iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Information Security and Data Hiding

Kavita
M.tech Scholar, Department of Computer Science & Engineering
B. P. M. V Mahila Vishvavidyala Khanpur Kalan,Sonipat Haryana,India

Abstract: ***As the numbers of attacks increasing during transmission of information between the originate and target place, therefore need arises some secure methods which are free from different types of attacks. Two popular methods used for security purposes are Cryptography and Steganography. Both these methods transform data and information such that actual meaning of information is not visible. Hence these two methods provide integrity (correctness), confidentiality (privacy) and availability of information for indented recipients. In this paper, information security and data hiding system that is based on steganography and cryptography is proposed to secure data transfer between the source and destination. A LSB (Least Significant Bit) method is the easiest way of hiding information in an image and yet it is effective. The proposed system ensures the security of data being transferred.***
Keywords: Cryptography, Decryption, Encryption, LSB, Steganography

I. INTRODUCTION

Information Technology is the most essential aspect in today's world. Based on this fact computer application is still developing to handle securely the financial as well as the personal data more effectively. These data are extremely important from every aspect and we need to secure this from unauthorized access. Security is the process of preventing and detecting unauthorized use of data or computer or network. Prevention measures help us to stop unauthorized users from accessing any part of computer system. To achieve that security we may use various cryptography techniques. However, today data encryption is not everything or we cannot achieve strong security through this, we also need to secure the presence of date. Here comes the necessity of Steganography.

A. What is Cryptography?

It is the process of changing information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can understand the meaning of information. The cryptographic technique uses various types of algorithms which are generally impossible for unauthorized users to break.

Cryptography can be divided into following three categories depending upon the types of key used: secret key (symmetric) cryptography, public key (asymmetric) cryptography and hash functions. With Symmetric key cryptography where both the sender and the receiver share the same key for encryption of data. With Public-key cryptography, two different keys are used for encryption and hash function computes hash value of fixed length from the given data for encryption. It is impossible to recover the length of the original plain text from this hash value.

Figure 1 shows the basic concept of cryptography.



Fig. 1 Cryptography

©IJRASET: All Rights are Reserved

B. What is Steganography?

It is the process of hiding information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. As the message is not visible so it does not get any attention of unauthorized users which safeguard the secret message. This method of secret communication is also prevalent in ancient time where messages are written with some special ink etc. The modern Steganography uses different mediums for hiding secret information such as image, text, audio and video. Figure 2 below shows the basic concept of cryptography.

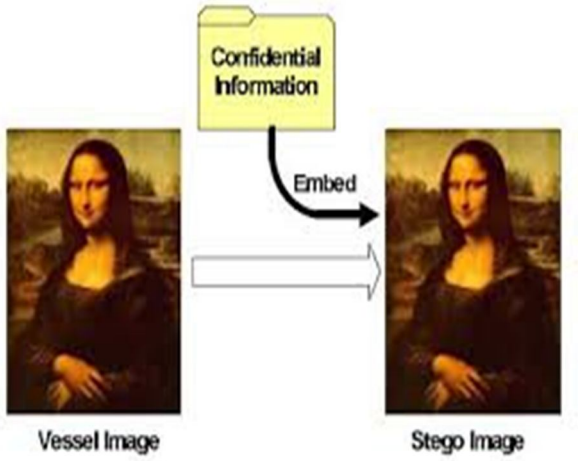


Fig. 2 Steganography

C. What is the Difference between Cryptography and Steganography?

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security

II. TECHNIQUES FOR INFORMATION SECURITY

A. Private Key Cryptography or Symmetric Cryptography

In private key cryptography, both the sender and receiver share the same private key. The key is used to encrypt the plaintext and also to decrypt the cipher text. The key must be kept private to ensure system security. A spy who obtains the key will likely be able to decrypt encoded messages. In the encryption schemes currently in use, keys are often either very large prime numbers or the product of large primes.A simple example, using a cipher that is not secure, should clarify the idea behind private key cryptography. Suppose Alice wants to send this message to Bob. “meet me at the roadhouse at noon urgent” For example, if Alice and Bob agree on a key of 5, the ciphertext of Alice’s message will be “meehannearotutetounrttasogmhdeoe” When Bob receives the ciphertext, he decrypts it using the private key, 5. First, Bob counts the number of characters in the ciphertext, which in this case is 32. Since there are 5 characters per row, based on the agreed-upon cipher and key, Bob realizes that the message is seven rows long—six full rows and onr row containing two characters. Bob writes out the message in row-formats as follows:

meetm
eatth
eroad
house
atnoo
nurge

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

nt

Writing the text horizontally row-by-row, Bob obtains meetm eatth eroad house atnoo nurge nt. Reading from left to right, Bob can determine the original message. If a spy knew the cipher and the private key, he or she could also decrypt the intercepted message.

B. Few Features of Private Key Cryptography are

1) Traditional private/secret/single key cryptography uses one key Shared by both sender and receiver if this key is disclosed communications are compromised

2) Also is symmetric, parties are equal Hence does not protect sender from receiver forging a message and claiming is sent by sender.

Figure 3 below shows private key cryptography.

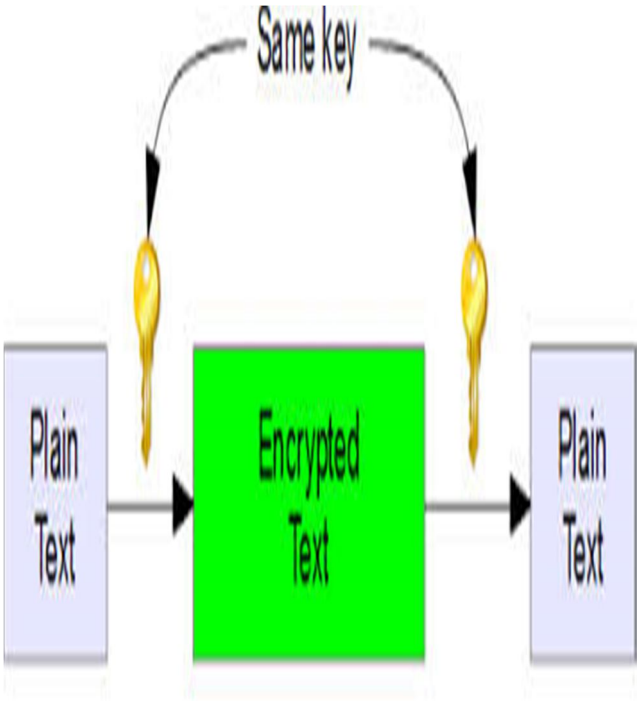


Fig.3. Private Key Cryptography

C. Public Key Cryptography or Asymmetric Cryptography

Another security issue is the problem of authentication. When Bob receives a message, how can he be sure that Alice sent it? That is, how can he be sure that the message is authentic? Private Key Cryptography allows two parties to exchange messages and maintain confidentiality but not authenticity. If the cipher text is intercepted, it will be difficult to decrypt without access to the private key and without knowing the encrypting cipher. Public Key Cryptography is useful for this purpose. In Public Key Cryptography one key is used to encrypt the plaintext and other key is used to decrypt the ciphertext. The important here is that it doesn't matter which key is applied first but that both keys are required for the process to work. Because a pair of keys is required, this approach is called Asymmetric Cryptography. Alice wants to sends the message to Bobs and she encrypted the message by using her private key. When Bob receives the ciphertext, he tries to decrypt it by using Alice public key which is available to everyone. If Bob can decrypt the message he know that it must come from the Alice, because Alice public key can only decrypt the message and encrypted by her private key and Alice know her private key. Notice that if Alice message had been intercepted, anyone could have decrypted it using her public key. Privacy is not provided by Public key cryptography only authentication.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Figure 4 below shows public key cryptography.

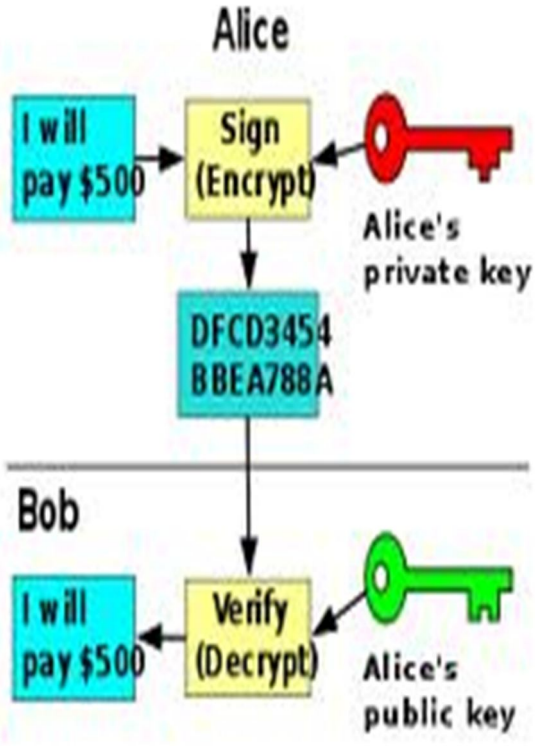


Fig.4 Public Key Cryptography

III. METHOD FOR INFORMATION HIDING

A. *LSB (Least Significant Bit)*

This method is the easiest way of hiding information in an image and yet it is effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in an image for example, the following steps would need to be taken

1) First load up both the host image and the image you need to hide.

2) Next choose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.

3) Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM- one byte per pixel, JPEG- one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: 10110011

4) Get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change the bits extracted now become the most significant bit

Host Pixel: 10110011
Bits used: 4
New Image: 00110000

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



Fig. 5 Least Significant Bit Method

Figure 5 above shows Least Significant Bit Method.
This method works quite well when both the host and secret images are given equal numbers of bits. When one has significantly more room than another, quality is sacrificed. Notice that the same technique could be used to hide sound or text inside an image. All you need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data; and of course, it is unlikely to survive lossy compression very well.

B. Encoding

LSB method allows large amount of secret information to be encoded in an audio file. Audio file contains set of bytes which can be used for encoding. Some audio files may contain several bytes depending on their sizes. The following steps were used during the encoding stage:

1) Encrypt the message using public key
2) Convert the audio file into bit stream
3) Convert each character in the message into bit stream
4) Replace the LSB bit of the audio file with the LSB bit of character in the message to hide.

C. Decoding

In this stage, the encoded file is decoded to get the hidden message. The message is decoded first and then decrypted by the public key that is known only by the authorized receivers or users of the proposed system.

D. Encryption

During encryption, the user is allowed to enter a password/key in any combination of numbers, symbols and characters. The key contains set of characters, which are used to encrypt the message before encoding.

E. Decryption

The user's password/key is supplied to decrypt the encrypted message in order to get the original message. The processes of encryption and decryption are handled by DES (Data Encryption Standard) algorithm.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Figure 6 below shows basic encryption and decryption.

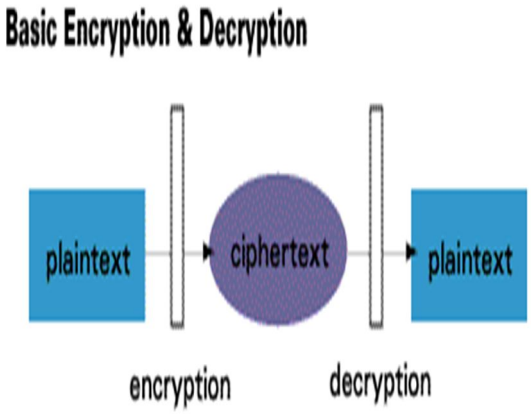


Fig. 6 Basic Encryption and Decryption

F. Use Case Diagram

Use case diagram represents the functionality of the system from the user's point of view. In Unified Modeling Language, use case diagrams are used to show the functionality that the system will provide and to show which users will communicate with the system in some way to use that functionality [6]. The use case diagrams for the encoding and decoding processes of the proposed system are shown below:

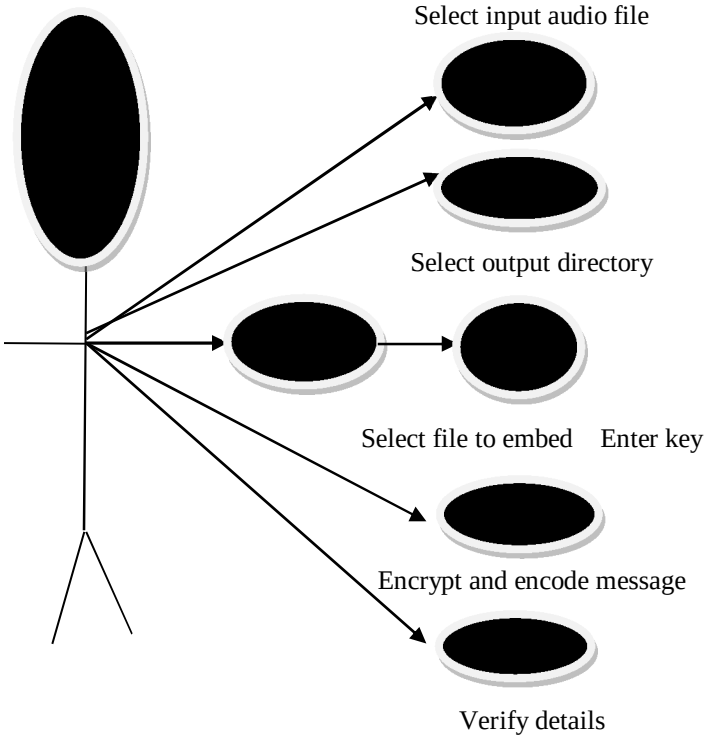


Fig. 7 Use case diagram for embedding/encoding

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

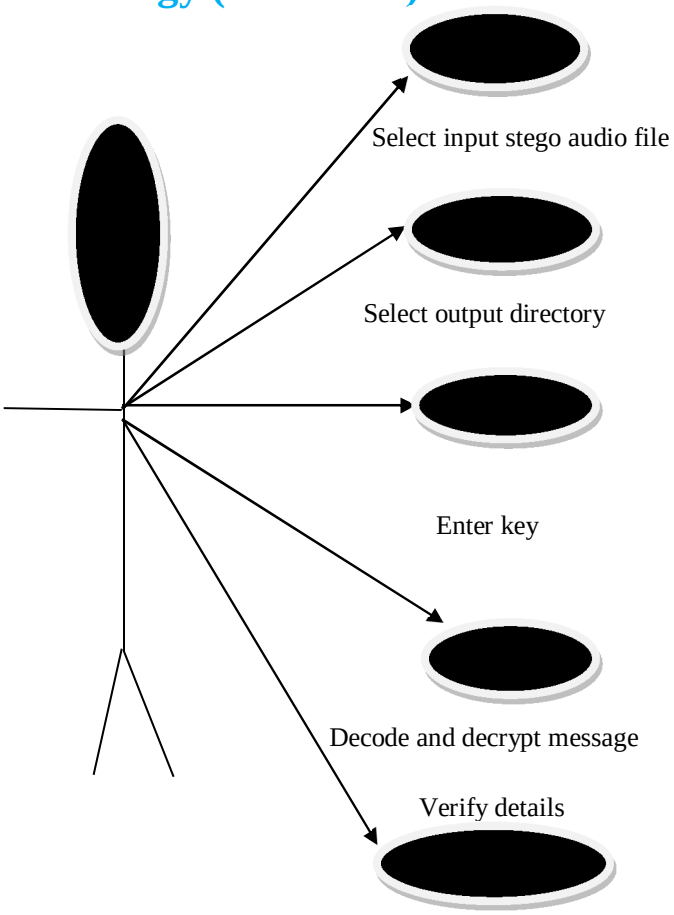


Fig. 8 Use case diagram for extraction/decoding

IV. APPLICATIONS OF STEGANORAPHY

A. *Secret Communications*

The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient.

B. *Feature Tagging*

Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

C. *Copyright Protection*

It prevents digital data from being copied by unauthorized user. The insertion and analysis of water-marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

V. CONCLUSION

In today's world, we often listen a popular term "Hacking". The unauthorized access of data being transferred on transmission medium is term as hacking. Steganography along with Cryptography provide some solution for this above mentioned problem. Cryptography is the process of changing information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can understand the meaning of information. It is the process of hiding information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can know the very existence of information. In this paper, information security and data hiding system that is based on Steganography and

©IJRASET: All Rights are Reserved

cryptography is proposed to secure data transfer between the source and destination.

REFERENCES

A. Journal Papers

[1] Raphael, A.J., and Sundaran, Cryptography and Steganography-A Survey, International Journal of Computer Technology Application, 2(3), 2011, 626-630.

[2] Doshi, Ronak, Pratik Jain and Lalit Gupta, Steganography and Its Applications in Security, International Journal of Modern Engineering Research, 2(6), 2012, 4634-4638

B. Books

[1] Greenlaw, Raymond and Ellen Hepp, In-line/On-line: Fundamental of the Internet and the world wide web-2nd ed. (CA, USA, Mcgraw-Hill, 2001)

[2] Wayner, Peter, Disappearing Cryptography: Being and Nothingness on the Net (Boston, AP Professional, 1996)

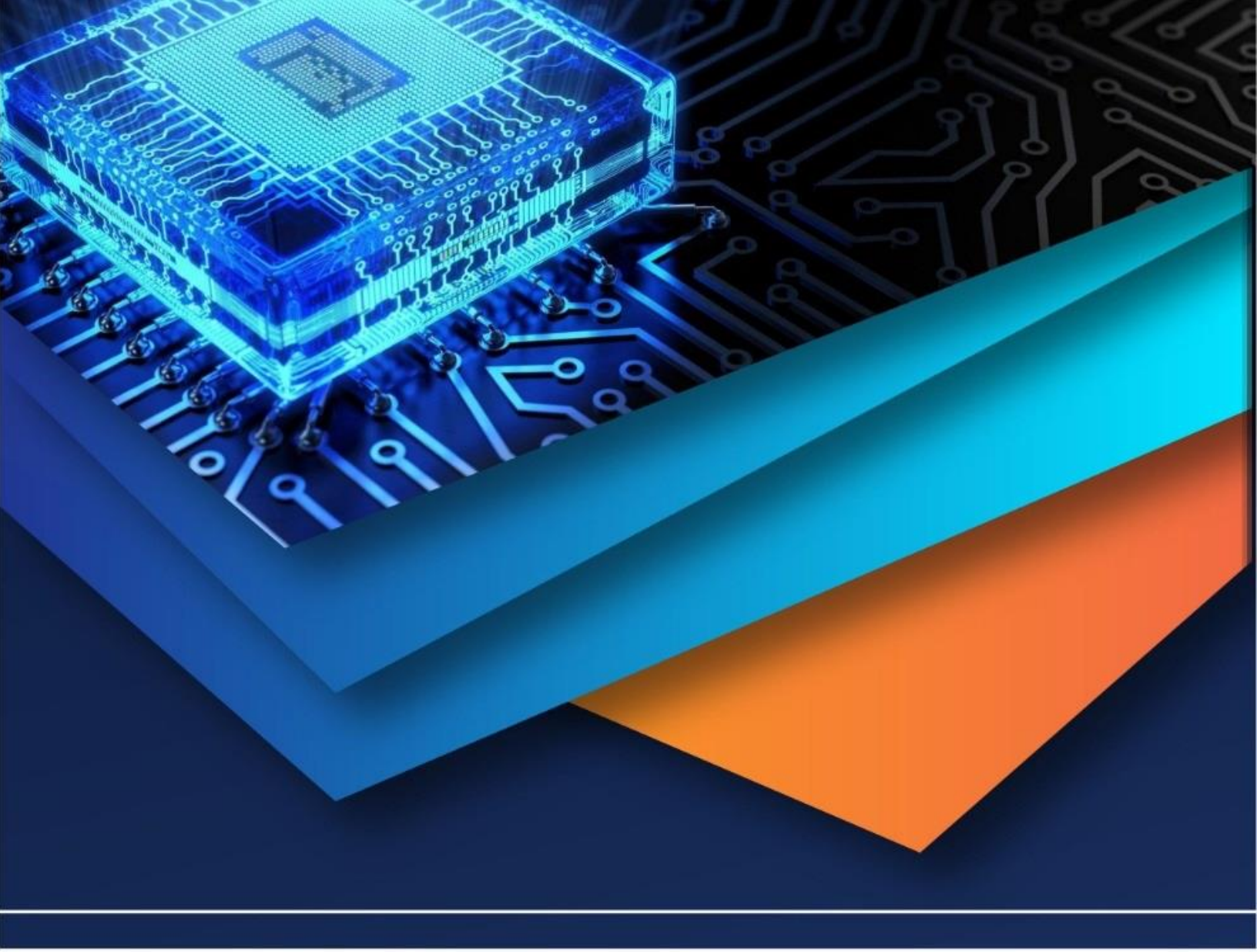
C. Proceedings Papers

[1] Johnson, Neil F., Zoran Duric and Sushil Jajodia, Information hiding: Steganography and Watermarking- Attacks and Countermeasures Volume 1 of Advance Information Security (Heidelberg, Germany, Springer Science and Business Media, 2001)

D. Thesis

[1] Jenita Kshetrimayum, A Secure Image Steganography Using LSB Technique and Pheudo Random Encoding Technique, National Institute of Technology, Rourkela, India, 2013.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)