iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6151

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Steganography Data Hiding Technique

Satyam Mishra[1], Ms. Deepica S. Dominic[2]
[1]*School of Computing Science and Engineering, Galogotias University, Greater Noida, UP, India*
[2]*Assistant Professor (SCSE) Galgotias University, Greater Noida, UP, India*

Abstract: ***Steganography is a common term used for all methods for the inserting of extra secret content into some form of carrier, with the aim of securing of the introduced alterations. Now a days the art of transfer the secured information has got more observation and challenges. So, different techniques have been proposed for data hiding in different fields like LSB, RABS and others. This paper provides an analytical aspect of different existing techniques/methods of steganography where one of these is hiding of information on the bulletin board display. It uses the LSB technique over here. These methods can be further used to other means such as stadium, railway station or airport and other public places and even for officials. It also gives the overview of the methods like Watermarking, steganography-cryptography system which will be discussed.***
Keywords: LSB, RABS, cryptography, steganography, watermarking, bulletin board.

I. INTRODUCTION

As the use of technology and its work in all fields is increasing day by day the problem of data security has also become a great challenge for humans. Since a long-time people did and are even doing great work for introducing creative methods for secured communications that are described as RABS (Rule based Adaptive Batch Steganography) which tries to conceal the huge amount of confidential information in a concealed image set very fast. Another is its different colour models which are altered in their energy contributing in ach sub matrix of wavelet decomposition when the algorithm is applied.

Further techniques discussed in this paper are steganalysis which attempts to ruin the steganography by detecting the hidden information and extraction, steganography-cryptography system where the message is first transformed into indecipherable code and then this code is inserted into an image file which provide encoding and data hiding both. As we know that now all experts are using the steganographic techniques in combination with the other different methodologies of data security, which in result has upgraded the level of technology considerably. In addition to that, usage of the secret transmission of message between two parties, prevention in making of illegal copies steganography has increased its applications in overall.

At the time of 2nd World war and after that period undercover agents used pictorially produced dots for message transmission. The dots were inserted in paper which was visualized by receiver in focus light. It shows that steganography was used in some or the other way since long.

One of the protocols that is used in steganographic techniques is the public key rule which helps in allowing two different group of people (who have not ever communicated), to transmit information over a public channel

Steganography is acquired from the Greek for secured writing and essentially means “to be hidden in the plain sight”. The main aim is to alter the carrier media in such a way so that it cannot be perceived easily means neither the inserting of message data nor the inserted message data can be checked. Another definition of Steganography is that it securely conceals the data inside other data. Steganographic techniques wants to be particular and sure enough that no unauthorized receiver is not able to depict the carrier of steganographic medium that is having the hidden data. Uncomplicated steganographic methodologies have been used for a long time period, but with the huge amount of usage of files in any e-doc type new techniques for data in message hiding has come into picture.

Table I. Contrasting Data Transfer Methods

Data Transfer Methods	Privacy	Unification	In-removability
Encrypting	Present	Not Present	Present
Digital Sign	Not Present	Present	Not Present
Steganography	Both	Both	Present

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Above Tabular representation shows depicts the contrast in data transfer. Here the encrypting method gives us a secure talking medium which requires a private key for reading the message. Any sort of intrusion can't destroy the effect of encryption but comparatively it is simple to alter the message which makes it difficult for any other to decode.
Technically plenty rules are there and different embedding methods which permits us for concealing information in some object. But all varieties of protocols and methods should complete the no. of requirements so that steganography can be used efficiently.

Here we have a list of crucial requirements that the steganography techniques must be satisfying:

1) The probity of hidden data after being embedded in the steganographic object must be maintained efficiently.
2) The steganographic object should retained to the human vision throughout.
3) In the watermarking, updation in stego object must have no change on watermark.
4) At last, we have to assume that the attacking person knows that there is hidden data in the steganographic object.

II. BASIC STRUCTURE

This figure (i) shows a simple view of the general inserting and retrieving method in steganography. Here we are having a secret image that is being set in a cover picture to give steganographic image. Initially in inserting and hiding data we move both secret and cover message into encoder. Where one or the other rules will be applied to embed the unaccessed data into the cover data.

