iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VIII **Month of publication:** August 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

A New Approach to Provide Security to Audio Information Using Cryptography & Steganography

Mr. Sanket. N. Wawale[#1], Prof. Arindam Dasgupta[*2]

[#]*Department of Information Technology, Amrutvahini College of Engg, Pune University*

Abstract*— Information in any form is a very important resource for any organization or individual person. Due to research and new technologies it is possible to store and exchange information in different formats. Information can be stored and distributed through different medium such as text, audio, video, graphics, etc. Audio or sound medium is found to be used in many applications for providing security, voice commands, voice synthesis and entertainment. This project is an approach for providing security to audio information. This concept is based on Cryptography and Steganography. With the help of these two techniques, two levels of security is provided. Cryptography will convert the original data in different form and Steganography will hide one audio file into other audio file.

***Keywords*— Cryptography, Information Hiding, Steganography and LSB.**

I. INTRODUCTION

Every human being is having personal data that can used for identification or other purpose. Data which is related to an individual or other available information, e.g. name, address, telephone numbers, personal email addresses, date of birth, bank and payroll details, passport particulars, images, etc. It can also include data automatically collected when using computers and the internet. Personal Data and Commercial data both can be in Audio form due to advanced technology and multimedia. Personal data that may be related any system or individual such as audio Password, audio commands, etc. Commercial data, such as audio sound tracks for entertainment purpose.

Giving access to intended user and avoiding unintended access is a very difficult task. This Project is an approach for providing security for audio information. Unauthorized users may be harmful because they may try to reduce the effectiveness or take control of valuable resources by taking advantage of loop holes or drawbacks of these resources. For hiding secret information, there are number of different steganography techniques [6][9].

People want to exchange their confidential information or data , but they want to achieve this in a secure manner so that unauthorized person should not gain access to their data or even if someone gets that data, it will be difficult for that person to recognize and fetch out information. One of the possible solutions as cryptography to encrypt or decrypt data and steganography to hide data in different carrier media files like image, audio, video, etc.

II. LITERATURE SURVEY :

Steganography consist of study and science of hiding communication and important data. A steganography system puts secret content in some part of cover media so that an unauthorized user should not be able to track or identify that their is secret data. In ancient days, people used pictures or different kind of medium to send secret information. Today technology provide efficient and easy to use communication channels and storage for steganography [1]. The information hiding is done in a steganography system by identifying a cover medium's data bits that are repeated (those that can be modified without affecting that medium or distorting it). The embedding process creates a stego medium by replacing these bits with data or message [7]. The objective of

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

steganography system is to keep the presence of the message undetectable from an unauthorized access.

A. *INFORMATION-HIDING SYSTEM FEATURES*

Any information hiding system is based on three aspects capacity, security, and robustness. *Capacity* is concern about the amount of information that can be hidden in the cover medium, *Security* refers to an unauthorized users inability to detect hidden information, and *robustness* refers to the amount of modification the stego medium can handle before showing any negative effects or destroy secret information [5].

B. *RELATED WORK –*

AUDIO CRYPTOGRAPHY:- In this method the audio data is divided into two or more parts called as shares. Each single part does not convey any meaningful information, but when all parts or shares are combined together they will reveal the original audio data [2].

Pros- If any unauthorized user plays one part in an audio player, he or she will only hear meaningless hiss sound, or irritating noise sound. But when all parts are mixed and played together, i.e. using an audio editor, the original audio comes back.

*ECHO HIDING :-*An echo is generated and added in a signal by manipulating the parameters (initial amplitude, decay and offset) such that the echo is not audible. If we consider a signal f(t), an echo f(t-dt), with some delay can be added to produce the stego signal s(t)=f(t) + f(t-dt). Figure 1 represents the same [3].

