iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35417

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 9 Issue VI Jun 2021- Available at www.ijraset.com

Digital Image Watermarking using Chaotic Encryption and Arnold Transform

Santhosh Voruganti[1], U. Sairam[2]
[1, 2]*Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, India-500075*

Abstract: ***Internet has caused an extraordinary increase in the transfer and sharing of digital data like text, videos, images, audio, etc. over it. However, with the advent of modern access technology, multimedia data is more prone to security risks as data can be modified or redistributed without prior permission. Chaotic encryption-based blind digital image watermarking technique applicable to both grayscale and colour images. Discrete cosine transform (DCT) is used before embedding the watermark in the host image. Arnold transform is used in addition to chaotic encryption to add double-layer security to the watermark. Three different variants of the proposed algorithm have been tested and analysed. The simulation results show that the proposed scheme is robust to most of the image processing operations like joint picture expert group compression, sharpening, cropping, and median filtering. To validate the efficiency of the proposed technique, the simulation results are compared with certain state-of-art techniques.***

Keywords: ***Discrete cosine transform, Image Processing Techniques, Chaotic Encryption, Digital watermarking, Arnold Transform.***

I. INTRODUCTION

We are living in an age where the Internet has such a great impact on our lives, that we are dependent on it in every aspect. This internet has transformed the entire world into a global village and in last few years, there has been an extraordinary increase in the transfer and sharing of digital data like text, videos, images, audio, etc. over it. However, with the advent of modern access technology, multimedia data is more prone to security risks as data can be modified or redistributed without prior permission. The security risks may include copyright violations, piracy, hacking, unapproved production and distribution, information theft and several other statistical and differential attacks. According to the Motion Picture Association of America (MPAA) and the Institute of Policy Innovation (IPI), billions of dollars and thousands of jobs are lost annually due to piracy and copyright violation faced by movie, music and software industries.

A. Image Processing Techniques

Image enhancement operations improve the qualities of an image like improving the image's contrast and brightness characteristics, reducing its noise content, or sharpen the details. This just enhances the image and reveals the same information in more understandable image. It does not add any information to it.

Image restoration like enhancement improves the qualities of image but all the operations are mainly based on known, measured, or degradations of the original image. Image restorations are used to restore images with problems such as geometric distortion, improper focus, repetitive noise, and camera motion. It is used to correct images for known degradations.

Image analysis operations produce numerical or graphical information based on characteristics of the original image. They break into objects and then classify them. They depend on the image statistics. Common operations are extraction and description of scene and image features, automated measurements, and object classification. Image analyze are mainly used in machine vision applications.

Image compression and decompression reduce the data content necessary to describe the image. Most of the images contain lot of redundant information, compression removes all the redundancies. Because of the compression the size is reduced, so efficiently stored or transported. The compressed image is decompressed when displayed. Lossless compression preserves the exact data in the original image, but Lossy compression does not represent the original image but provide excellent compression.

Image synthesis operations create images from other images or non-image data. Image synthesis operations generally create images that are either physically impossible or impractical to acquire.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

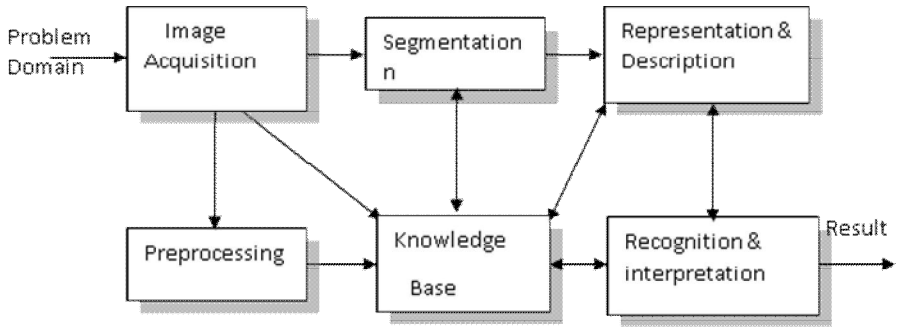


Fig.1. Fundamental Sequence Involved In Image Processing System.

B. Motivation

The watermark security unit is aimed at improving the security of the embedded watermark so as to make it impossible for an adversary to get the exact watermark even if it has the knowledge of embedding algorithm. Chaotic theory and Arnold encryption have been used to achieve a better security. In recent times, due to great developments in computer and internet technology, multimedia data i.e. audio, images and video have found wide applications. Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing multimedia data. Encryption of multimedia products prevents an intruder from accessing the contents without a proper decryption key. But once the data is decrypted, it can be duplicated and distributed illegally. To enforce IP rights and to prevent illegal duplication, interpolation and distribution of multimedia data, Digital watermarking is an effective solution. Copyright protection, data authentication, covert communication and content identification can be achieved by Digital watermarking. Digital watermarking is a technique to embed copyright or other information into the underlying data.

C. Problem Statement

There is a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data such as information about the owner, recipient and access level without being detectable in the host multimedia data. Though cryptography has been used as a potential tool to tackle some of the issues but cryptographic methods involve the modification of data visually and statistically, which often arouses suspicion and invite attacks. Information hiding, which involves steganography and watermarking has furnished as an effective and alternative method for security and authentication in multimedia images.

D. Objective

The watermark security unit is aimed at improving the security of the embedded watermark so as to make it impossible for an adversary to get the exact watermark even if it has the knowledge of embedding algorithm. Chaotic theory and Arnold encryption have been used to achieve a better security.

II. LITERATURE SURVEY

Digital watermarking has been shown to be one of the best solutions for protecting IPR and authenticating the content. Digital watermarking is a technique of hiding information in host media like video, images, etc., in a way that it is unnoticeable to human visual system (HVS). It ensures the security of the information hidden in the images/videos and acts as an important tool to take care of various multimedia related IPR issues. The pixel domain and coefficient domain methods are respectively called spatial domain and transform domain methods. A genetic algorithm based multiple watermarking techniques utilizing DWT and SVD has been presented in. Though the scheme has been shown to be robust and has better imperceptivity, it has no provision for security of the watermark and the scheme is computationally complex. Among the various transform domain techniques, DCT has proven to be efficient as it favours low hardware design cost. There are usually three methods for computing DCT of an image. DCT is computed either on the whole image or is computed on the blocks of the image or only the DC coefficient of blocks of image are computed directly in spatial domain.

©IJRASET: All Rights are Reserved

A chaotic based encryption algorithm is an effective method for data encryption. Chaos signals possess the qualities of pseudo-randomness, irreversibility and dynamic behaviour. The systems having chaotic nature possess high sensitivity to initial parameters. The result of Arnold transform is an encrypted image which has a one-to-one correspondence with the original image. The pseudo-random nature of the Arnold encryption results in a scrambled image which is not possible to be cracked down without knowing the sequence used.

Watermarking is a technique for labelling digital pictures by hiding secret information into the images. We embed the watermarks with visually recognizable patterns into the images by selectively modifying the middle-frequency parts of the image. In our approach, a block DCT-based algorithm is developed to embed the image watermarking. Let X be the original gray-level image of size N1 x N2, and the digital watermark W be a binary image of size M1 x M2 . In the watermark, the marked pixels are valued as one's, and the others are zero's.

Since only the middle-frequency range of the host image will be processed during the watermark embedding, the resolution of a watermark image is assumed to be smaller than that of the original image . For example, for each 8 x 8 image block, only coefficients will be used for the watermark embedding. The ratio of (M1 x M2) and (N1 x N2) determines the amount of information to be embedded into the image. In general, for more robust and invisible embedding, the amount of information can be embedded should be reduced. On the other hand, in order to provide a visually recognizable watermark with nontrivial amount of information, instead of using an ID number with trivial amount of data, making the watermark embedding perceptually invisible is not a trivial problem.

III.METHODOLOGY

A. Existing System

A comparison of PSNR has been made with certain existing. The comparison results show that our technique produces high-quality grayscale images compared to the schemes under comparison. The watermarked images and the corresponding extracted logos for luminance component based embedding and RGB plane based embedding.

Discrete Cosine Transformation (DCT) like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away.

DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.

DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image.

B. Proposed System

The watermark security unit is aimed at improving the security of the embedded watermark so as to make it impossible for an adversary to get the exact watermark even if it has the knowledge of embedding algorithm. Chaotic theory and Arnold encryption have been used to achieve a better security.

The proposed architecture scheme below shows better robustness to singular and simultaneous attacks as a result of guard bands utilized in extraction process. This is due to the fact that, when the watermarked media experiences an attack, then the difference between the coefficients may be modified; but this difference has to cross the guard bands on either side of the difference zone to extract a wrong bit.

To ensure a better security, the watermark is encrypted at two levels, it is first encrypted by using Chaos and then by using Arnold transform, which results in enhanced security to the embedded watermark.

©IJRASET: All Rights are Reserved

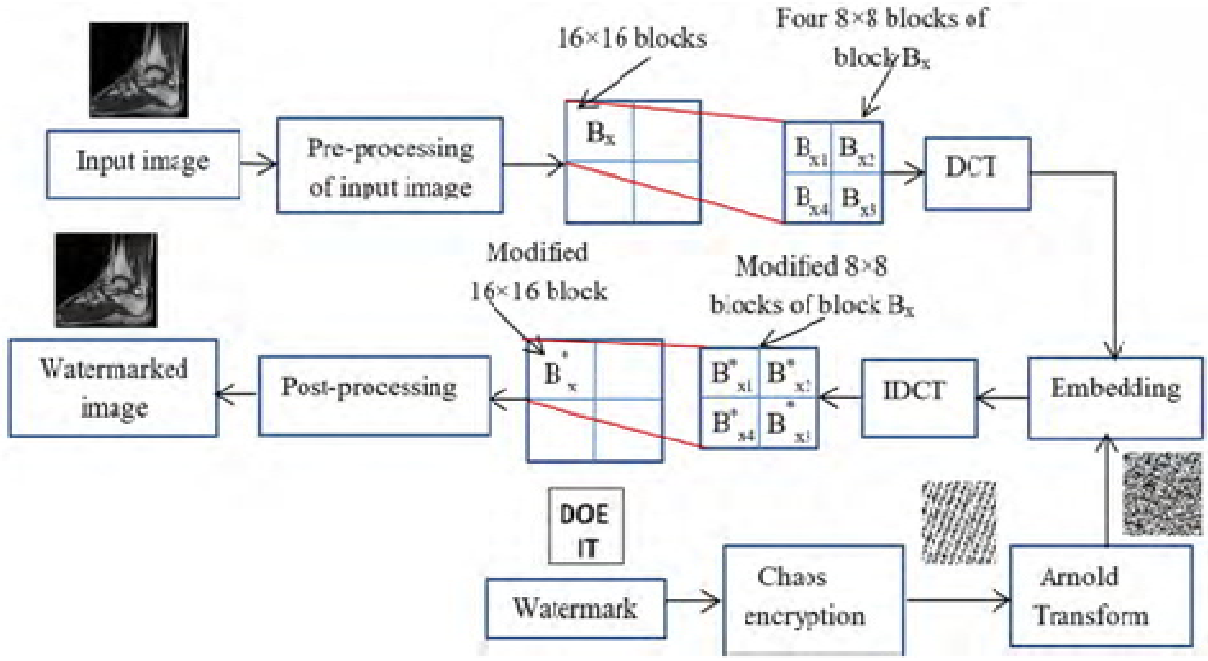


Fig .2.Architecture Of Proposed Technique

C. Chaotic Encryption

If key is based on chaotic sequence and plain text. First, the chaotic sequence and the plain text are used; the result is the key, so even someone obtains the initial value he cannot decrypt the cipher text. The initial value is destroyed. Then the key is used to encrypt the plain text and destroy the plain text. If someone obtains the chaotic initial value, he still cannot decrypt the cipher text because the real key is based on chaotic sequence and plain text. Obviously, the other people do not have the plain text. So, the key cannot be obtained by others. The other people have to use force-to-attack way to decrypt the cipher text. From the result of the experiments, one can see that the algorithm's security is improved and strengthened.

Most chaotic encryption algorithms use the chaotic sequence as the key to encrypt the data. The key is produced by logistic map or other maps using chaotic value. However, these maps are not perfect. These maps are sensitive to the initial value. When the initial value equals some certain value, the sequence is periodic. Moreover, if someone obtains the initial value, he can decrypt the cipher text. However, using the new algorithm even if someone obtains the initial value, he can get the chaotic sequence, but still he cannot decrypt the cipher text, because the key is also related to the plain text. Obviously, the other people do not have plain text, so they cannot get the key; if they get the cipher text, they have to use force-to-attack way to decrypt the cipher text. So, the binary sequence of the plain text should be better to be long. In other words, the algorithm is suitable for large amounts of data. Through experiments we can see that its encryption time is a little more than the previous chaotic encryption algorithms. But its decryption time is less than the previous chaotic encryption algorithm.

D. Arnold Transform

Image scrambling techniques are greatly important image encrypting methods in the space domain. They can be used to enhance the robustness of occlusion attacks and noise attacks. They have two groups. The first group is matrix transformations, e.g. the Arnold transform [1-2]. They need correct parameters of the transformation to solve inverse of the matrix transformation. They have good security; and the decoding process of the scrambled images requires keys and the transformations are simple.

The Arnold transform of a two-dimensional image is defined as

$$A^{M}:\begin{bmatrix} u_i \\ v_i \end{bmatrix} = \mathrm{mod}\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x_i \\ y_i \end{bmatrix}, M\right),$$

©IJRASET: All Rights are Reserved

where (xi, yi) and (ui, vi) are the position coordinates of image before and after the Arnold transform. The operator "mod" is the modulus after division operation. The period p of the transform depends on the parameter M, which is the size of the image. The covert image is scrambled by the Arnold transform for iterative number n and the scrambled image

Advantages:

- Speed and security, the use of chaotic encryption has been shown to offer increased security.
- Two encryption methods is that we do not need a large overhead of keys.

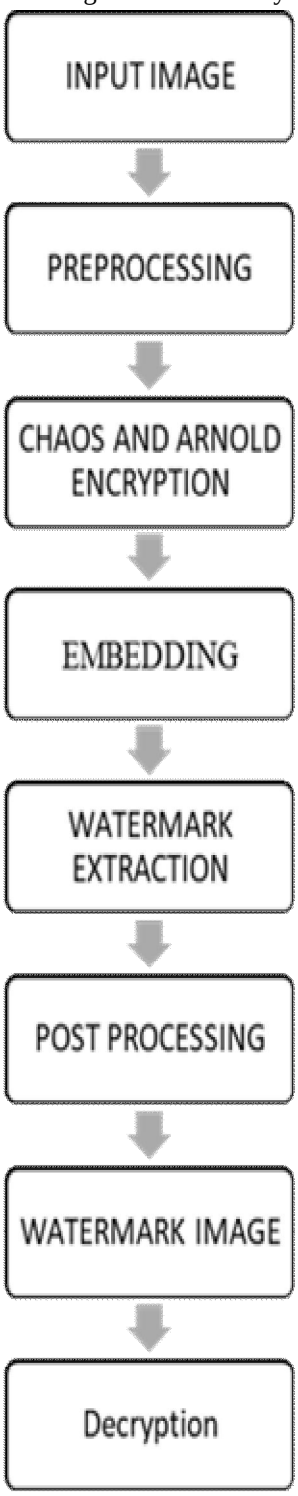


Fig.3. Block Diagram Of Proposed System

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

IV. IMPLEMENTATION

A. Pre-Processing

The pre-processing operations include the binarization of a facial image to increase the processing speed and conserve memory capacity and noise removal. The image processor developed performs the expansion and contraction operation on the white pixels and processing for noise removal is performed on the small black pixels of the facial images. After the binarization, the noise removal procedure involves an expansion processing method combined with the use of a median filter.

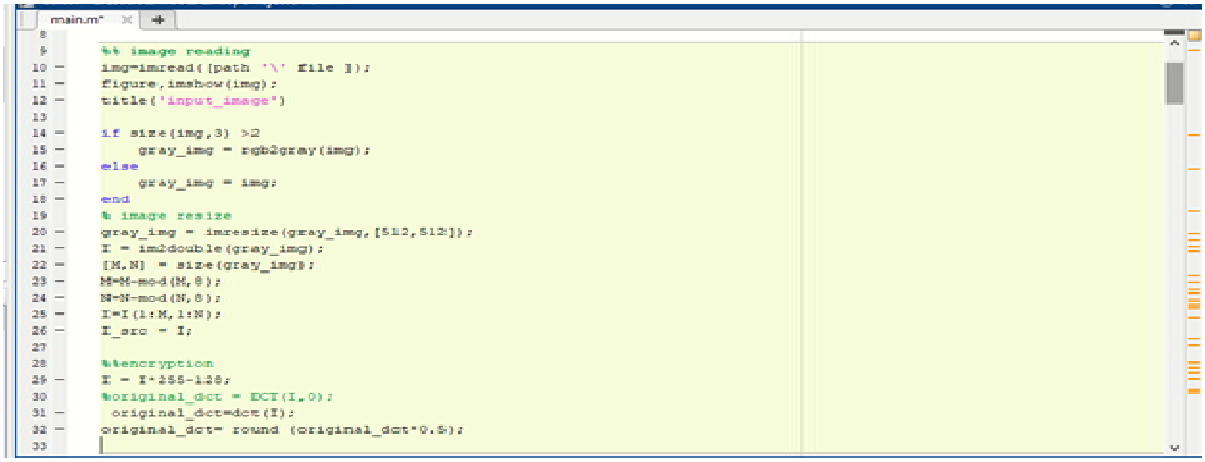


Fig.4. Snippet For Pre-processing

The input image `I' is passed through the pre-processing unit which acts as a buffer for grayscale images and as a converter for color images. To carry out watermark embedding into the luminance part of the image the pre-processing unit converts the input RGB image into YCbCr image, where Y stands for luminance information, Cb stands for chrominance blue information and Cr stand for chrominance red information of the image. The luminance part `Y' is put forward as cover for the watermark because modification of this part of the image brings less noticeable changes to actual image compared to the chrominance information.

B. Chaos Encryption

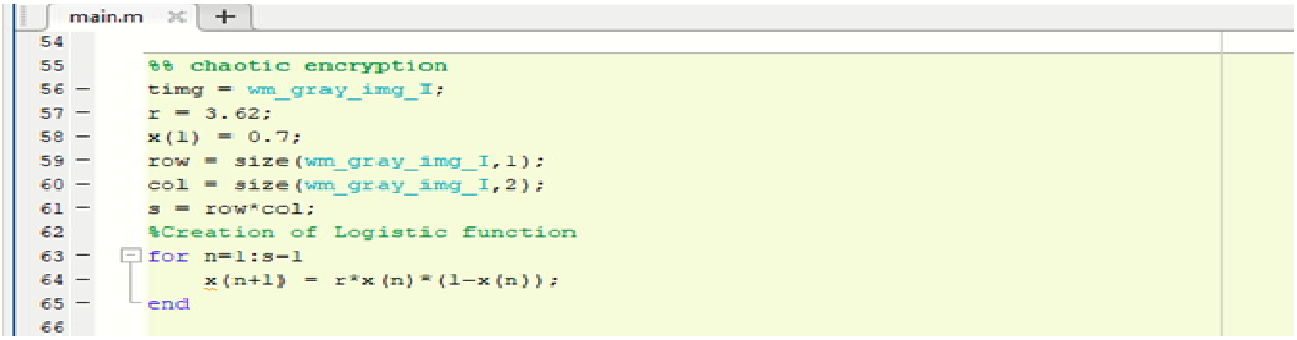


Fig.5. Snippet Of Chaos Encryption

A chaotic based encryption algorithm is an effective method for data encryption. Chaos signals possess the qualities of pseudo-randomness, irreversibility and dynamic behaviour. The systems having chaotic nature possess high sensitivity to initial parameters. The output chaotic sequence is similar to white noise having random behaviour with improved correlation and complexity and is defined and given by

$$C_{n+1} = \mu \times C_n \times (1 - C_n)$$

where $0 < \mu < 4$ typically μ is set to value 3.9 in order to achieve highest randomness and $0 < Cn < 1$ is the nth value generated from Eqn. 1. Different values of Cn could be obtained by varying the value of n from 0 to L-1. Here, L is the maximum number of chaotic values. By setting the initial values of μ and C0, we can get the required chaotic signal. As it offers the joint advantage of speed and security, the use of chaotic encryption has been shown to offer increased security.

©IJRASET: All Rights are Reserved

$C_{n+1} = \mu \times C_n \times (1-C_n)$

0<C(1)<1 for highest randomness.The logistic parameter `μ' is restricted to a range of 1.35 to 3.9 because this range of `μ' produces the chaotic values with highest chaotic behaviour at 3.9 which in turn provides high security to the watermark that is why we have chosen `μ' between 1.35 to 3.9

C(1)=0.7

C(1+1) = 3.62 × 0.7 × (1 – 0.7) = 0.7602

C(2+1) = 3.62 × 0.7602 × (1 – 0.7602) = 0.6599

C. Arnold Transform

The security of information can be increased by using various encryption techniques, and one of the effective techniques is Arnold transform. This encryption method, is two dimensional and works well in applications for encrypting images of type N×N. The Arnold transformation is mathematically represented as

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N)$$

where (xn, yn) and (x, y) respectively represent the input image and encrypted image pixel coordinates represented as 2D matrices. The transform results in the change of the pixel positions to generate an image which is disordered and different from original one. The result of Arnold transform is an encrypted image which has a one-to-one correspondence with the original image. The pseudo-random nature of the Arnold encryption results in a scrambled image which is not possible to be cracked down without knowing the sequence used. The strength of encryption depends on the number of iterations, which can be defined at the start of the process. Inverse Arnold transform is used to decrypt the encrypted message by using the equation.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod} N)$$

xn = (xn-1 + yn-1) modn

yn = (xn-1 + 2yn-1) modn

where (xn, yn) and (x, y) respectively represent the input image and encrypted image.

x1 = (1 + 1) mod32 = 2

y1 = (1 + 2) mod32 = 3

D. Watermark Generation

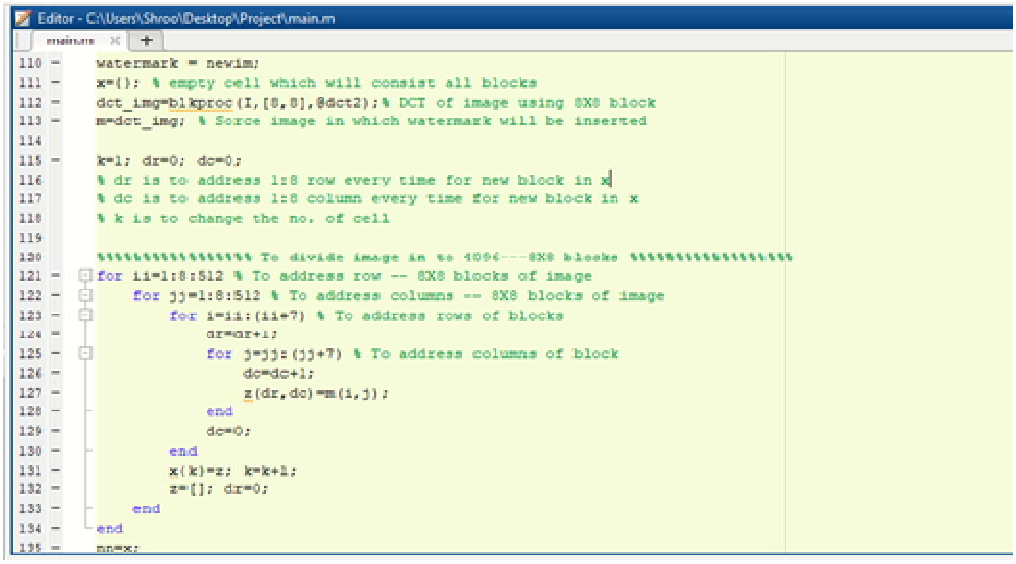


Fig.6. Snippet For Watermark Generation

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

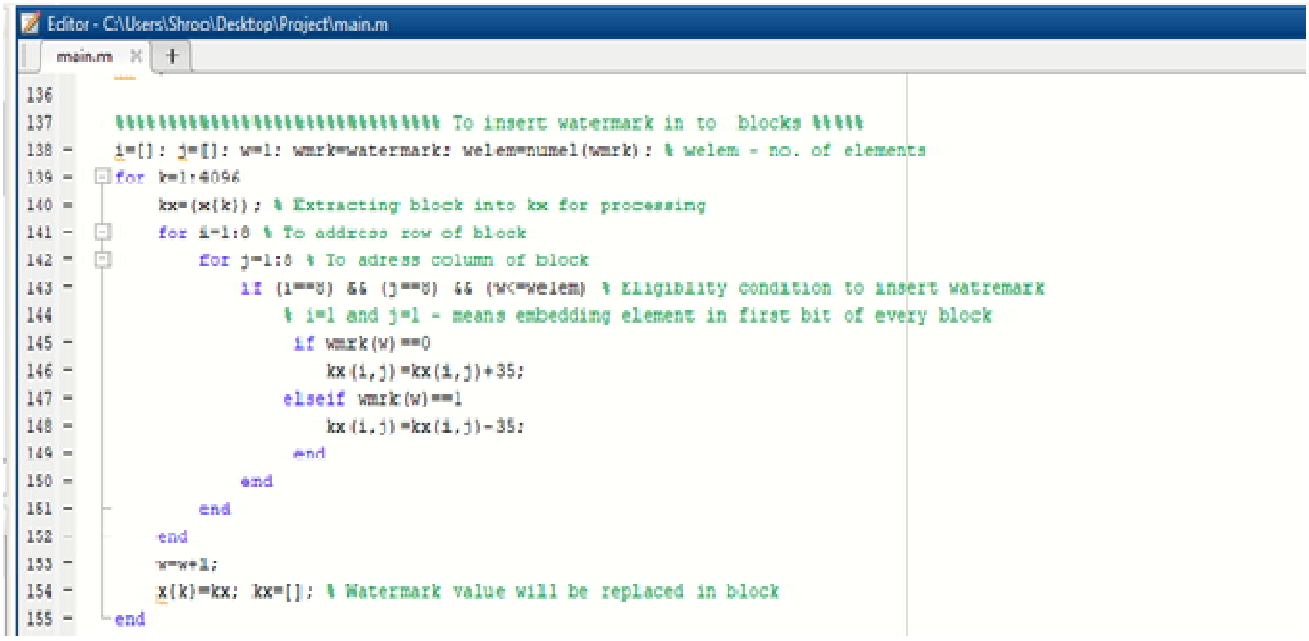


Fig.7. Snippet For Embedding Watermark

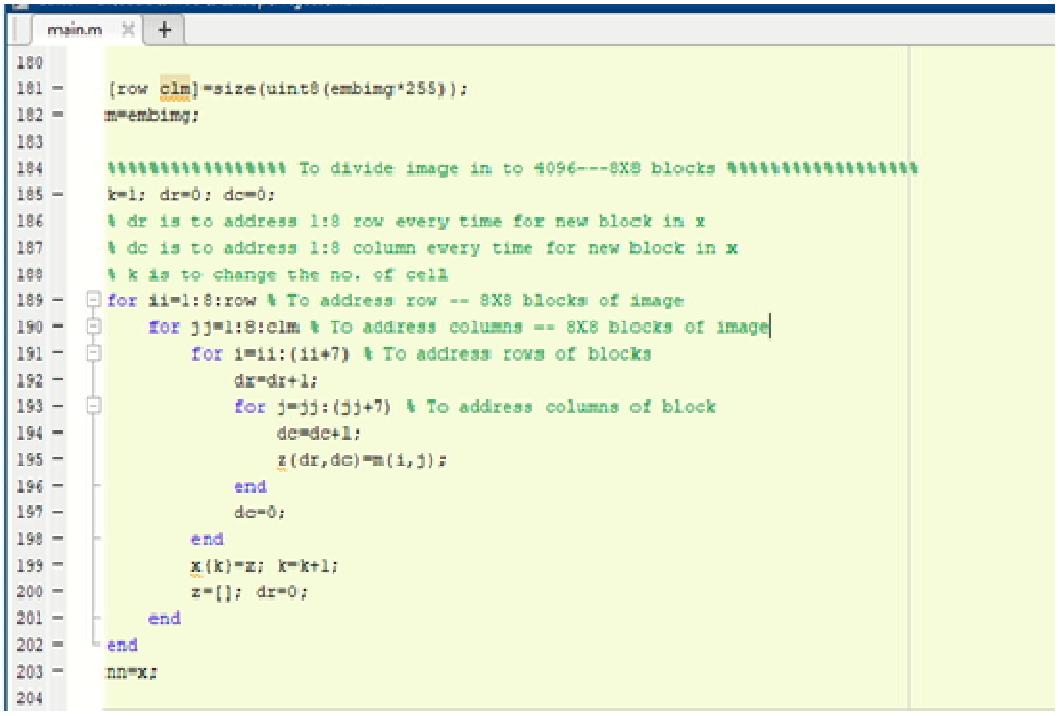


Fig.8.Snippet For Watermark Extraction

Watermark extraction involves steps like pre-processing, the partition of the watermarked image into 16×16 blocks and 8×8 blocks; DCT computation is carried out in exactly the same way as in case of the watermark embedding process. Only those DCT coefficients which are modified during embedding are used for watermark extraction. A watermark bit is obtained by analysing the difference between the two predefined coefficients.

If the difference lies anywhere in zone 2 or zone 5, bit `1' is obtained while bit `0' is obtained if the difference lies either in zone 1 or zone 4.

©IJRASET: All Rights are Reserved

V. RESULTS

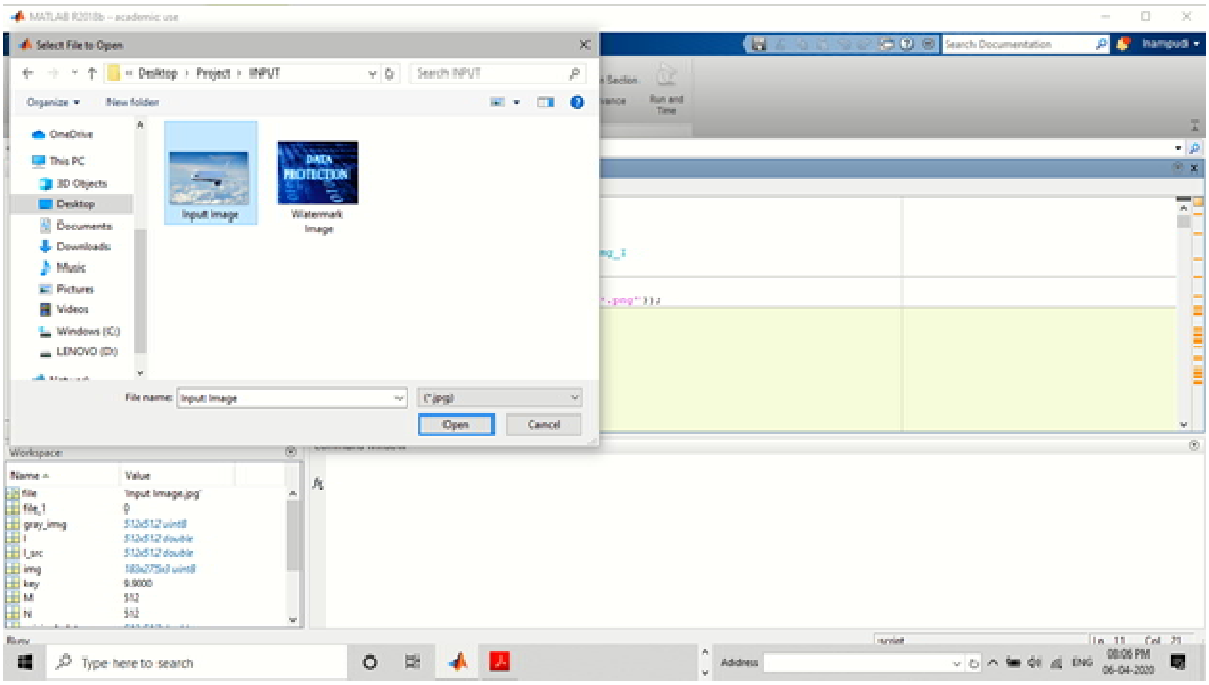


Fig.9. Selecting Input Image

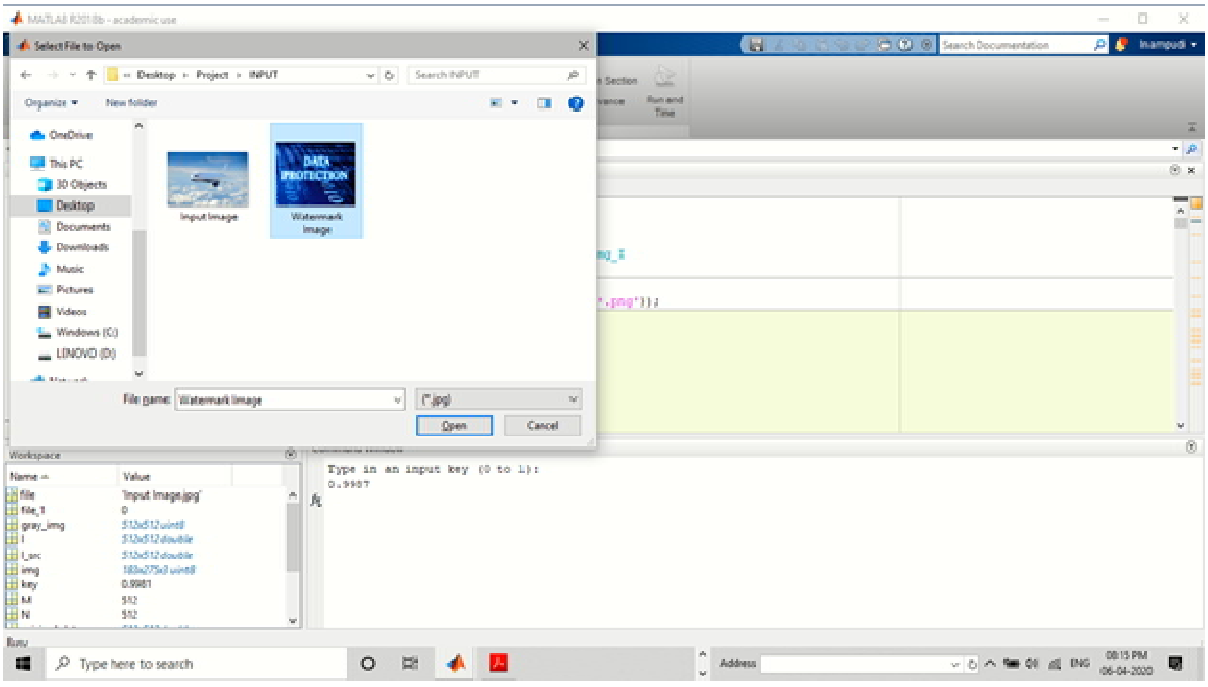


Fig.10. Select Watermark Image

The above Fig.10 givers the sender an option to select the watermark image which has to be embedded on the input image.
Two encryption algorithms are applied on the watermark image. First Chaotic encryption is performed which results in a chaos based encrypted image. This encrypted image is further made secure with Arnold Transform which results in Arnold transform encrypted image.The Arnold transform encrypted image is embedded on the input image given by the user and the watermarked image is sent to the receiver.

©IJRASET: All Rights are Reserved

Fig.11. Watermarked Image

The above Fig.11 is the input image with the watermark image embedded on it.

Fig.12. Retrieved final Output image

VI. CONCLUSION & FUTURE SCOPE

A secure and blind watermarking scheme in the DCT domain was proposed. Arnold transform and chaotic encryption were utilized to add double layer security to the watermark. The comparison results depict that proposed scheme outperforms many state-of-art schemes in terms of imperceptibility, robustness, and payload. Further, the double layer of security of the embedded watermark ensures that the scheme is highly secure in nature. Given the merits of the proposed scheme, we conclude that it is well suited for the application of copyright protection and ownership verification. The scheme could be used to solve various medical image integrity and electronic patient record (EPR), security issues in contemporary telemedicine and e-healthcare setups. The main limitation is the effective sharing of the key used in key security analysis for enhanced security. If an intruder gets their hand on the key while it's being shared by the sender to the receiver, then he can easily decrypt and access the watermarked image.

In the future, this paper can be developed with an option to compare the accuracy of the input image and final retrieved watermark image. Also, the proposed algorithm will be tested for real time applications by implementing it on Field Programmable Gate Array (FPGA) platform. keys. Future works will focus on making our scheme more robust to attacks like lossy image compression (e.g., JPEG) and reducing the complexity of our algorithm.

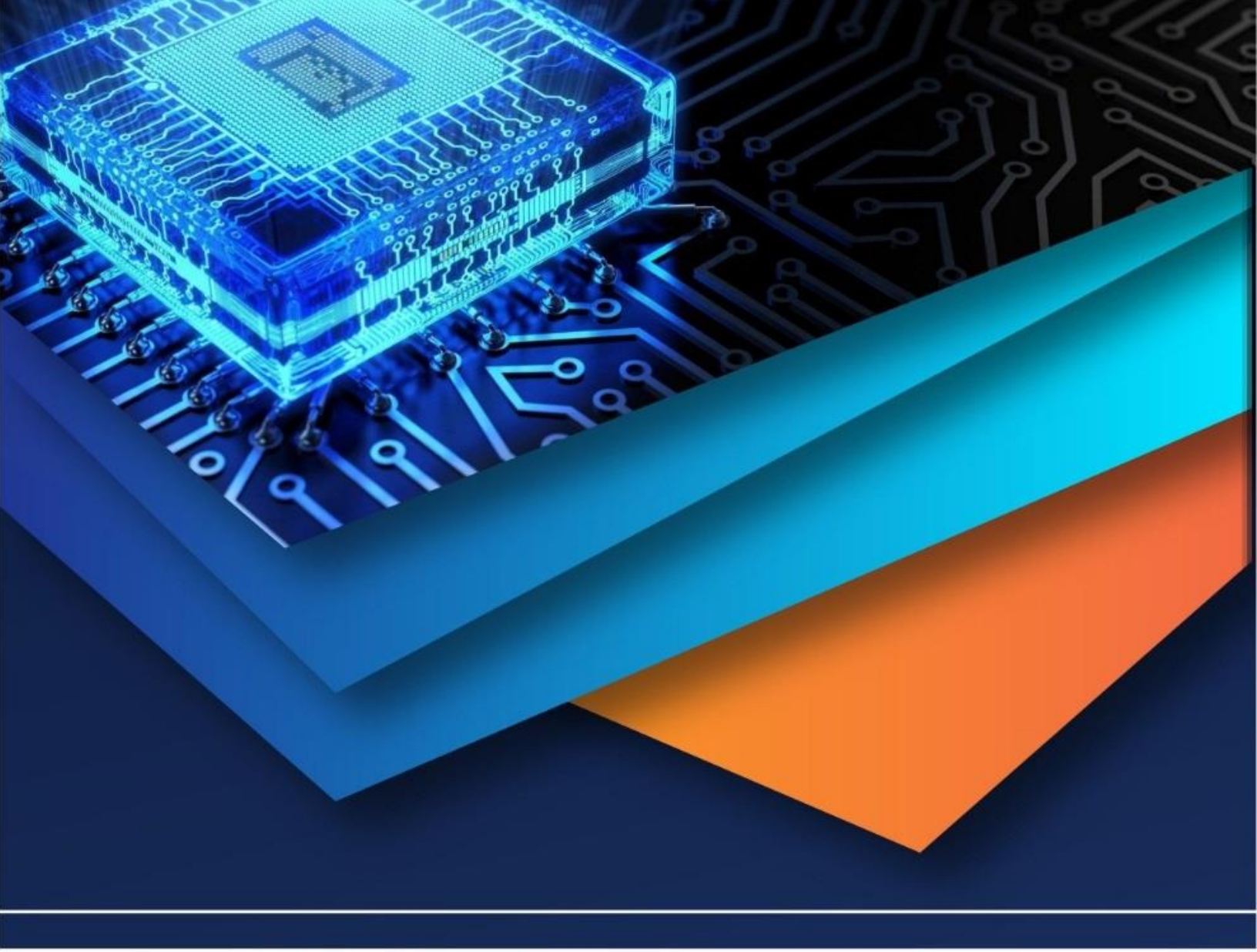
©IJRASET: All Rights are Reserved

REFERENCES

[1] N. Mohananthini and G. Yamuna, ``Comparison of multiple watermarking techniques using genetic algorithms," J. Electr. Syst. Inf. Technol., vol. 3, no. 1, pp. 68_80, May 2016.
[2] J.Won, S.-H. Seo, and E. Bertino, cryptographic protocols for efficient drone-based smart city applications," IEEE Access, vol. 5, pp. 3721_3749, 2017.
[3] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S.W. Baik, ``A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools Appl., vol. 75, no. 22, pp. 14867_14893, 2016.
[4] J. B. Lima, F. Madeiro, and F. J. R. Sales, ``Encryption of medical images based on the cosine number transform," Signal Process., Image Communication., vol. 35, pp. 1_8, Jul. 2015.
[5] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, ``CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method," Multimedia Tools Appl., vol. 76, no. 6, pp. 8597_8626, 2017.
[6] Santhosh Voruganti Map reduce A programming model for cloud computing based on hadoop ecosystem published in International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3794-3799.
[7] Santhosh Voruganti Survey on Data-intensive Applications, Tools and Techniques for Mining Unstructured Data. International Journal of Computer Applications (0975 – 8887), volume 146-No.12, July 2016.
[8] Santhosh Voruganti Comparative Analysis of Dimensionality Reduction Techniques for Machine Learning IJSRST Volume 4 Issue 8 Print ISSN: 2395-6011 Online ISSN: 2395-602X Themed Section: Science and Technology June 2018.
[9] Santhosh Voruganti Enhanced Rating Prediction Based On Location And Friend Set published in JETIR May 2019 volume 6 issue 5 ISSN-2349-5162.
[10] Santhosh Voruganti Local Security Enhancement and Intrusion Prevention in Android Devices published in International Research Journal of Engineering and Technology Volume: 07 Issue: 01 January 2020 e-ISSN: 2395-0056 p-ISSN: 2395-0072.
[11] Santhosh Voruganti EFFECTIVE IOT TECHNIQUES TO MONITOR THE LEVELS OF GARBAGE IN SMART DUSTBINS published in International Research Journal of Engineering and Technology Volume: 07 Issue: 06 June 2020 e-ISSN: 2395-0056 p-ISSN: 2395-0072.
[12] U. Sairam Vanitha Kunta, Haritha Tuniki ,Multi-Functional Blind Stick for Visually Impaired People, Fifth International Conference on Communication and Electronics Systems, July 2020.
[13] Yashwant Adepu, Vishwanath R Boga, U Sairam, Interviewee Performance Analyzer Using Facial Emotion Recognition and Speech Fluency Recognition,2020 IEEE International Conference for Innovation in Technology (INOCON), pages 1-5 in 06.11.2020.
[14] M V Bhanu Prakash U Sairam, Feature Prospect of the VAST Applications of Machine Learning, Research Review international Journal of Multidisciplinary, volume 4 and issue 4 in April 2019.
[15] B Surya Samantha, M Trupthi, U Sairam, A review on using crow search algorithms in solving the problems of constrained optimization, International Journal of Scientific Research in Science and Technology,2018.

.

©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)