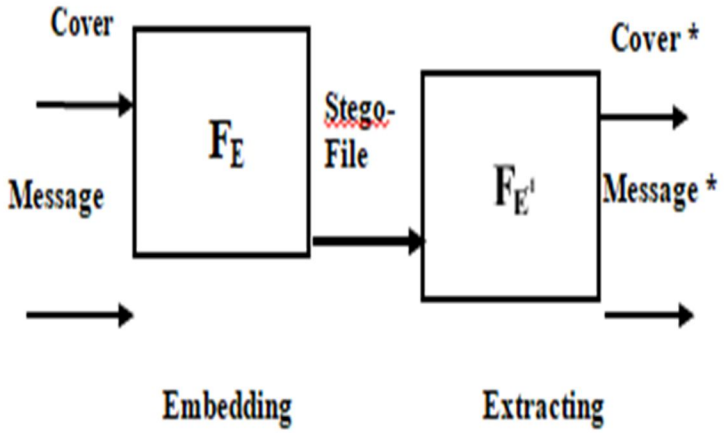


Fig. 1. Steganography Method

After getting the steganographic object, it will be delivered off through any transmission source medium like, mails to the particular receiver for decryption. A receiver should decrypt the steganographic object for visualizing the concealed data. One should know that the decrypting method is just the opposite of encrypting method. It can be understood as a retrieval of concealed data from steganographic object.
In decrypting method, the steganographic object is placed within device. The public/private key that can decrypt the real key which is applied in encrypting method is required so that the concealed data can be decrypted. After completing this, the steganographic object can be viewed.

III. STEGANOGRAPHY TYPES

It is of 4 types:

A. Audio
B. Image
C. Video
D. Text

But text steganography is most difficult out of these due to lack of redundancy.

Now we compare the different methodologies of steganography in tabular form.

Table II. Contrasting Different Steganographic Methods/Techniques

SR. NO	VARIOUS METHODS	MEDIA	INSERT PROCESS	MERITS
I.	Combination of two files	File	Watermark inserted by updating the code that do not affect file implementation.	Simple implementation
II.	Textual matter	File	Insert data in a file we can simply alter some of its features.	Alterations cannot be seen by human eye
III.	Picture Hiding: a) LSB- Least Significant Bit	Picture	Performs by usage of LSB of each pixel in 1 image.	Simplest method of picture hiding
	b) DCT -Direct Cosine Transform		Insert data by changing transform DCT co-efficient.	Provides robustness
	c) DWT-Discrete Wavelet Transform		Works with taking wavelets to encode full image	Wavelets co-efficient are changed with noise.
IV.	Audio method	File type of MP3	Encoding message in an order which sound as type of unwanted high volume.	Applied in watermarking by combining with thin bandwidth of the inserted data to the big bandwidth of media.
V.	Visual Method	File type of MP4	Cluster of audio and visual method.	Large database storage capacity.

IV. STEGANOGRAPHY VS CRYPTOGRAPHY

As we know that both cryptography and steganography are used for the concealed transmission of data. But in overall steganography is differentiable from cryptography. Cryptography prevents the data from unauthorized people, but steganography even hides the presence of the data. In case of cryptography, the system is damaged when intrusion takes place but for destroying a steganography system the intruder needs to check the presence of steganography first.

Table III. Steganography and cryptography comparision

SR. NO.	STEGANOGRAPHY	CRYPTOGRAPHY
I.	Cover message	Secret message
II.	Secret communication	Data protection
III.	Used for audio, video, image, text	Used only for text files
IV.	No integrity	Integrity
V.	No change	Changed on transmission

We can also unite both these methods by encoding the data using cryptography and concealing the encoded data using steganography and the resultant can be sent by keeping its secrecy.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

V. STEGANOGRAPHY VS WATERMARKING

Steganography focuses to the level of undetectability but the watermarking technique provides maximum of its behaviour to the strong security of the information and its capacity to manipulate the working on it, like the picture functioning, aural functioning in the case of picture and aural files that are processed for watermarking simultaneously.

It is the reality that rationality of a watercraft with an initialised information is the changeability purpose of the algorithm over the watercraft.

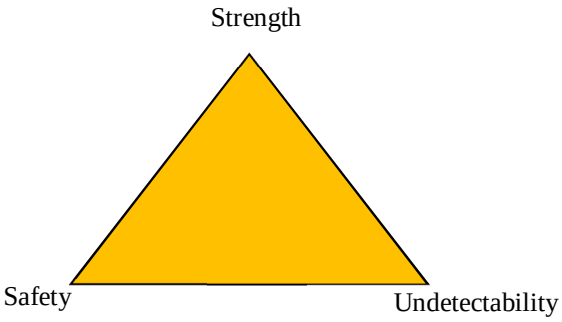


Fig. 2. Features

This is how the algorithm changes the watercraft and the importance of such manipulation regulates with no doubt the captivity of message, since captivity is the responsibility of data features divergence from the set standard, inserting operation attitude and alter intensity of such alteration confirms the watercraft data captivity.