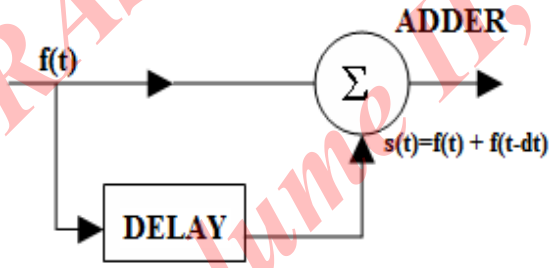


Figure 1: Echo Hiding

III. TWO LEVELS OF SECURITY:-

This system uses Two levels for providing security, so that it should not be easy to detect or access the sensitive data.

A)CRYPTOGRAPHY:-

Cryptography is the process of making or converting sensible data into a different form.

B) STEGANOGRAPHY:-

Steganography is the process of Hiding the data into another media file.

Steganography and Cryptography are two different techniques. Cryptography involves converting the message so as to make it meaningless to unauthorized people who had tracked or received it. In cryptography, the system is not broken until the unauthorized user can read the secret message. Breaking a steganographic system needs the unauthorized user to detect that steganography has been used and he is able to read the embedded message. Steganography provides a means of secret communication, which cannot be removed without changing the data in which it is hidden [10]. The security of steganography system depends on the strength of the data encoding system.

Using Cryptography and Steganography together provides an approach for adding multiple layers of security. By combining, the data encryption can be done by a using certain techniques and then hide the cipher text in an audio media. Using these two methods will increase the security of the secret data. The requirements such as capacity, security and robustness for secure data transmission and storage can be fulfilled by using these two techniques together [8].

IV. PROPOSED SYSTEM

This system uses XOR operation for cryptography. And Least Significant Bit(LSB) algorithm for Steganography.

A) *LEAST SIGNIFICANT BIT (LSB)*

This system uses two least significant bits in some bytes of the cover file to hide a sequence of bytes containing the secret data [4]. LSB coding is the simple way to hide information in a digital audio file by replacing the least significant bit of each byte with a secret message. The least significant bit (LSB) is the bit position in a binary

integer giving the unit value similar to unit value in decimal. The LSB is also referred to as the right-most bit.

B) SYSTEM ARCHITECTURE AND MODULES:-

This system consist of two main modules hiding and unhiding which contains submodules. These submodules perform the task of hiding the MP3 audio file into a Wave file and extracting the original MP3 from the Wave file as shown in figure 2 and 5.

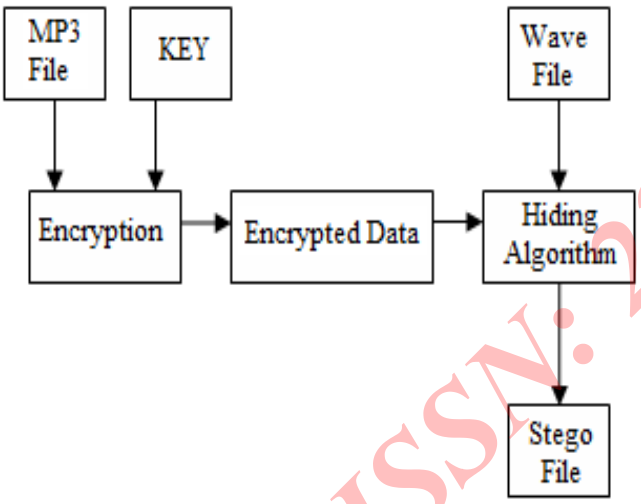


Figure 2: Hiding Process

HIDING SECTION

1) BYTE EXTRACTION:

This module provides the data from both the files (MP3 and Wave) in byte form (8 bits). The entire operation is performed at the bit level, so this module provides the data in bits form to other modules for processing.

2) ENCRYPTION:

This module converts the binary MP3 data into un-meaningful binary data. This is achieved with the help of a key. The Encryption module performs an XOR operation between original MP3 data and the key provided by the user as shown in figure 3.

