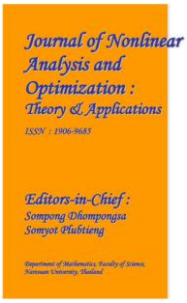
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2, No.1 : 2024
ISSN : **1906-9685**



SECURITY FOR SECRET COMMUNICATIONUSING IMAGE STEGANOGRAPHY

M.SIVA Student, III Year (Digital Cyber Forensic Science) Rathinam College of Arts and Science, Coimbatore-21
Dr T VELUMANI Assistant Professor Department of Information Technology Rathinam College of Arts and Science, Coimbatore–21

INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a goodsteganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications

DRAWBACKS OF EXISTING SYSTEM:

There are large number of information, huge file size, therefore someone can suspect aboutthis approach is gone in the wrong hands such as hackers, terrorist, criminals then this can be very much is not without its disadvantages. However, these can be rectified and once it is performed and it can strengthen the element of data hiding approach take advantage of humanperceptual deficiency, but they have deficiency of their own. However, these can be independently major disadvantage of steganography is that, unlike cryptography, it needed a lot of overhead to hide associatively few bits of information. Because the steganographic system is found, it is rendered useless. However, it fares no worse than cryptography and is still the preferred medium.

ADVANTAGES OF PROPOSED SYSTEM:

It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc.,as a cover object. Steganography can be used in the case of covert channels, which occur in theOSI layer network model The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities arethe key to data concealment in image steganography Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography Cover-Image - Unique picture that can conceal data Message - Real data that you can mask within pictures. The message may be in the form of standard text.

MODULE DESCRIPTION:

1. Import Modules.
2. Create a Function to make a main frame
3. Function to go back to the main frame
4. Function to Encoding and Decoding frame.
5. Create function for encoding image
6. Create function for decoding image

7. Function to decoding and generation of data
8. Function to modify the pixels of image
9. Function to enter the data pixels in image
10. Function to enter hidden text
11. GUI loop

ALGORITHM :

The most commonly method used for steganography technique is a Least Significant Bit (LSB) algorithm. LSB algorithm performs the embedding operation of message along with the image file where each pixel has a size of 3 bytes. Each and every bit of the message is taken and this message bit is embedded along with the bytes of the image file such that,it doesn't make any perceivable change in the message embedded file. Findings: That is theease of cracking the message which is hidden in the image file due to the simplicity of the Algorithm that provide the simple platform for the easy cracking and detectability of the hiding data. Thus the Security Extensibility algorithms for steganography used as a F5algorithm and cryptography used as a AES algorithm which is used to provide the more security such that the cracking is made quite tough which is almost improbable.

Steganography F5 algorithm is more secure than other existing algorithm such as LSB algorithm, RSA algorithm. Conclusion: F5 algorithm performs the matrix encoding to improvethe efficiency of embedding and extraction operation. Thus it minimizes the number of necessary changes. F5 algorithm employs per mutative straddling to scatter the message over the whole cover medium to reduce the chances of detectability and improving the security of data. This paper also introduces the quality of the image using various data hiding and diffusiontechniques

SOFTWARE DESIGN AND EXPERIMENTAL RESULTS:

There are many techniques used to hide secret image. Here, LSB with XOR as well asDCT techniques are used. LSB technique is based on bit of an image, hence, taking it into consideration, types of LSB hiding techniques are variable size technique and fixed size technique. Variable size technique is implanted when number of bits in every pixel are relies on contrast and luminance qualities. And fixed size technique is implanted when number of bits in secret image's pixel are same as those of cover image. For transforming eight by eight-pixel matrix of an image in to every 64 coefficients of JPEG image for every colour component,Discrete Cosine Transform (DCT) technique is used. The Exclusive- OR,XOR is logical operation for binary numbers. It's an important method of encoding. It's being used for loop codes while connecting to safe data centers, that are widely employed in internet browsers.

Strong protection provided by this technique after using correctly. However, once thecode is not being used correctly, this privacy is simply beaten. Below table is a truth table of XORfor 2 bits A & B. Let us assume that, A is a cover data bit and B is a bit of a key. The lastcolumn is result of XOR operation.

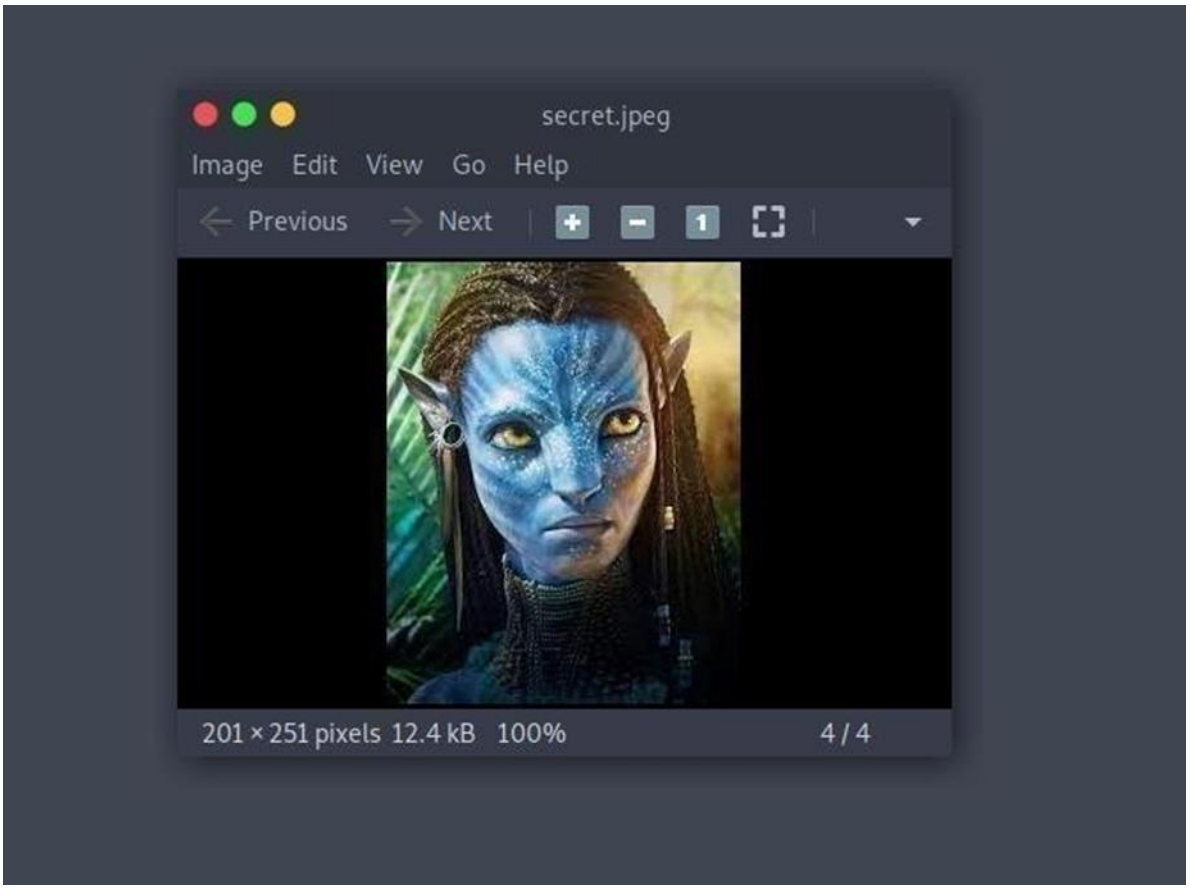
Acknowledgment

This article / project is the outcome of research work carried out in the **Department of Computer Science under the DBT Star College Scheme.** The authors are grateful to the Department of Biotechnology (DBT), Ministry of Science and Technology, Govt. of India, New Delhi, and the Department of **Computer Science** for the support.

REFERENCES

1. Richard Bergmair: Natural language steganography and an "AI-complete" security primitive.talk, December 2004.
2. Li, Mingjie, Zichi wang, "Disguise of steganography".
3. Dr.Amarendra K, Venkata Naresh Mandhala, B.Chetangupta, G.GeethaSudheshna, V.Venkata Anusha.Image Steganography Using LSB (2019)
4. A.J. Raphael and V. Sundaram, "Cryptography and Steganography-A Survey", International Journal ofComputer Technology and Applications.
5. K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods," Multimedia

Toolsand Applications
6. N.Subramanian, Somaya Al-Maadeed, Ahmed Bouridane, Image Steganography:
7. 7. A Review of the Recent Advances
SREELAKSHMI (2015, Nov 9), " Image Steganography using LSB,"
8. Secure Data Transfer Through Internet Using Cryptography and Image Steganography 2020
9. Savitha Bhallamudi, "Image Steganography", December 2015



1. SYSTEM DESIGN

INPUT DESIGN:

The growing capabilities of modern communication technology call for special means of computer network security. With increasing data exchange rate through internet, network security is becoming more and more important. Therefore, the confidentiality and integrityof data is required to prevent unauthorized access and use. This trend brings the significantgrowthin the field of information hiding. In addition, the development of publishing and broadcastingtechnology also calls for other solutions of information hiding, such as audio,video, other sources and all rights reserved. Availability of digital format may result in widelyunauthorized copying because digital format provides the possibility to make many more high-quality copies. Steganography refers to a science of invisible communication. While reverse cryptography aims to secure communications.

OUTPUT DESIGN:

Steganography, reverse other ways of communications, and one's awareness of underlying communication between the sender and receiver defeats whole purposes. Therefore, first requirement of steganography way is its undetectability. In other words, the steganography wayis considered to be insecure, if the warden Wendy is able to distinguish between cover- objectsand stego objects. For information hiding, there is no such active enemy because the deletion of information hidden in the content will create no value over-object: refer to the object used as carrier to conceal messages in many various objects. It can be used to conceal messages intomany kinds of media, such as image, audio, video, file structure, HTML page and so on.

Stego object: refer to the object which carries the hidden message

SYSTEM TESTING
LITERATUREREVIEW:

A strategy to stego pictures to enhance PSNR as well as MSE standards is recommended. LSB and DCT methods study the impact of a conversion [2]. A document wherein the RGBpicture method Least Significant Bit Steganography is displayed. It conceals RGBimage in 3 planes of the color image since bit lane slicing in this way which minimal noise in stego image is induced with minimal change in the image's noticeable quality that could not beidentified by bare eyes [7]. Some cryptographic and steganographic techniques are being usedto accomplish the objective that providing safety for data or file during processing.

Cryptographic techniques turn the initial message into a pre-transmission code signal,while the basic concept used in steganography is to conceal the message's presence in a file. This enables only the formal address as well as the recipient to recognize the presence of confidential information. A new clustering and noise-based method is suggested in this article to improve the safety of the concealed information. The above method suggested comprises of two stages. During the first stage, the cover image pixels are collected in to the separate clusters which used the k-means clustering algorithm accompanied by the method of encoding.

INTEGRATION TESTING:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basicoutcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components