The triangular representation shown over here gives us the message of undetectability and strong security. Undetectability is an evaluation of significance of the data of the message within the watercraft.

VI. RABS

A. Rule-based Adaptive Batch Steganography

Having known the concealing ability of picture, we can insert in the picture a section of concealed message where its size is less than or equal to the concealing ability of picture. The left-over exposed part of concealed message can be covered in any other cover pictures. We focus to upgrade the unreadability of steganographic data while using the cover pictures efficiently.

In addition to that, RABS attempts to protect a huge amount of concealed message in a concealed picture section very fast. Unlike static batch steganography, it is quite empirical and pragmatic to make some expectations before performing the operation.

B. Expectations

1) The steganographic expert is having the authority to choose the concealed picture from picture index.
2) Bulk of confidential information is irregular.
3) No. of concealed picture in concealed picture segment is irregular.
4) The recipient knows the technique of steganographer for disintegrating the draft into segments and the sequence of steganographic data.

Here, stego expert can choose concealed picture in an arbitrary way from the index. In RABS, firstly the steganographic capability of concealed picture is evaluated using ‘Sign of Clean Images’ and then inserting algorithm is applied for execution.

VII.LSB

A. Least Significant Bit

Simplest method of inserting any message in picture. The idea behind this method is that if we change the last bit value of a pixel there won’t be large change in colour and so it inserts the bits of the data straight into LSB plane of secret image in an order.

Manipulation of least significant bit not results in change of individual percept as magnitude of the alteration is small. Here, the embedded ability is upgraded by 2 or extra LSB.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

VIII. PROPOSED WORK

Steganographic techniques aims to alter the carrier media in such a way so that it cannot be perceived easily means neither the embedding of message data nor the embedded message data can be checked. (like picture shown by computerized bulletin board). Usage of these kind of techniques can be seen in crowded area. So, we analyzed that this is a sort of steganographic technique, but is done in actually computerized on the screen of a device like bulletin board. This is a schematic representation of inserting secured data within a concealed medium.

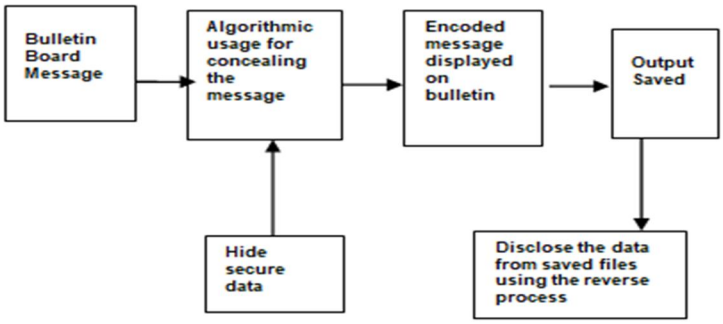


Fig. 3. Schematic representation of method

1) Transfer the common message that is to be shown on bulletin board.
2) By applying any particular algorithm conceal the secured message into the common message before transferring it to the bulletin board.

Methodology described over here can be utilized for creating any sort of announcement containing any confidential message in general area. Can be further used to other means also like around restaurant, stadium, etc.

A. Stepwise Procedure For Performing Above Described Technique Is Given

1) Firstly, go through the origin of the picture.
2) Now distribute the image into (X x Y) small blocks. Where X & Y are the 1st & 2nd bytes of the key **(Figure 4).**
3) The LSBs of element are altered which depend upon design segment and data segment.
4) The design segment is taken in sequential form of itsmost significant segment.
5) If the design segment is null, then the 1st unimportant segment of the element is changed otherwise it remains same.

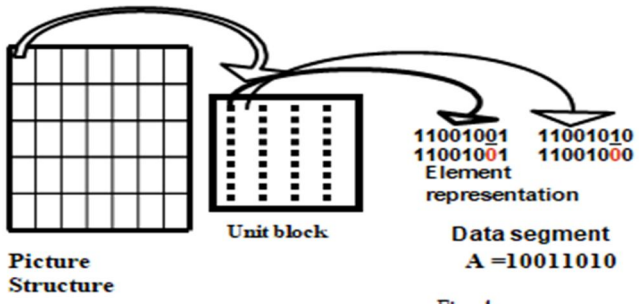


Fig.4. Distribution

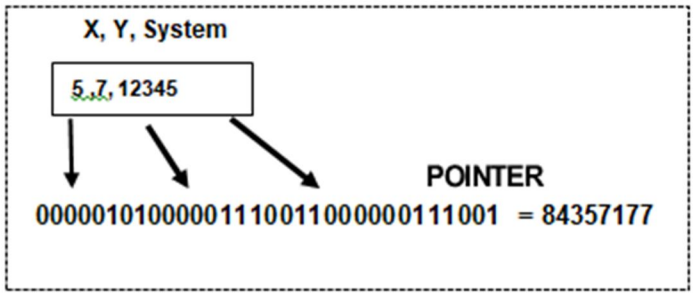


Fig. 5. Pointer Generation

6) If the system segment is 1, then the 2nd most unimportant element is changed according to it.
7) Single segment of secured data message is distributed all over the block.
8) In the same way other bits are inserted in the left-over blocks.
9) Now if the length of secured data message is large, then it can be distributed and saved in more than two structure.
10) For the retrieval of data, steps opposite to that of inserting are processed.
11) The data obtained over here is just based on a theory but can also be applied practically.

Pointer over here plays a very vital role in embedding the message. Larger the pointer size, more it will be challenging to inspect the confidentiality. Above figure shows the pointer generation. The first 8 segment shows the no. of rows X & the next 8 segment shows the no. of columns Y.

B. Execution Assessment

Execution assessment relies on success rate of execution of the full system wrt following measures:

1) The probity nature of confidential information must not alter post inserting.
2) Steganographic object should be viewed in same way as earlier by the naked eye.
3) Retrieved data should have correctness.

IX. RESULT

For showing online data transfer, 3 set-ups are used:

A. Generate and send the general bulletin board data.
B. Conceal the data message.
C. To show any data coming from 2nd set-up.
D. 4 approaches are described below by the help of pictures:

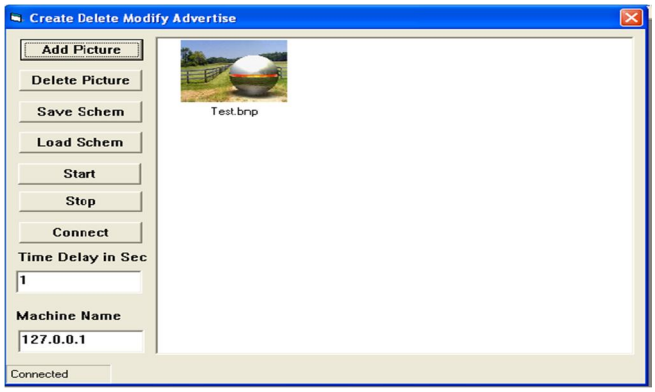


Fig 6. Set-up for generate, alter, remove

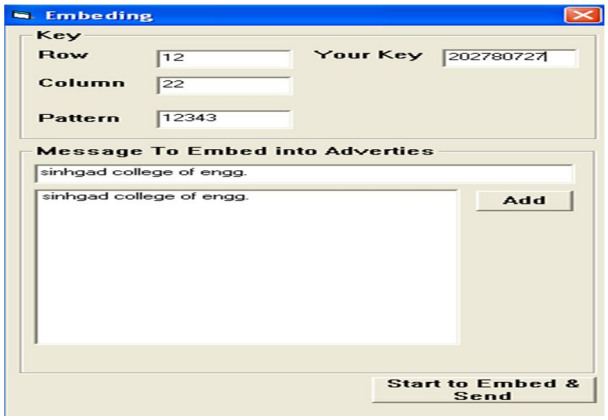


Fig 7. Set-up for inserting data of message

Fig 8. LCD Display

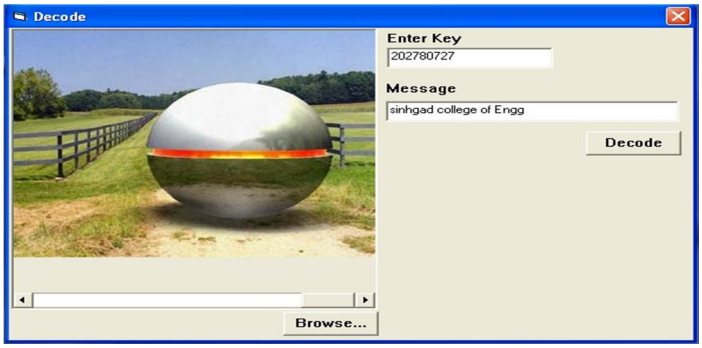


Fig 9. Set-up for decoding

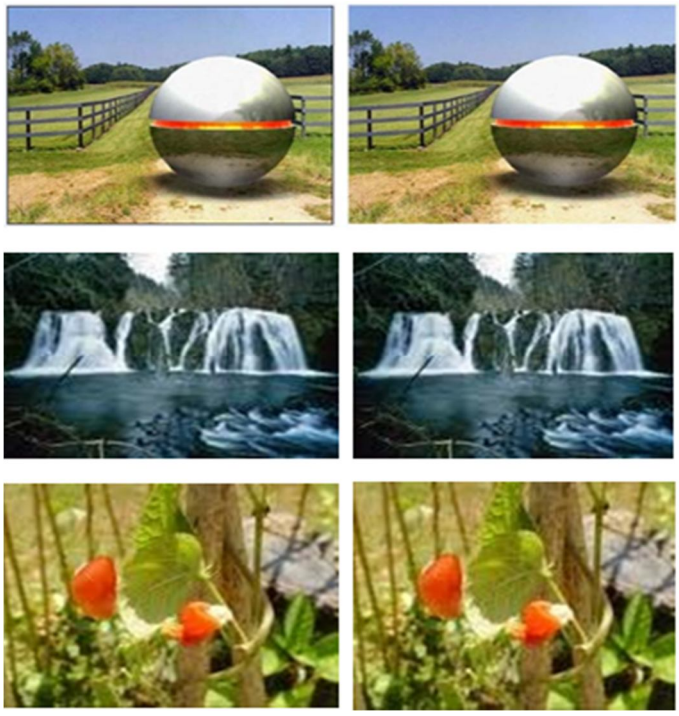


Fig 10a. Real images Fig 10b. Steganographic images

Set-up 1 (generate, alter and remove) is particularly used for generating a database for the bulletin and send it to the 2nd set-up, where the concealment of data is taking place. The steganographic image from the 2nd set-up is then sent to the display on bulletin board. This image is then clicked by the camera & the decryption module decodes the given data. The results shown here consist of the image that is particularly saved on to the device.

X. CONCLUSION

However, we have many benefits of internet but it has takeover the confidentiality through the unauthorized access of attackers. Different methodologies are being created to solve the problems being faced in the field of technology. Among these data security by the help of internet is becoming very useful and efficient day by day. Watermarking, LSB, Cryptography are some the common and popular techniques of steganography. We must clearly know that the steganographic techniques does not change the originality of the picture or image on which the operation is being done. Because of this if any unauthorized recipient gets the image then he/she is not able to recognize that there is any message hidden in it.

With the utilization of these techniques one can hide the confidential data easily like applying invisible watermark or encryption technique or LSB method while transmission. At some places visible watermark can also be applied for writing author, writer, files, etc. One must know that images/pictures have some of the useless section that he/she is not able to identify and so it can be useful for the sender to insert that section by some data which may be ignored by unauthorized recipient. Sender can also alter the LSB in each element with self-data without degrading picture standard and even though it not modifies colour strength.

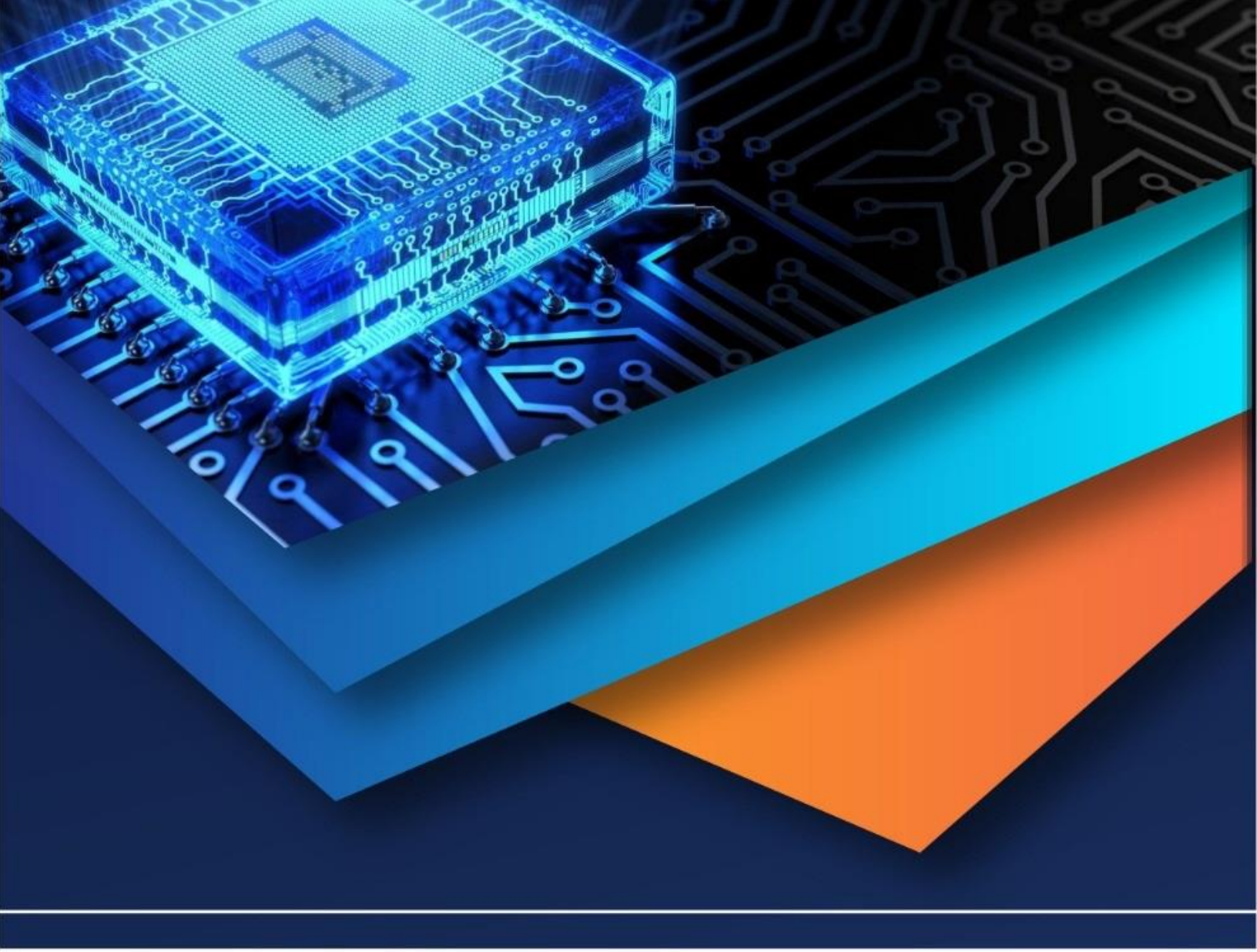
As discussed, there are some techniques which do not have enough capacity to intercept depiction and removal of inserted message. So, the usage of the criteria set for evaluation of techniques/methods has to be more specific and stronger enough for solving the security problems.

This paper shows that a proposed steganographic technology can be used for transmission of particular amount of data with security amongst two different groups. We also conclude that both cryptography and steganography can be used in together making the chances of data vulnerability very less and we get to know that any type of textual information or message can be made secured if necessary, that is sent over a communication channel. In addition to that the proposed methodology can be applied easily because of its simplicity.

At last we should be knowing that the different steganographic files or images used over here are only for representing the idea and procedure of the proposed technique and so it is not only limited to this file type only. This theory can be applied in general.

REFERENCES

[1] Souvik Bhattacharyya. and Gautam Sanyal. “An Image Based Steganographic Model for Promoting Global Cyber Security”.
[2] Kumar V and Kumar D. (2010): “Performance Evaluation of DWT Based Image Steganography”.
[3] Seth, L. Ramanathan, and A. Pandey, “Security enhancing: Combining Cryptography and Steganography”.
[4] J. Fridrich and M. Goljan, “Practical study of steganography of digital images: State of art,” Proc. SPIE, Security and Watermarking of Multimedia”.
[5] Yuk Ying Chung, fang Fei Xu, “Developing video watermarking for MPEG2 video”.
[6] S. Katzenbeisser, F.A.P. Petitcolas (Ed.), “Information Concealing Techniques for Steganography and Digital Watermarking”.
[7] Alturki, F., & Mersereau, R. “A novel approach for increasing security and data embedding capacity in images for data hiding applications”.
[8] Babu, K. S., Raja, K. B., Kiran, K. K., Manjula Devi, T. H., Venugopal, K. R., & Patnaik, L. M. “Authentication of secret information in image steganography”.
[9] Neeta, D., Snehal, K., & Jacobs, D. “Implementation of LSB Steganography and its Evaluation for various bits”.
[10] Li, B., Biswas, S., & Blasch, E. P. “An estimation approach to extract multimedia information in distributed steganographic images”.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY