International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Secure Message Transmission using Image Steganography on Desktop Based

**Sidharth Sai S[1], N. Priya[2]**

[1]PG Student, [2]Assistant Professor,
[1,2]Department of MCA, Jain Deemed-to-be-University, Bangalore, Karnataka, India

**ABSTRACT**

The rapid increase in our technology has made easier for us to send and receive data over internet at most affordable way. There are many transmission medias like emails, facebook, twitter, etc… which led way for the intruders to modify and misuse the information what we share over the internet. So in order to overcome these kinds of issues many methods has been implemented such as Cryptography, Steganography and Digital watermarking to safeguard our data transmissions in a most prominent way. In this paper, hiding text inside a digital image using Stegano tool for secure data transmissions has been described.

***KEYWORD:*** *Cryptography, Steganography, Stegano tool*

***How to cite this paper:*** Sidharth Sai S | N. Priya "Secure Message Transmission using Image Steganography on Desktop Based" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.864-866, URL: www.ijtsrd.com/papers/ijtsrd38067.pdf

IJTSRD38067



## INTRODUCTION

As the current generation is getting developed, internet has become one of the most essential thing that every human needs now and then. With the invention of internet, life became more comfortable and ease. In today's generation, the technologies have reached to a great extent where internet is being used as a primary medium by each and every individuals to transfer data's, medias and information from one point to another across the biosphere. There are many transmission methods to transfer information using the internet via emails, facebook, whatsapp, etc which focuses on point to point transmission making the work to complete really fast and accurate.

But one of the main and major problems what we are facing during data transmissions and communications over internet is security threat. During these data transmissions, our sensitive information's gets intruded by third party in many ways. Therefore, it becomes a significant factor in safeguarding our medias during the transmission.

Taking this data security into consideration, as data security prevents unauthorized users/hackers from accessing one's files, many security techniques has been developed in recent times which includes cryptography, steganography and digital watermarking.

Steganography is a practice of hiding text message into an image file, audio file or video files for safe point to point data transmissions.

People often gets confused between steganography and cryptography. Both techniques are implemented to provide security for data transmissions but cryptography is a method which uses encryption and decryption phase in form of cipher text blocks. This cipher text generation gets differed depending on the algorithms we use such as AES, RSA, etc….

Whereas the Steganography techniques hides a text inside many media formats which ll be seen as a normal image, audio or video when a data transmission is done. So, if a person views the article, then he/she has no idea that there is a hidden text inside, therefore he/she won't indulge to decrypt the evidences.

### Existing system

For transmission of data from one point to another, many of us use cryptographic technique. This technique can be easily recognized and intruded by the middle men. Though crypto techniques provide security for data transmission, it can be easily gathered and our information gets leaked. It doesn't provide much security to the user until and unless a deep and more prominent algorithm is used. So to overcome from such existences, this STEGANOGRAPHY technique can be used.

### Problem statement

When it comes to data transmission, there arises a question "How to do secure transmission". In order to overcome this issue, steganography techniques comes into action which

hides our data inside several carriers such as image, audio or video files which becomes difficult for the the intruders to gain authorization.

**Proposed system**

The main aim of the paper is to introduce a technique to overcome unauthorized data access during point to point transmissions over the internet. This is achieved through Steganography technique which hides the text message inside an image. This modified image looks similar to the original image with no changes in its pixel quality and its size. The encrypted image shared via social medias or other formats shouldn't be noted that there is a hidden message embeded in it. By doing so, the act of stealing information can be reduced since the middle men doesn't recognize that there is a message hidden inside the image when he/she tries to intrude into it.

Past systems included lower embedding capacity and also quality of the image was very poor. So, this algorithm created a path for better image quality and embedding capacity. When it comes to atmost security, both data hiding algorithm and the image on which data is embedded should also be equally secured. Therefore, the security system is implemented in two layers, i.e the message that is to be hidden inside an image is encrypted using AES algorithm and this encrypted data is then hidden in the image. Again the image with hidden data is encrypted. Therefore, the person with the decryption key will have the full authorization to retrieve the secret message in its original form.

**AES algorithm**

The Advanced Encryption Standard is a symmetric cipher text block algorithm which is used to encrypt and decrypt the information for security purposes. It is considered as one of the safest mode, hence it is used in world wide standard. It is also known as Rijndael algorithm whose function is to take plain text in 128bit format and converts them into cipher blocks using keys of 128,192 and 256bits.

**Methodology**

The proposed topic includes two modules:

- Encrypt
- Decrypt

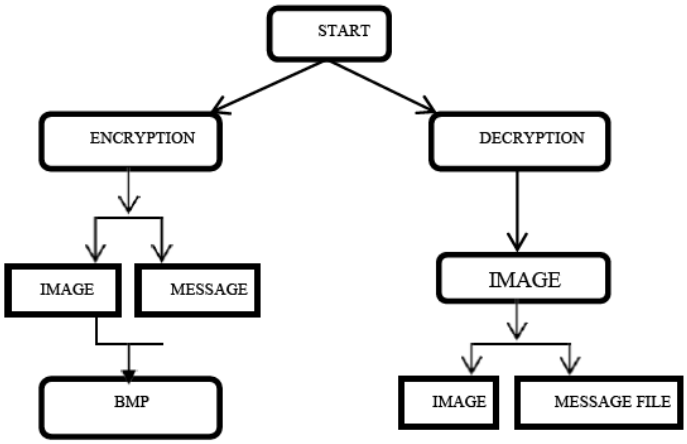
Where the user has to first open and run the application. Then the user has to select the image file in which he has to hide the text and transfer to the other end. Then he has to type the key format which is used to carry out the algorthim. Later the text message which he has to send it to the other end has to be typed in the required column

Once done, he/she will be given with two tabs – encrypt and decrypt.

In ENCRYPT options, the text message which he/she wants to transfer it to the other end will be embedded inside an image.

In DECRYPT mode, the other end user once he receives the encrypted image, he/she can decrypt the text image, save it to the required path and can view the hidden message.

**BLOCK DIAGRAM OF STEGANOGRAPHY**




**Conclusion**

This system provides at most security since the intruder doesn't know that there is a message hidden inside the image. Thus making him only to recover the image may be by using his practical familiarity.

In the generation of in advance information swapping by means of internet and World Wide Web, steganography has developed lifeblood tool for information security. Steganography can be ranked based on many ethics and one among them is positioned on the type of cover media.

**REFERENCES**

[1] Kolakalur, Anush, Ioannis Kagalidis, and Branislav Vuksanovic. "Wavelet Based Color Video Steganography." International Journal of Engineering and Technology 2016.

[2] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advanced in Control Engineering and Information Science, Dec. 2011, pp. 2767-2772.

[3] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes." Systems, Applications and Technology Conference (LISAT), 2015.

[4] Vidhya, P. M., and Varghese Paul. "A Method for Text Steganography Using Malayalam Text." Procedia Computer Science 46 , pp 524-531, 2015.

[5] Mstafa, Ramadhan J., and Khaled M. Elleithy. "An Efficient Video Steganography Algorithm Based on BCH Codes." 2015.

[6] Satpute, Snehal, et al. "An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding)." 2015.

[7] Jenifer, K. Steffy, G. Yogaraj, and K. Rajalakshmi. "LSB Approach for Video Steganography to Embed Images." International Journal of Computer Science and Information Technologies 2014.

[8] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE International Conference on Informatics, Electronics & Vision (ICIEV), May 2014, pp. 1-6.

[9] Bandyopadhyay, S. K., 2010. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in Technology

[10] S. Krishnagopal, S. Pratap, and B. Prakash, "Image Encryption and Steganography Using Chaotic Maps with a Double Key Protection", 4th International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing, Dec. 2014, pp. 67-78.