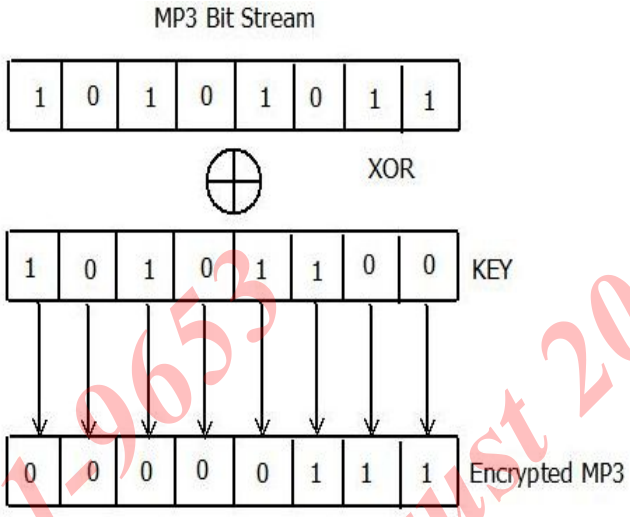


Figure 3: Encryption Using XOR Operation

3) HIDING

The function of this module is to hide the data. After the data is encrypted the hiding module hides the encrypted MP3 data in a Wave file. For this purpose a different version of LSB algorithm is used. Two bits of encrypted MP3 will be hidden in two LSB bit position of the cover Wave file as shown in figure 4. After hiding all the Encrypted MP3 bits the hiding module generates a single Wave File but MP3 file is hidden in it.

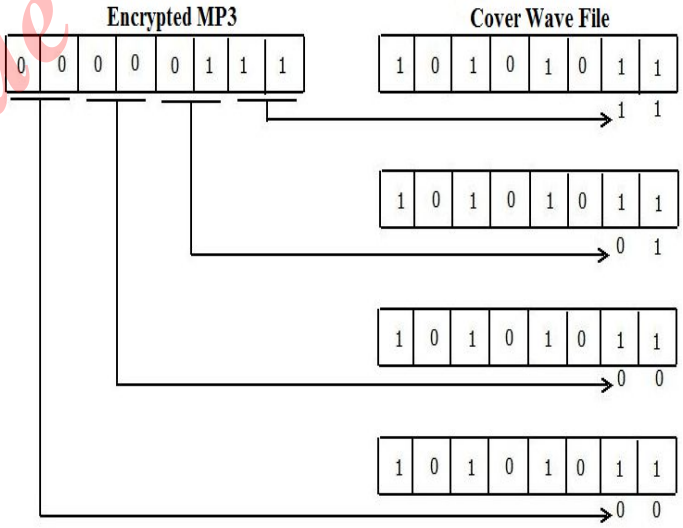


Figure 4: Hiding using a modified LSB algorithm

UN-HIDING SECTION

1) EXTRACTION OF MP3

The function of this module is to extract the encrypted MP3 data from a WAVE file. This module uses a Reverse LSB algorithm to fetch out the MP3 Bits from a Wave File (Stego File).

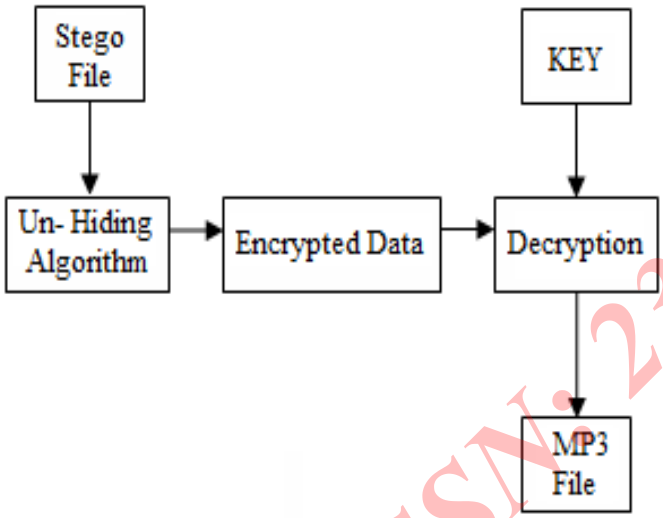


Figure 5: Un-hiding Process

2) DECRYPTION

The function of this module is to construct the original MP3 data again from the encrypted MP3 data which has been extracted from the Stego Wave file. For this purpose a user needs to enter the key. The algorithm performs XOR operation between the encrypted MP3 data and the Key provided by the user. And the original MP3 file will be generated.

V. ALGORITHM

A. Hiding Algorithm:

1. Start

2. Select the Mp3 file which you want to hide

3. Convert the Mp3 into its binary form

4. Get the key from user.

5. Convert key into binary form.

6. Take byte of Mp3 and key perform XOR operation between these two bytes.

7. Repeat Step 6 till the end of file.

8. Select the Wave file as cover File

9. Check if wave file is 4 times greater than mp3 file.

10. If no then go to Step 8.

11. Else Convert the Wave file into Binary form

12. Replace two LSB bits from byte of Wave file with two bits of encrypted Mp3.

13. Repeat Step 12 till the end of Mp3 file.

14. Stop

B. Un-hiding Algorithm:

1. Start

2. Select the Stego file which you want to Un-hide.

3. Convert it into Binary form.

4. Get the key from user

5. Convert it into Binary Form.

6. Extract two LSB bits from byte of stego file and save them in memory.

7. increment the Byte pointer of Stego file.

8. Repeat Step 7 and 8 till the size of mp3 file has reached.

9. Take byte of encrypted Mp3 data and perfom XOR operation with the Binary key.

10. Repeat Step 9 till the end of Mp3 file.

11. Stop

VI. MATHEMATICAL MODEL

X = Total No of bits within data section of wav file which we can manipulate.

ISSN: 2321-9653

Y = Total No of bits in MP3 file.

x = 8 bits of mp3 file.

z = 4 byte of wave file.

K= 1 byte of data.

Ψ = X/(Y/2)

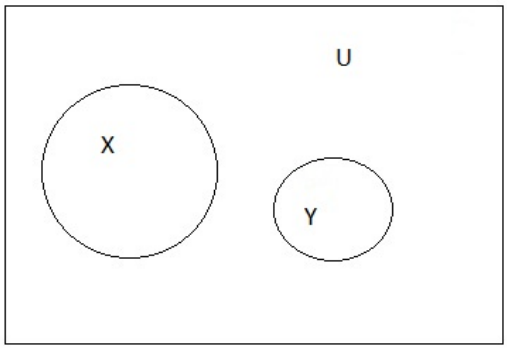


Figure 6: Set Theory Before Processing

For Encryption-

$$\text{Enc(mp3)} = \sum_{i=1}^{K} mp3_i \oplus key$$

For Hiding-

$$\text{Hide(F)} = \sum_{i=1}^{\Psi} z_{4i} Fn(x_i)$$

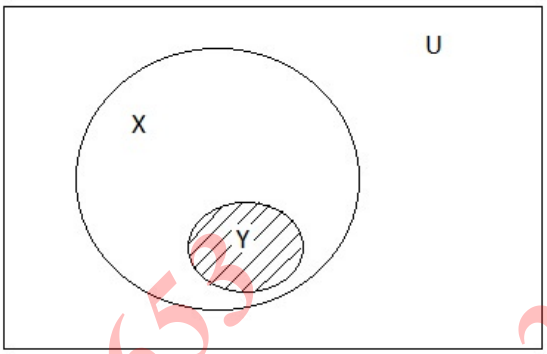


Figure 7: Set Theory After Processing

VII. RESULTS AND DISCUSSION

1) The original Wave file before hiding the MP3 content and the Wave file after hiding the MP3 content (stego file) are having same size.

2) The MP3 file generated after un-hiding process is having the same quality and same size as that of an original MP3 file before hiding.

The Cover wave file with different sample rates were used for testing purpose. But their were not any adverse effects due to change in sample rate. The original MP3 can be securely and properly extracted from the stego file. One thing that is observed in this process is , if the contents of wave file are modified then a hiss sound gets added for a short duration.

