iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 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 Novel Cryptography Scheme Based on Decomposition of an Image or Its Transformed Version to be watermarked

Abhishek Tripathy[1], Dinesh Kumar[2]

[1,2]*Dept of Computer Science & Engineering*

Shekhawati Institute of Engg. & Technology

Sikar (Rajasthan)

Abstract*— Cryptography and watermarking are two key aspects for information hiding to communicate secure information from one source to other source over network. The communication over network is very secure due to these techniques. These two techniques are differing from each other for hiding information behind or in image. In this paper we present that if these two techniques are combined together than what good results can come out with effect. In the proposed method "Cryptography" is used to encrypt the plain text message in to the cipher text using the Hill Cipher Algorithm, and second technique is "Watermarking "for the image decomposition or its transformed version using self-fractional Fourier function (SFFFs). So this method is much effective than older ones.

Keywords*— Cryptography, Steganography, self-fractional fourier function.

I. INTRODUCTION

The proliferation of digitized media object such as audio, image, and video is creating a pressing need for copyright enforcement schemes that protect copyright ownership [1-2]. Conventional cryptographic systems permit only valid key holders to access encrypted data, but once such data is decrypted there is no way to track its reproduction. Therefore, conventional cryptography provides little protection against data piracy, in which an owner is confronted with unauthorized reproduction of information. Therefore the solution for the problem that arise in the conventional cryptography is that the digital watermarking [1].

Watermark and cryptography are both effective methods to protect information, but they serve in different way. We intend to take cryptography as copy-protecting, while the watermark copyright-protecting method. In modern cryptography, it is crucial for the future development of cryptography that robust methods are developed to protect the intellectual property rights of data owners against unauthorized copying and redistribution. Classical encryption systems do not completely solve this problem, because once encryption is removed from a document, there is no more control of its dissemination. To solve the difficult problem, the new effective technique was put forward for copyright and safety maintenance of digital products, i.e. information hiding techniques, including both steganography

and digital watermarking. A digital watermark is therefore intended to complement the cryptographic processes. Steganography is related to cryptography and is the basis for many of the digital watermarking techniques currently developed. Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed. Many steganographic techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing and microdots [3]. Usually the secret information is concealed by the use of an innocuous cover as not to arouse suspicion if hostile agents discover the cover [4]. Digital watermark hide specific marker (digital watermark) in digital images, audio, documents, books, video and other digital products to prove the copyright of the author, and to serve as evidence for identification and prosecution of illegal infringement. At the same time, the detection and analysis of digital information can ensure the integrity and reliability of the digital information; therefore serve as a means to protect the rights and interests of the author. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. In the context of this work, data refers to audio (speech and music), images (photographs and graphics), and video (movies). Many of the properties of the scheme presented in this work may be adapted to accommodate audio and video implementations, but the algorithms here specifically apply to images.

Watermarking is the process of embedding data called a watermark (also known as Digital Signature or Tag or Label) into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object [1]. The object may be an audio, image or video. Digital watermark techniques are now eventually becoming one of the most reliable methods to prove the copyright of both observed and processed digital marine data, especially when the data have to be distributed through Internet. It decoding and divided the copyright information, often after some kind of transformation, to liquid-like form and adhere to the original data **so** that it can still carry the copyright information with it while it keeps completely invisible. A simple example of digital watermark would be a visible "seal" placed over an image to identify the copyright [1-2]. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the object.

Researchers have proposed various watermarking schemes in the spatial as well as frequency domains [1-10]. Jung et al. [8] transformed the host image to the YCbCr color space and the watermark to the frequency domain using Discrete Cosine Transform (DCT). Next, the luminance Y was transformed to the frequency domain using the Discrete Wavelet Transform (DWT). Then, the transformed watermark was embedded in the luminance Y band. Voyatzis and I. Pitas [9] transformed the host image using DCT, and scattered the watermark using pseudorandom permutation. Next, the scattered watermark was embedded in the transformed host image. They used the embedding scaling factors to control the robustness and the imperceptibility but the factors of the schemes are both defined manually. Nishcha [10] has also proposed an optical image watermarking scheme using fractional Fourier transform (which is a general version of Canonical Fourier transform (CFT)). Here the watermark is encrypted using double random fractional order Fourier domain encoding scheme [10]. Encrypted image is watermarked into a host image. The watermark is recovered by applying corresponding correct fractional order and random phase masks.

In this dissertation report a novel cryptography/watermarking process based on decomposition of a signal using SFFFs [10-12] is proposed and is shown in Figure 3.7 and Figure 3.8 here. The proposed decomposition scheme and the use of some transform provide additional encryption or security in the sense that a hacker or attacker cannot obtain the original image unless all the decomposed images and the parameter of the transform are known.

In this section, we will discuss the different kind of cryptography techniques that are required to encrypt and decrypt

ISSN: 2321-9653

original message, when we send the message from sender to receiver in secure manner, steganography and their objective, different kind of watermarking, different type of watermarks, watermarking process, watermarking insertion and extraction algorithm, characteristics of watermarking, application of watermarking and some transform techniques.

II. PROPOSED METHOD

In this section, we proposed an advanced system of encrypting data that combines the features of cryptography and watermarking along with data hiding. This system will be more securing than any other these techniques alone and also as compared to watermarking and cryptography combined systems shown in figure 1 and 2. The basic idea of this proposed method is that it provides the high rate of security when the secure data transfer from sender to destination via the some transmission media shown in figure 1 and 2. We shall use traditional cryptographic techniques to achieve data encryption.

As above mentioned, this method purely based on the two different kinds of technologies such as the cryptography and watermarking .So basically, if we combine both techniques in to a single, then gain the high rate of the security during the transmission. In this proposed method, the first technique "Cryptography" is used to encrypt the plain text message in to the cipher text using the Hill Cipher Algorithm, and second technique is "Watermarking " for the image decomposition or its transformed version using self-fractional Fourier function (SFFFs).So by taking the ideas from the previous work that effectively worked on the 1-D function ($f(x)$) ,extends work for 2-D and original image (2-D function $f(x,y)$) or its transformed version is decomposed in to M SFFFs images f_i (x,y), i = 1, 2, 3, ... M using equation (1). After decomposing of the original image, we encrypt the original plaintext message into the cipher text(non-readable format) using the equations (1) and (2) that we want to transfer from some communication channels .The detail description of encryption procedure will be discussed in Appendix (I) .Now construct different kinds of watermarks including encrypted message. Always bear in mind, the value of the M should be same for original image decomposing and watermark. For example, if original image decomposes in to four SFFFs (M = 4), they only require four watermarks..This watermark called the encrypted watermark. Decomposed images are then watermarked by different encrypted watermarks denoted by h_i (x, y), i = 1, 2, 3 . . . M to obtain the encrypted watermarked images

$w_i(x, y)$ as given below.

$$w_i(x, y) = f_i(x,y) + a\, h_i(x,y),\ i = 1, 2, 3, \ldots\ldots M, \qquad (1)$$

where a is an arbitrary constant that ensures the invisibility of watermarked images and the robustness of the watermarked image against distortions. The suitable value of the parameter a can be selected by simulation experiments. These all activities done at the sender side, and pictorial representation of this process shown in figure 1:

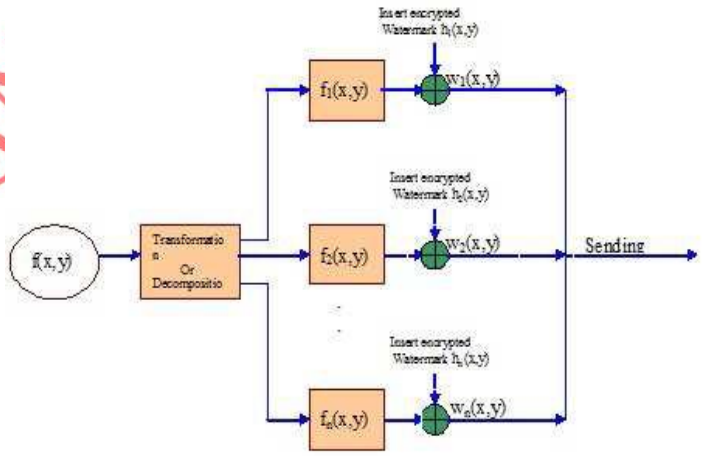


Fig. 1 Sending of the encrypted message inside the decomposed image

These decomposed images with encrypted watermark send from sender to destination one by one in order manner in which they constructed, through the communication channel. After receiving (in same order of sending) at the destination these individual watermarked images $w_i(x, y)$ are then combined to obtain the original watermarked image $w(x, y)$.

$$w(x, y) = \Sigma\, w_i(x, y),\ i = 1, 2, 3 \ldots\ldots\ldots M \qquad (2)$$

ISSN: 2321-9653

At the receiving end, we perform some operation using equation (2), and the pictorial representation as follow.

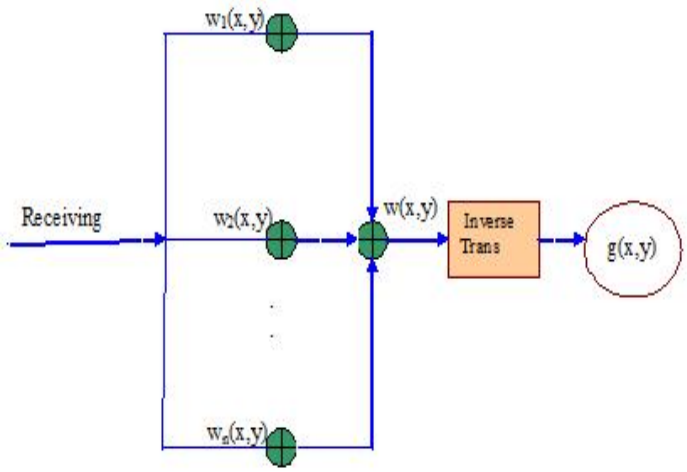


Fig. 2 Receiving the individual watermarked image to construct a single image

III. RESULT AND DISCUSSIONS

A. SIMULATION RESULTS

In this section results of computer simulations carried out on MATLAB platform are presented. Figure 4 shows the Cameraman image of size 256 256 pixels, to be used as a host image $f(x, y)$.

Fig. 4 Host Cameraman image $f(x, y)$

The image $f(x, y)$ is then decomposed into four SFFF images $f_1(x, y)$, $f_2(x, y)$, $f_3(x, y)$, $f_4(x, y)$ based on proposed scheme for M 4.

The decomposed images are shown in Figures 5 (a-d).

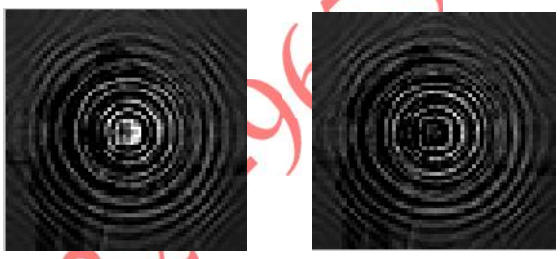


Figure 5 (a) Figure 5 (b)

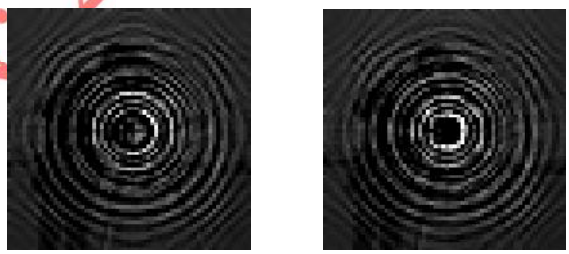


Figure 5 (c) Figure 5 (d)

Fig. 5 (a-d) SFFFs of Cameraman generated for M 4

Now take the original message that we want to transfer and encrypt it into the unreadable format using the Hill Cipher algorithm, and the result for this process carried out on JAVA platform. For example, we want to send the abbreviated form (SGVU) of "Shekhawati Gyan Vidhya University". So first we encrypt the message SGVU in ciphertext, and construct the individual watermarks according the value of the M.

Figure 6 shows different watermark images of the encrypted message ($h_1(x, y)$, $h_2(x, y)$, $h_3(x, y)$, $h_4(x, y)$) of size 256×256 pixels which are to be embedded into the decomposed images. This technique will be discussed in detail in Appendix I.

ISSN: 2321-9653

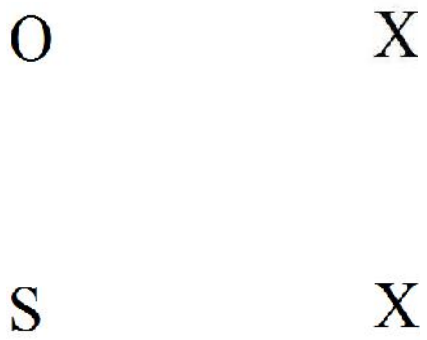


Fig. 6 Watermark images of encrypted message

These watermarks are embedded into the decomposed images shown in Figure 7 (a-d and the resulting watermarked images w_1 (x, y), w_2 (x, y), w_3 (x, y), w_4 (x, y) are shown in Figure 7 (a-d).

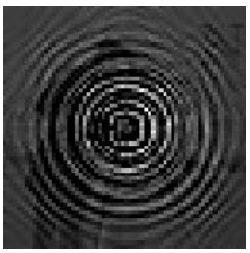


Figure 7 (a)

Figure 7 (b)

Figure 7 (c)

Figure 7(d)

Fig. 7 (a-d) Decomposed encrypted watermarked images

Now, we send these individual watermarked images from sender to receiver via the some transmission channel. At the destination end, after receiving the individual watermarked images $w1$ w_1 (x, y), w_2 (x, y), w_3 (x, y), w_4 (x, y) combines them to obtain the resulting (watermarked) image w x, y as shown in figure 8

Fig. 8 Reconstructed watermarked image

The recovery of watermark obtained by subtracting the decomposed images (f_1 (x, y), f_2 (x, y), f_3 (x, y), f_4 (x, y)) from the decomposed watermarked images w_1 (x, y), w_2 (x, y), w_3 (x, y), w_4 (x, y) or its transformed version is shown in Figure 9. The watermark cannot be recovered without using the correct decomposed images f_1 (x, y), f_2 (x, y), f_3 (x, y), f_4 (x, y).

Fig. 9 Recovered encrypted watermark

B. EFFECT OF NOISE

In this section the effect of white Gaussian noise in the watermarked image on the recovery of watermark is studied.

The watermarked Cameraman image embedded with white Gaussian noise with SNR=40db, SNR=30db & SNR=20db are shown in Figure 10, Figure 11, and Figure 12 respectively.

Fig. 10 Watermarked image with white Gaussian noise of SNR=40db

Fig. 11 Watermarked image with white Gaussian noise of SNR=30db

Fig. 12 Watermarked image with white Gaussian noise of SNR=20db

The effect of the white Gaussian noise on the recovery of watermark is shown in Figure 13, Figure 14, and Figure 15 respectively.

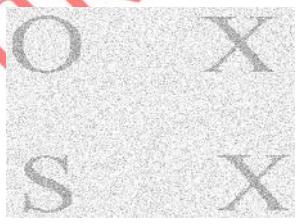


Fig. 13 Recovered encrypted watermark with SNR=40db

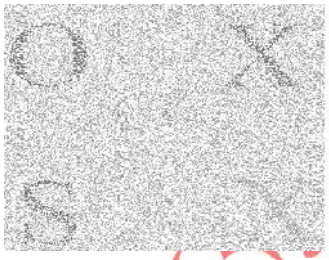


Fig. 14 Recovered encrypted watermark with SNR=30db

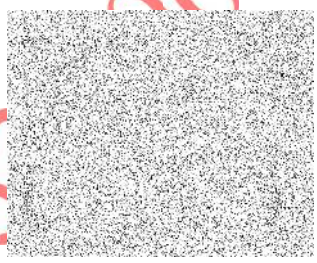


Fig. 15 Recovered encrypted watermark with SNR=20db

It is observed that below an SNR =20db, the original watermark recovery is not possible whereas for SNR=40db the watermark is fully recovered. With SNR=30db most of the information content of watermark is recovered but some information is embedded in noise.

IV. CONCLUSION

In this paper a novel cryptography scheme based on decomposition of an image or its transformed version to be watermarked using SFFFs is proposed.

The proposed decomposition scheme and the use of some transform before the decomposition step offers additional degrees of freedom to enlarge the encryption/decryption key size enhancing the level of security. Robustness of the recovery of the watermark in the proposed watermarking scheme under different signal-to-noise ratio (SNR) has also been demonstrated through simulation results.

The proposed scheme provides encryption or security in the sense that hackers or attackers cannot obtain the original image of message during the transmission and cannot see the original message unless all the correct set of decomposed images is

ISSN: 2321-9653

known, due to the uniqueness of such a set. Hence, cryptography using decomposition of an image is inherently secure. However the proposed scheme offers watermark recovery only above a certain SNR values.

There are two disadvantage of the proposed cryptography scheme. First is increase in cost of terms of its memory requirements for storage or transmission purpose. Secondly Hill cipher algorithm is not sufficient when we want to encrypt and transmit a large amount of the plain text message.

Appendix-I

Message Encryption Procedure

In this section, we will discuss the technical details for encrypting the original message using the Hill Cipher algorithm already discussed in previous section (1.2.3.2). First of all, we take the original message that we want to transmit from one location to another, then convert the individual character into a number starting from A=0, B=1 and so on. For example, we want to encrypt the first later of each phrase of Shekhawati Gyan Vidhya University is that SGVU. Then, follow the following steps.

(1) For encryption, algorithm takes m successive plaintext letters, and each character is assigned a numerical value like A 0, and so on. For SGVU the numerical values are following

S	p1
G	p2
V	p3
U	p4

where m =4, p_i= p1,p2,p3,p4

(2) Now need m m random key matrix, denoted by ki j

$$k_{i\,j} = \begin{pmatrix} 3 & 5 & 7 & 9 \\ 11 & 13 & 15 & 17 \\ 19 & 21 & 23 & 25 \\ 27 & 29 & 31 & 33 \end{pmatrix}$$

(3) Multiply ki j with p_i for ciphertext denoted by c_i using the following equation

$$c_{i=\,[}k_{i\,j} \quad p_{i\,j\,mod26}$$

$$_{[}k_{i\,j} \quad p_{i\,j=} \begin{pmatrix} 3 & 5 & 7 & 9 \\ 11 & 13 & 15 & 17 \\ 19 & 21 & 23 & 25 \\ 27 & 29 & 31 & 33 \end{pmatrix} \begin{pmatrix} 9 \\ 6 \\ 20 \\ 21 \end{pmatrix} 18$$

$$_{[}k_{i\,j} \quad p_{i\,j=} \begin{pmatrix} 404 \\ 933 \\ 1448 \\ 1973 \end{pmatrix}$$

$$c_{i\,=} \begin{pmatrix} 404 \\ 933 \\ 1448 \\ 1973 \end{pmatrix} \text{ mod } 26$$

$$c_{i\,=} \begin{pmatrix} 14 \\ 23 \\ 18 \\ 23 \end{pmatrix}$$

(4) Perform inverse process of step (1) to convert into alphabets and result is

$$\begin{pmatrix} 14 & \\ & \\ 18 & S \\ 23 & X \end{pmatrix} \quad X$$

So that cipher text of the plaintext of *"SGVU"* is that *"OXSX"* which will transfer from sender to destination.

REFERENCES

[1] I.J.Cox, J.Kilian, T.Leighton, and TShammoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] I.J.Cox, and M.L. Miller, "A Review of Watermarking and the Importance of Perceptual Modeling," in Proc. of SPIE Conf. on Human Vision and Electronic Imaging II , vol. 3016, pp. 92-99, Feb. 1997.

[3] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon," Image Steganography: Concepts and Practice", April 22, 2004 1:49 WSPC/Lecture Notes Series: 9in x 6in

[4] Ki-Hyeok Bae and Sung-Hwan Jung, "A study on the robustness of watermark according to frequency band," ISIE, pp.641-773, 2001.

[5] I.Pitas, "A Method for Signature Casting on Digital Images," in Proc. of IEEE Conf. on Image Processing, pp. 215-218, Sep. 1995.

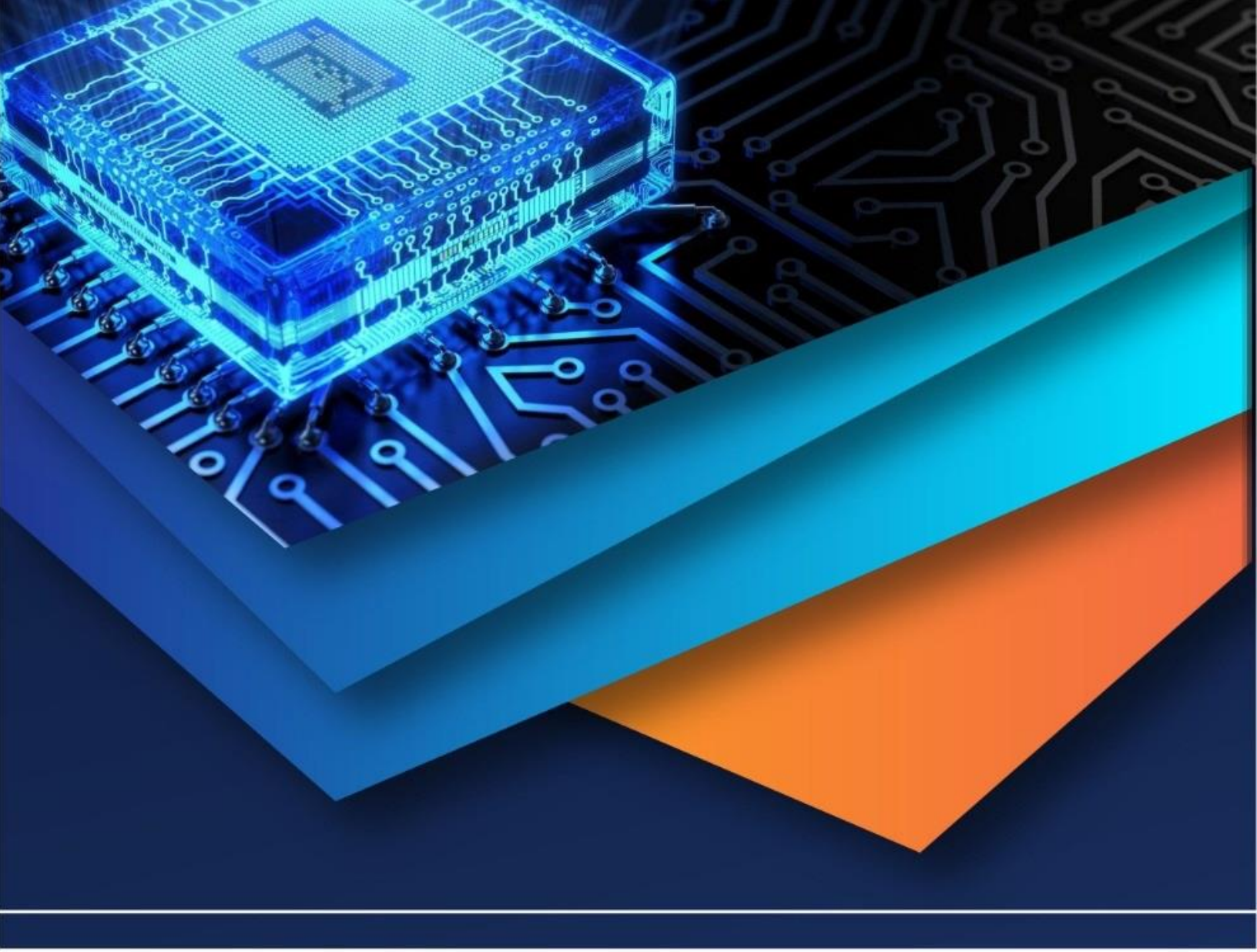
[6] M. Kutter, F. Jordan and F. Bosson, "Digital Signature of Color Images using Amplitude Modulation," in Proc. of SPIE, vol.3022, pp. 5 18-526, 1997.

[7] M.Barni, "Image Watermarking of Secure Transmission over Public Networks," in Proc. of Workshop on Emerging Techniques for Communication Terminals, Toulouse, France, pp.290-294, July 1997.

[8] Jung S. Cho, Seung W. Shin, Won H. Lee, Jong W. Kim, and Jong U. Choi, "Enhancement of Robustness of Image Watermarks Image Watermark into Colored Image, Based on Wt and Dct," in Proc. of Int. Conf. on Information Technology Coding and Computing, pp. 483 - 488, Mar. 2000

[9] G. Voyatzis and I. Pitas, "Applications of Torus Automorphisms in Image Watermarking," in Proc. of Int. Conf. on Image Processing (ICIP), vol. 3, pp. 237 - 240, Sept. 1996.

[10] N. K. Nishchal, "Optical image watermarking using fractional Fourier transform," J Opt, vol. 1, no. 38, pp. 22-28, Feb. 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY