iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5024

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: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Analysis of Secure Channel Establishment Techniques for Transmission of Watermarked Image

Manju Rani[1], Sanjay[2]
[1]*Student, Department of Computer Science, Himachal Pradesh Technical University, Hamirpur, India*
[2]*Head of Computer Science, SIRDA Institution of Technology, Sundernagar, (H.P), India*

Abstract: ***The image processing is the technology which can process the digital information which is stored in the form of pixels. The watermarking is the scheme which can hide the sensitive image behind the non sensitive image. The techniques of DWT, DCT are applied for the generation of watermarking images. In this research work, the diffie-helman and RSA algorithms are implemented to establish secure channel from source to destination to transmit watermarked image. On the destination, inverse operation is applied to extract original image from the watermarked image. The simulation of proposed modal is tested in MATLAB and it is analyzed that PSNR is increased and MSE value is reduced***
Keywords: DWT, DCT, SVD, RSA, Diffie-Helman.

I. INTRODUCTION

Image processing is the technique which can process the information which is stored in the form of pixels within the images. Image processing is a technique to perform a few operations on an image, with a specific end goal to get an enhanced image or to extract some helpful information from it. It is a kind of signal processing in which input is an image and output might be image or characteristics/features associated with that image. These days, image processing is among quickly growing technologies. It forms core research area within engineering and computer science disciplines as well. It is a kind of signal dispensation in which input is image, similar to video frame or photograph and output might be image or characteristics associated with that image . Typically Image Processing system includes treating images as two dimensional signals while applying effectively set signal processing methods to them. It is among quickly growing technologies today, with its applications in different parts of a business. Image Processing forms core research area within engineering and computer science disciplines as well. Digital watermarking is the act of concealing a message identified with a digital signal (i.e. an image, song, and video) inside the signal itself. It is a concept firmly identified with steganography, in that they both hide a message inside a digital signal. Be that as it may, what separates them is their goal. Watermarking tries to hide a message identified with the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is only utilized as a cover to hide its existence. Watermarking has been around for several centuries, as watermarks discovered initially in plain paper and consequently in paper bills . Be that as it may, the field of digital watermarking was just developed during the most recent 15 years and it is presently being utilized for various applications. In the analog world, an image (a photograph) has for the most part been acknowledged as a "proof of occurrence" of the depicted occasion . A shared secret is generated by establishing Diffie-Hellman algorithm with the help of which secret communications can be provided within which data can be exchanged across the public network. A password-authenticated key agreement (PAKE) form of Diffie–Hellman is utilized when a password is shared by Image a and Image b. This helps in avoiding the man-in-the-middle attacks occurring within the systems. With the help of password that is compute in independent manner on both ends of channel, a simple mechanism of comparison of hash is provided. Only one particular password for each iteration is tested with the other part as per the features of these schemes. This helps in generating a good security mechanism with relevance to the weak passwords within this system . As a part of public-key infrastructure the Diffie–Hellman algorithm is utilized. The RSA utilizes dominant public key algorithm due to which it is not at all similar to the Diffie-Hellman algorithm. A certificate authority is generated by RSA security in order to provide key signing. The certificates cannot be signed with the help of Diffie–Hellman algorithm. However, there is a relation amongst them.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

II. APPROACH

MATLAB solves many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in language such as C or Fortran. MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

III. SIMULATION AND RESEARCH METHODLOGY OF WATERMARKED IMAGE

With the rapid growth of internet the various digital methods has been proposed to protect the multimedia information from the non authorized accesses use and change. The water marking methods have been categorized as spatial domain method and frequency domain method. In spatial domain method we modify the lower order bits of cover image to embed the water mark. This work is based on the image watermarking in which original image can be hiding under the watermark image and it will be the final watermarked image. This technique increases the security of the images by using various type of encoding schemes. When the encoding schemes are applied to generate the final watermarked image, the properties of the original image need to be analyzed and these properties are color and textural properties. The propert

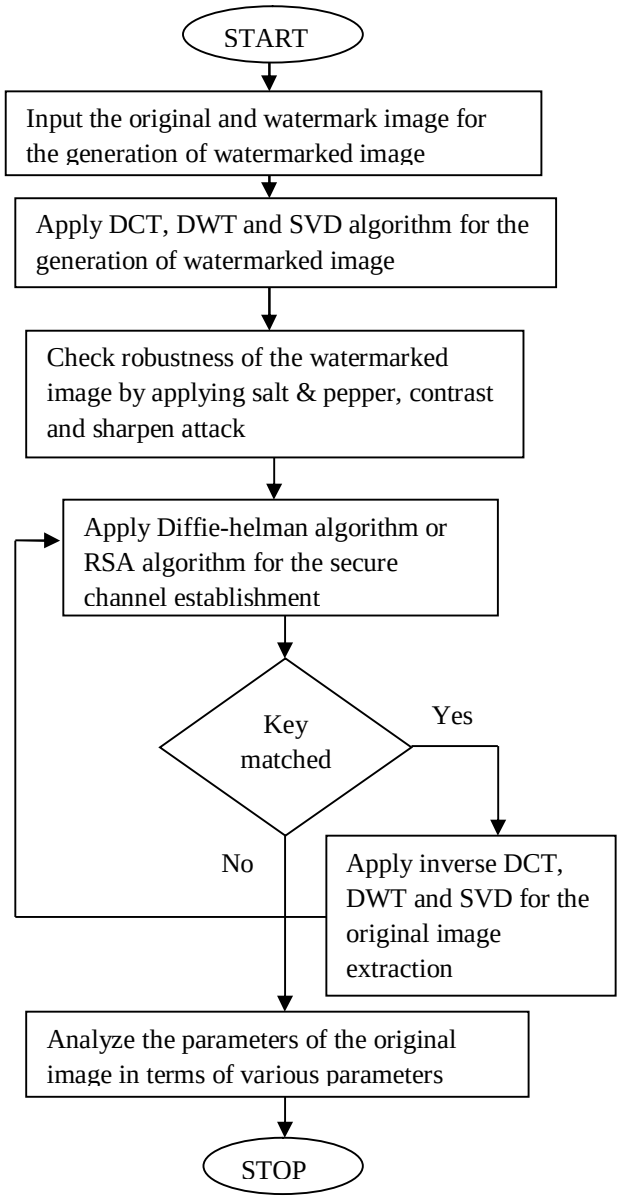


Fig. 2. Steps of Simulation

©IJRASET: All Rights are Reserved

These algorithms are based on wavelet transformation techniques for image processing. The encoding schemes which can be applied are RSA and Diffie-helman. These two algorithms are used to establish secure channel from source to destination and data which is watermarked data is transmitted through secure channels. In this work, RSA and Diffie-helman algorithm are compared in terms of security in image watermarking .The proposed algorithm consists of following steps :-

A. Pre-Processing Phase

pre-processing the first phase of the proposed algorithm. In this phase the size of the input and watermark image will be made size for the efficient watermarking

B. Apply DCT, DWT and SVD algorithm for watermarking

In the second phase, the DCT and DWT and SVD algorithm are applied which will generate the watermarked image.

C. Analyze Robustness' Of The Watermarked Image

In this phase, the watermarked image is analyzed by implementing salt & pepper, contrast and sharpen attack on the watermarked image.

D. Apply Secure Channel Establishment Algorithm

In the fourth phase, the algorithm of secure channel establishment is implemented which will establish secure channel from source to destination. In this steps proposed algorithm is analyzed under two algorithms. The first algorithm is RSA algorithm and second algorithm is diffie-helman algorithm. These two algorithms are used to establish secure channel from source to destination. This provides extra security to the watermarked image at time of transmission.

E. Extract of Watermarking

The watermarked image will be received at the destination and if the key which is generated gets matched with the entered key then the extract process takes place. To extract the original image from the watermarked image inverse SVD, inverse DWT and inverse DCT will be applied in the proposed algorithm.

IV. OVERVIEW OF DWT, DCT, SVD

The various methods used for watermarking embedding and its extraction are:

A. Discrete Wavelet Transform (DWT)

DWT is a partial transform and has the ability to multiscale analysis. The original image is decomposed into four sub-band images by DWT: three high frequency parts (HL, LH and HH, named detail sub-images) and one low frequency part (LL, named approximate sub-image). The detail sub-images contain the fringe information while the approximate sub-image is the convergence of strength of original image. Relative to the detail sub-images, approximate sub-image is much more stable, since the majority of image energy concentrates here. Therefore, watermark is embedded into approximate sub-image to gain a better robustness.

B. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain . It has been widely used because of its good capacity of energy compression and decorrelation. DCT is faster than DFT because its transform kernel is real cosine function while it is complex exponential in DFT.

C. Singular Value Decomposition(SVD)

If a m*n image is represented as a real matrix A , it can be decomposed as:

A= U S VT

It is called a singular value decomposition of A . Where U is a m*m unitary matrix, S is a m*n matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and VT denotes the conjugate transpose of V , an n*n unitary matrix. The nonnegative components of S represent the luminance value of the image.

Changing them slightly does not affect the image quality and they also don't change much after attacks, watermarking algorithms make use of these two properties.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

V. RSA

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone.

First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least i.e. numbers greater than 10154 [65]. We then generate the encryption key e which must be co-prime to the number $m = \varphi(n) = (p-1)(q-1)$. We then create the decryption key d such that de mod m = 1. We now have both the public and private keys.

A. Encryption

We let $y = E(x)$ be the encryption function where x is an integer and y is encrypted form of x.

$$y = x^e mod\ n$$

B. Decryption

We let $X = D(y)$ be the decryption function where y is an encrypted integer and X is the decrypted form of y

$$X = y^d mod\ n$$

C. Implementation

Selecting primes p = 3 and q = 11.

n = pq = 33 m = (p − 1)(q − 1) = (2)(10) = 20.

Try e = 3 gcd(3, 20) = 1 ⇒ e is co-prime to n

Find d such that 1 ≡ de mod m ⇒ 1 = Km + de Using the extended Euclid Algorithm we see that 1 = −1(20) + 7(3) ⇒ d = 7

Now let's say that we want to encrypt the number x = 9: We use the Encryption function y = x e mod n y = 93 mod 33 y = 729 mod 33 ≡ 3 ⇒ y = 3

To decrypt y we use the function X = y d mod n

X = 37 mod 33

X = 2187 mod 33 ≡ 9

⇒ X = 9 = x

VI. DIFFIE-HELLMAN ALGORITHM

A shared secret is generated by establishing Diffie-Hellman algorithm with the help of which secret communications can be provided within which data can be exchanged across the public network.

A. Example

Before establishing a symmetric key, the both the two parties need to choose two numbers n and p. Let n be a prime number and p be an integer [60]. The Diffie Hellman Problem (DHP) is the problem of computing the value of p^{ab}(mod n) from the known values of p^a (mod n) and p^b (mod n). The setup of Diffie Hellman algorithm

1) Suppose that we have two parties Image a (Master) and Image b (Slave), they want to communicate to each other.

2) They do not want the eavesdropper to know their message.

3) Image a and Image b agree upon and make public two numbers n and p, where n is a prime number and p is a primitive root mod n. Anyone has access to these numbers.

Image a	Image b
Choose a secret number a. Compute M≡ p^a (mod n)	Choose a secret number b Compute S≡ p^b(mod n).

Table 1: Private Computations

©IJRASET: All Rights are Reserved

4) Generated public values are exchanged.
5) Image a sends M to Image b ==M
6) S= Image b sends S to Image a
7) Image a calculate the number K≡ $S^a \equiv (P^a)^b$ (mod n).
8) Image b calculate the number $K \equiv M^b \equiv (p^b)^a$ (mod n).

Here Image a and Image b have the same key that is $K=p^{ab}$ (mod n). In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data, both agree on a symmetric key. For encryption or decryption of the messages symmetric key is used. We knows that Diffie Hellman algorithm is used for only key agreement or key exchange, but it does not used for encryption or decryption. Before starting the communication, secure channel is established between both the parties . Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

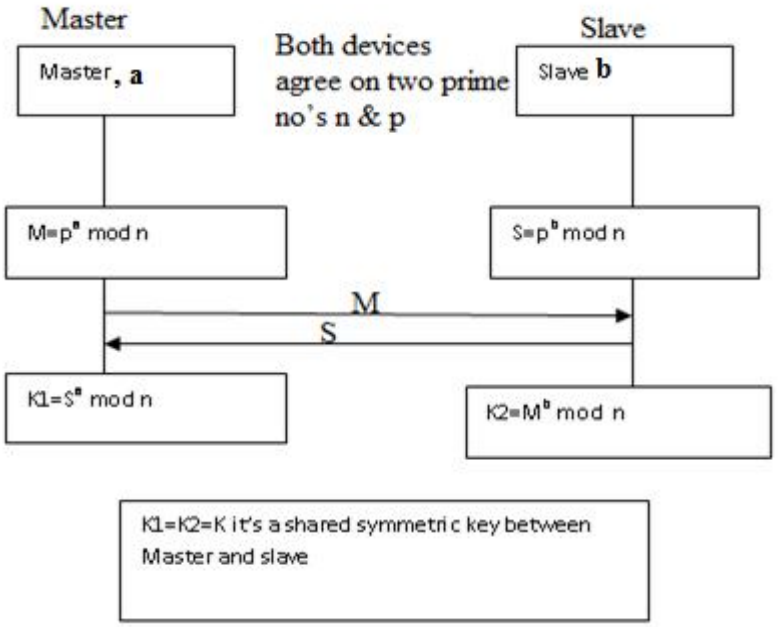


Fig. 2.Diffie-Hellman Key exchange

The above figure shows that Master and Slave want to communicate with each other. To start communication both parties need to establish secure channel. To establish secure channel, two random prime number p and n are selected, both devices are agreed on these two numbers. Selected p and n are the public numbers [62]. Both parties, say device 1 become master and device 2 become slave; both master and slave select their private numbers 'a' and 'b' respectively. Master and slave use their public and private number and calculated their private keys .

B. Master Computes
M= p^a mod n

C. Slave Computes
S= p^b mod n
Now both master and slave exchange their private keys such as 'M' and 'S'. After getting 'M' and 'S', master and slave calculates the secret keys such as K1, K2.

D. From S, Master Computes
K1= S^a mod n

E. From M, slave computes
K2= M^b mod n

©IJRASET: All Rights are Reserved

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of K1 and K2 becomes the shared symmetric key between master and slave .
To encrypt the messages, they used the public key or shared key (K) of both parties. For decryption of messages private key of both parties which is randomly chosen by the users i.e. 'a' and 'b' are used.

VII. QUALITATIVE ANALYSIS

The qualitative comparison is the in which the values of the algorithms are compared in terms of PSNR, MSE etc. The algorithms are diffie-helman, Basepaper algorithm and RSA algorithms


Fig. 3 Original Image


Fig .4 Watermark Image


Fig.5 Watermarked Image generation

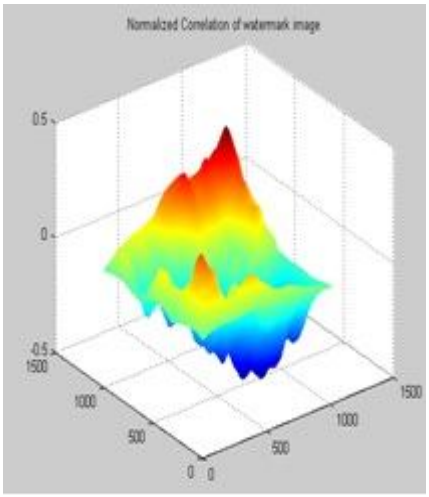
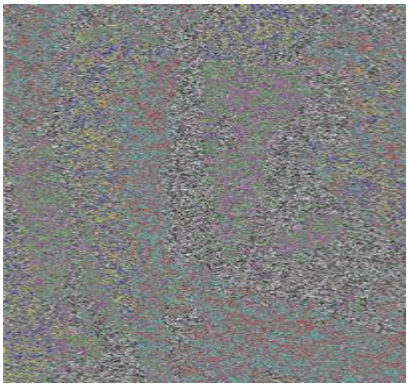


Fig.6 Normalized co-relation value


Fig.7 Apply Salt & pepper Attack


Fig.8 Apply Contrast Attack


Fig.9 Generation of encrypted image

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

	Parameter values	Basepaper Algorithm	Diffie-Helman	RSA
Watermarked image	PSNR	12.24	13.3917	18.0129
	MSE	3112.67	3001.26	2874.83
	Correlation Coefficient	0.01	0.01	0.01
	BER	6.78	7.9990	7.9989
Contrast Attack	PSNR	18.45	20.0542	26.0537
	MSE	789.56	647.22	547.30
	Correlation Coefficient	0.96	0.96	0.01
	BER	4.26	4.2319	4.2200
Sharpened Attack	PSNR	22.56	23.6209	29.4842
	MSE	290.67	284.70	243.80
	Correlation Coefficient	0.96	0.97	0.98
	BER	8.90	7.003	6.9047
Salt & pepper Attack	PSNR	21.67	22.4476	27.484
	MSE	378.78	373.00	293.80
	Correlation Coefficient	0.96	0.96	0.91
	BER	8.97	7.9012	7.9036
Decrypted image	PSNR	20.78	13.3848	18.0130
	MSE	3557.78	3006.02	3274.75
	Correlation Coefficient	0.1	0.01	0.00
	BER	8.965	7.6833	3.4237
Elapsed time		0.012789 sec	0.011795 sec	0.011994 sec

Table 2: Performance table of simulation with Diffie-helman and RSA algorithm

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

VIII. EXPERIMENTAL RESULTS

The proposed technique is implemented in MATLAB and the results are evaluated in terms of PSNR and MSE by making comparisons with existing algorithm.

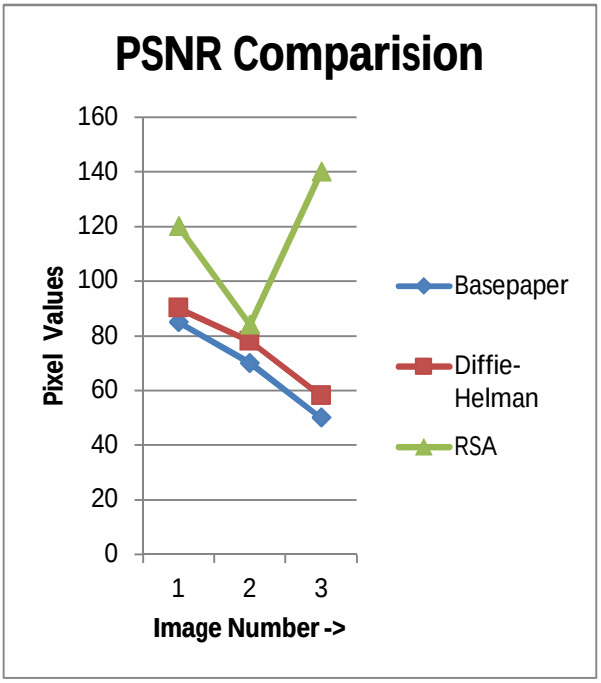


Fig 10: PSNR Comparison

As shown in figure 2, the comparison of proposed and existing algorithm is done in terms of PSNR. The algorithm which has maximum PNSR value is more reliable as compared to algorithm which has minimum PSNR value.

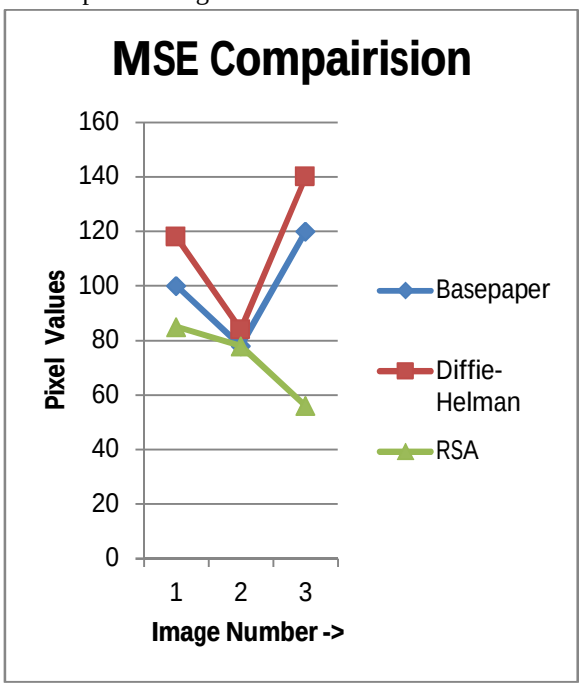


Fig 11: MSE comparison

As shown in the figure 3, the MSE of the proposed and existing algorithm is compared and it is been analyzed that algorithm which has high MSE value less reliable than the algorithm which has less MSE value.

©IJRASET: All Rights are Reserved

IX. CONCLUSION

The watermarking is the efficient technique which provides security to the original image. In this work, it is been concluded that to watermarked image is generated using DCT, DWT and SVD algorithms. To analyze the robustness of the watermarked image various attacks are implemented and these attacks are contrast, salt & pepper and sharpen attack. The differ-helman algorithm isapplied which will establish secure channel from source to destination. The performance of diffie-helman algorithm is comparedwith the RSA. It is been analyzed that performance of diffie-helman is matter than RSA in term of PSNR, MSE and SSIM.

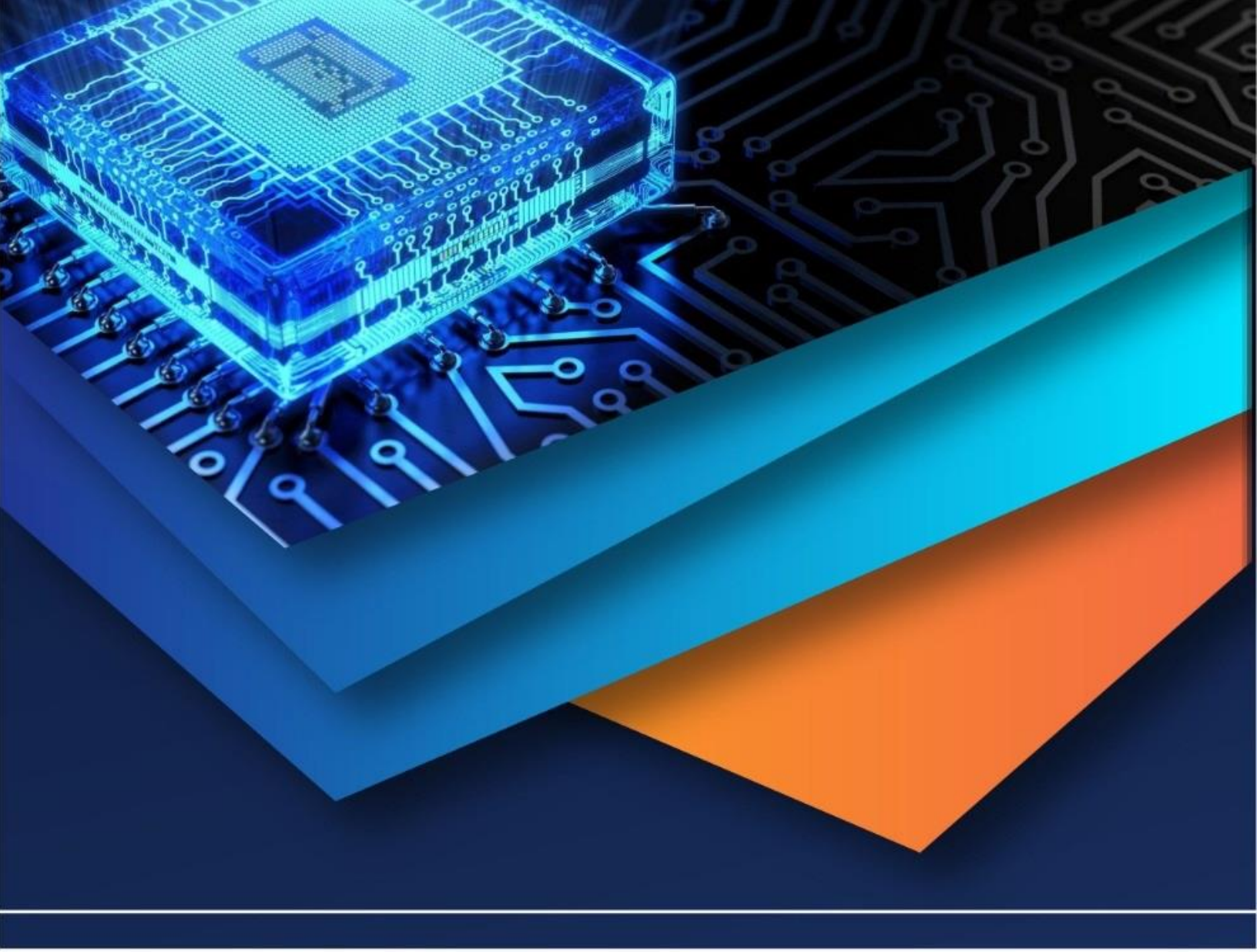
X. ACKNOWLEDGEMENT

I would like to take this opportunity to express gratitude to my advisor Mr. Sanjay and my parents for providing excellent guidance, encouragement and inspiration throughout the dissertation work. His extreme energy, creativity and excellent skills have always been a constant source of motivation for me.

REFERENCES

[1] M. Jiansheng and L Algorithm Based on DCT and DWT," International Symposium on Web Information System and Application (WISA), 2009, pp. 104-107.
[2] A. H. Ali and M. Ahmad, "Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition," Europe Journal of Science Research, Vol. 39, No. 1, 2010, pp. 6-21.
[3] W. Lu, H. Lu and F. L. Chung, "Feature Based Watermarking Using Watermark Template Match," Applied Mathematic
[4] Lu, K. Uehira and K. Yanaka, "Practical Evaluation of Illumination Watermarking Technique Using Orthogonal Transforms," Journal of Display Technology, Vol. 6, No. 9, 2010, pp. 351-358
[5] P. Zeng and C. Jin, "Image Adaptive Watermarking Using Visual Models," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, 1998, pp. 525-539.
[6] V. Nguyen and J. C. Patra, "A Simple ICA Based Digital Image Watermarking Scheme," Digital Signal Processing, Vol. 18, No. 5, 2007, pp. 762-776
[7] Shreyank N Gowda, "Advanced Dual Layered Encryption for Block Based Approach to Image Steganography", 2016, International Conference on Computing, Analytics and Security Trends (CAST)
[8] Zaid Y. Al-Omari, Ahmad T. Al-Taani, "Secure LSB Steganography for Colored Images Using Character-Color Mapping", 2017 8th International Conference on Information and Communication Systems (ICICS
[9] Mamta Jain, Rishabh Charan Choudhary, Anil Kumar, "Secure Medical Image Steganography with RSA Cryptography using Decision Tree", 2016, IEEE
[10] Nikhil Simha H.N., Pradeep M. Prakash, Suraj S. Kashyap, Sayantam Sarkar, "FPGA Implementation of Image Steganography using Haar DWT and Modified LSB Techniques", 2016 IEEE International Conference on Advances in Computer Applications (ICACA
[11] Shreyank N Gowda, "Dual Layered Secure Algorithm for Image Steganography", 2016, IEEE
[12] Sherin Sugathan, "An Improved LSB Embedding Technique for Image Steganography", 2016, IEEE

©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)