TABLE I: TEST RESULTS : HIDING PROCESS

Sr. No	Cover Media (Input)	Cover Media Size	Cover Media Sample rate	Secret Message (Input)	Secret Message Size	StegoFile (Output)	Stego File Size
Test1	NFS1.wav	3,099 KB	44,100 Hz	Secret1.mp3	361 KB	Stego1.wav	3099 KB
Test2	NFS2.wav	3,373 KB	48,000 Hz	Secret1.mp3	361 KB	Stego2.wav	3,373 KB
Test3	NFS3.wav	6,745 KB	96,000 Hz	Secret1.mp3	361 KB	Stego3.wav	6,745 KB

TABLE II: TEST RESULTS : UN- HIDING PROCESS

ISSN: 2321-9653

Sr. No	StegoFile (Iutput)	Stego File Size	Stego File Sample rate	Recovered Mp3 file after Un-hiding	Recovered Mp3 file size
Test 4	Stego1.wav	3099 KB	44,100 Hz	Decoded1.mp3	361 KB
Test 5	Stego2.wav	3,373 KB	48,000 Hz	Decoded2.mp3	361 KB
Test 6	Stego3.wav	6,745 KB	96,000 Hz	Decoded3.mp3	361 KB

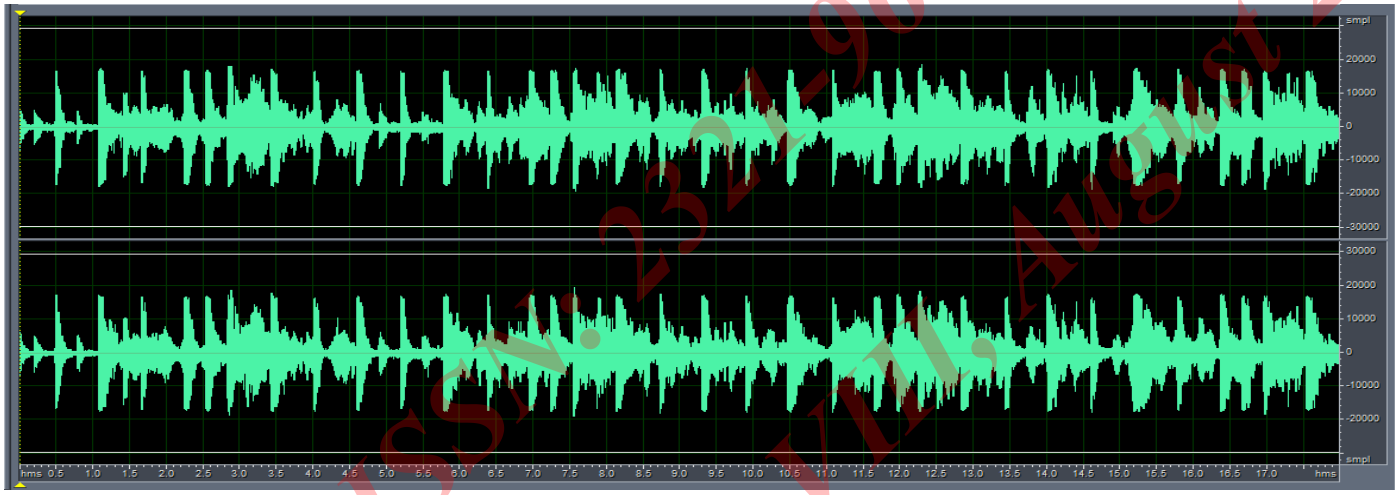


Figure 8: Original Cover Wave File

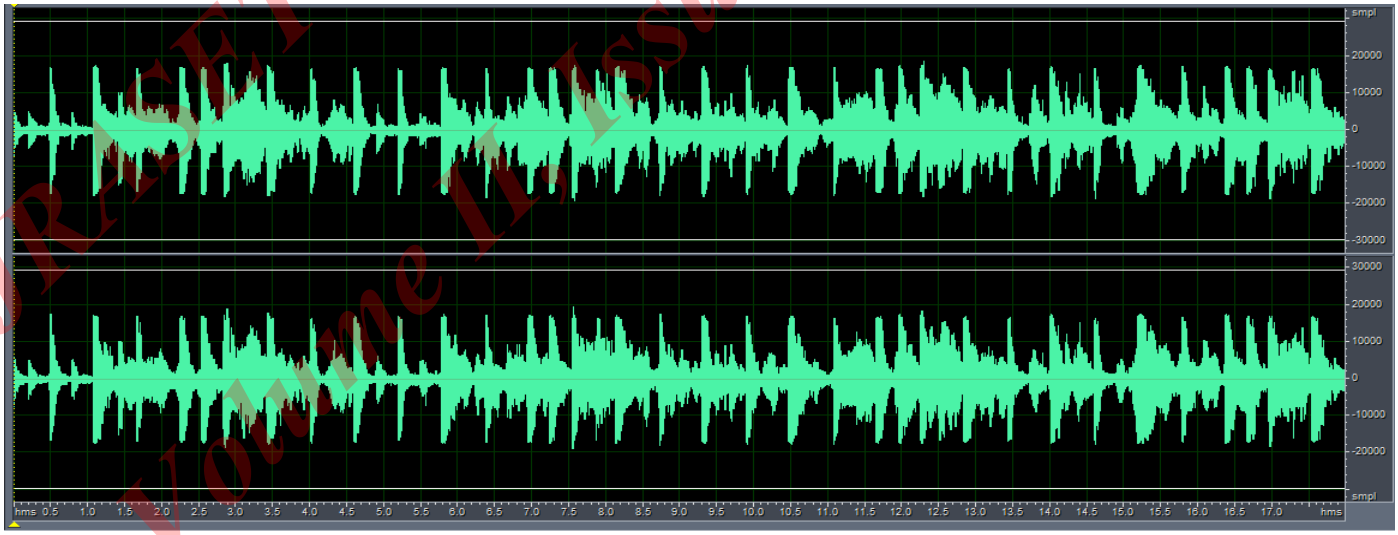


Figure 9: Stego Wave File

VIII. CONCLUSION

A different approach is introduced through this project for securing audio data. This technique has been used to meet information hiding system features like robustness to attacks, the data-capacity of the cover media and the inability of un-authorized user to detect the stego media which can be used in various applications. Cryptography is used as an additional security layer over information hiding.

ACKNOWLEDGEMENT

This work is implemented under the guidance of Prof. Arindam Dasgupta. His active guidance and valuable suggestion at every time encouraged me to carry out the same.

REFERENCES

[1] Abikoye Oluwakemi C, Adewole Kayode S. , Oladipupo Ayotunde J. December 2012 – "*Efficient Data Hiding System using Cryptography and Steganography*" International Journal of Applied Information Systems (IJAIS) ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4 No.11.

[2] Amresh Nikam, Poonam Kapade, Sonali Patil. 2010-*" Audio Cryptography: A (2, 2) Secret Sharing for Wave File".* International Journal of Computer Science and Application ISSN 0974-0767.

[3] Dr D Mukhopadhyay, Fellow A Mukherjee, S Ghosh, S Biswas, P Chakraborty. November 2005. *" An Approach for Message Hiding using Substitution Techniques and Audio Hiding in Steganography"*- IE(I) Journal-CP-Vol 86.

[4] Jayaram P, Ranganatha H. R, and Anupama H. S. 2011. " *Information Hiding Using Audio Steganography – A Survey"*. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[5] Lin T. and Delp J, "*A Review of Data Hiding in Digital Images,"* Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274-278, 1999.

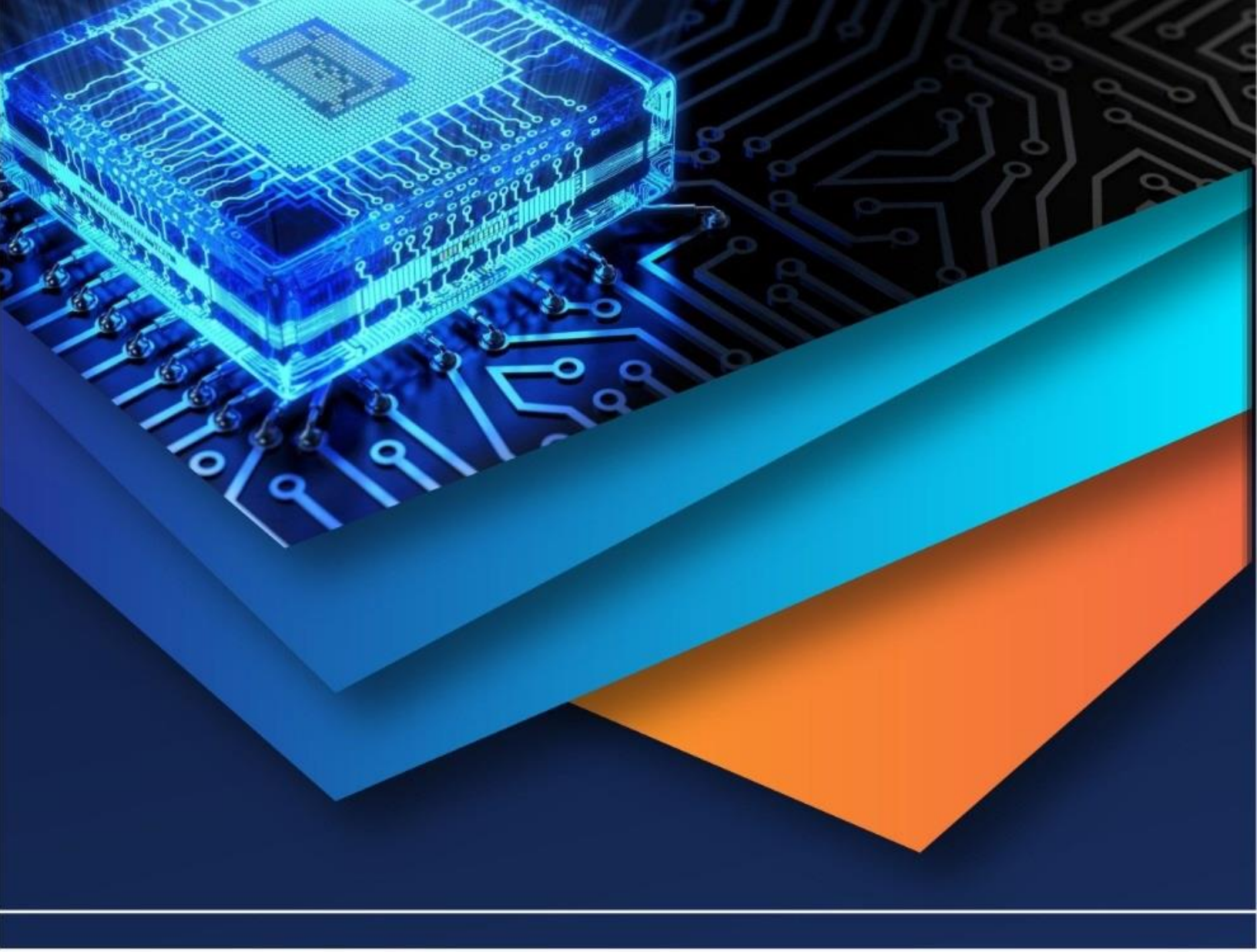
[6] Mohammad A. A, and Abdelfatah A. Y. 2010. " *Public-Key Steganography Based on Matching Method*". European Journal of Scientific Research, 40(2). ISSN: 1450-216X. Euro Journals Publishing, Inc., pp. 223-231.

[7] Niels P, and Peter H, 2003," *Hide and Seek: An Introduction to Steganography"*. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.

[8] Raphael A. J, and Sundaram V. 2011. " *Cryptography and Steganography - A Survey"*. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

[9] Sujay. N, and Gaurav P. 2010. *" Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions"*. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.

[10] Vivek. J, Lokesh. K, Madhur. M. S, Mohd. S, and Kshitiz Rastogi 2012. *" Public-Key Steganography Based on Modified LSB Method*". Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY