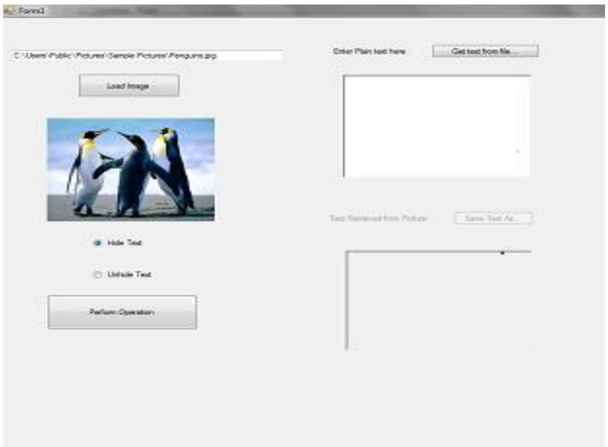
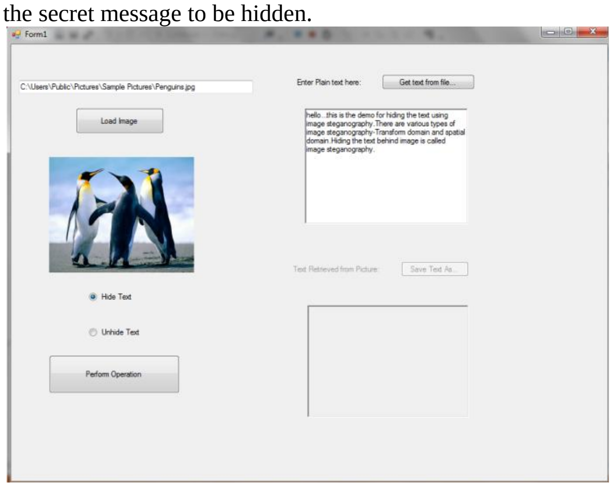

C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg

Fig 3: Hide Text

Get text from file: It will upload the text file which contains the secret message to be hidden.


C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg

hello...this is the demo for hiding the text using image steganography.There are various types of image steganography-Transform domain and spatial domain.Hiding the text behind image is called image steganography.

Fig 4:Get Text from file

Unhide text: This will enable the receiver end where it is used forunhiding the text.

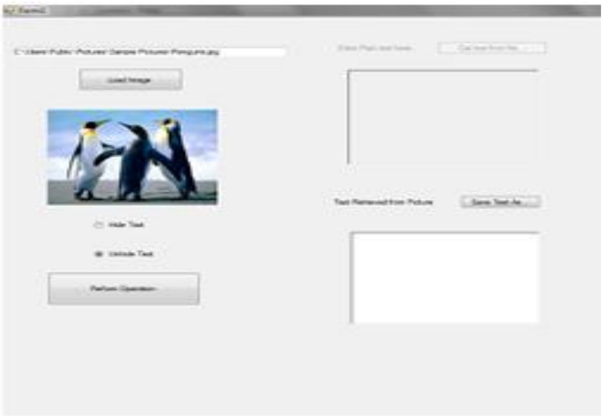
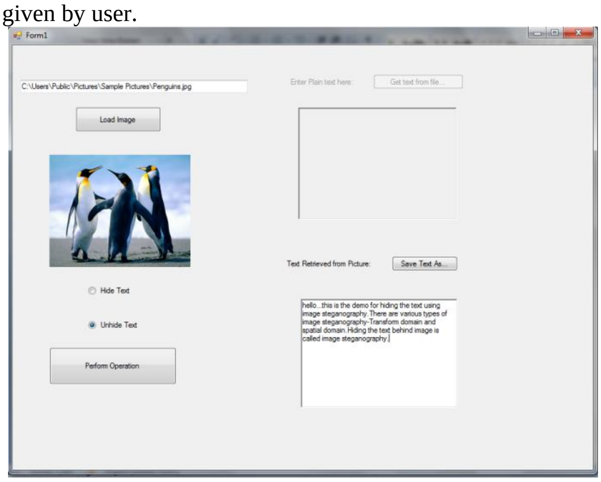

C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg

Fig 5: Unhide Text

Perform operation: This will either hide or unhide the text message.

Save text as: It will save the retrieved text at alterable path given by user.


C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg

hello...this is the demo for hiding the text using image steganography.There are various types of image steganography-Transform domain and spatial domain.Hiding the text behind image is called image steganography.

Fig 6: Save retrieved text displayed in textbox to a file

5. CONCLUSION AND FUTURE WORK

In this paper ,simple algorithms for processing raw images and auto-generated key have been used. This technique has been used to accommodate maximum payload. In this project the key is auto-generated to focus on minimum image distortion. The key in the form of image along with the original image will be sent to receiver side. In this, still there is a wide scope of research, as the context of security widens with importance of the information to be communicated. So further, this work can be extended with implementation of additional modules, as per the requirement of the users. Some new algorithms can be developed to embed the data into images of all types, eliminate the generation of extra key code image which may be suspicious and add it as module of the system, which will further enhance the secrecy.

6. ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of this research would be incomplete without mentioning of the people who made it possible, without whose constant guidance and encouragement would have made efforts go in vain. Gratitude and respect is expressed towards all those who guided throughout the completion of this research.

Sincere gratitude is expressed to project guide Mr.Yuvraj Hembade and Head of the Department for their valuable guidance, encouragement and for providing all the necessary facilities, in carrying out this research work and thanks to guide for constant support and encouragement in preparation of this research paper and for making available library and laboratory facilities needed to prepare this paper.

7. REFERENCES

[1] Rupali Jain, Jayashree Boradh, Advances in digital image steganography, IEEE 2016.

[2] Saha, B. and Sharma, S., Steganographic Techniques of Data Hiding using Digital Images Defence Science Journal, Vol. 62, No. 1, January, pp. 11-18, DESIDOC, 2012.

[3] Bhatacharya, A., Banerjee, I., and Sanyal, G., A survey of steganography and steganalysis techniques in image, text, audio and video cover carrier", Journal of Global Research in Computer Science, vol.2, no.4, pp.1-16, 2011.

[4] Morkel, J.H.P. Eloff, M.S. Olivier, "An overview of image steganography", http://mo.co.za/openistegoverview.pdf.

[5] Sellars, Duncan, "Introduction to steganography",http://www.cs.uct.ac.za/courses/CS400 WINIS/papers99/dsellars/stego.html.

[6] Moerland, T., Steganography and Steganalysis, Leiden Institute of Advanced Computing Science, www.liacs.nl /home/ tmoerl/privtech.

[7] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing", Pearson Education India, 2009.ISBN- 8131726959, 9788131726952.

[8] Gandharba Swain,Saroj Kumar Lenka,Classification of Image Steganography Techniques in Spatial Domain: A Study,Vol. No.5,IJCSET 2014.

[9] Chan, C. K. and Chang, L. M.,hiding data images by simple LSB substitution, Pattern recognition, vol 37 pp 469-474,2004.

[10] Wu, C., Tsai, W.H.,Asteganographic method for images by pixel-value differencing,Pattern Recognition Letters vol 24,pp1613-1626,2003.

[11] Kaur, J., Duhan, M., Kumar, A., Yadav, R.K.,Matrix matching method for secret communication using image steganography, Fascicule 3. ISSN 1584 – 2673, 2012

[12] William Stallings, "Cryptography and Network Security Principles and Practices", Fifth Edition, (2005).

[13] Mahendra Kumar," Steganography and steganalysis of JPEG images" ,2011.