iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** XII **Month of publication:** December 2019

DOI: http://doi.org/10.22214/ijraset.2019.12027

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

Embedding and Extraction of Image Watermarking Based on the Discrete Wavelet Transform and Alpha Blending using RSA

Narendra Kumar S[1], Sagar N. P[2], Mohammed Waseem[3], Nishanth S[4]
[1]*Assistent Professor*, [2, 3, 4]*Dept. of CSE JNNCE*, Shivamogga

Abstract: Digital watermarking has become a promising research area to face the challenges created by the rapid growth in distribution of digital content over the iPnternet. To prevent misuse of this data, digital image watermarking techniques are very useful. Here, a new algorithm in the domain of discrete wavelet transform (DWT) is introduced and used for copyright protection. The elements of the logo watermark are embedded directly to the one-level DWT decomposed sub-bands. In addition to that, the watermark is encrypted using RSA algorithm for secure transmission of watermark. Few attacks have been conducted which shows the security of this work. The experimental runs and results of this work have shown that this proposed technique or method has the desired properties of digital image watermarking i.e. invisibility and robustness.
Keywords: DWT, digital Image Processing, Alpha-Blending, RSA and digital Image Watermarking.

I. INTRODUCTION

Digital image Watermarking is kind of image processing technique where in it inserts the digital data such as a watermark or digital signature or tag or label into an object of multimedia such a way that watermark could be retrieved or extracted or detected later. With the fast increment of new technologies on Internet, lots of people have focused rigorously towards the security and integrity of the information which transmitted through the network. Digital data and info protection is a crucial and an very important concepts in view of the owners of the products which comes under multimedia product category. Digital image watermarking processes includes mainly two major processes i.e. embedding and extraction of the data, embedding processes is meant for hiding the data inside the multimedia object such as image, video, and voice in such a way that it is impossible remove and the other process i.e extraction, its meant for verifying the ownership of the multimedia products. High imperceptibility i.e. low visibility and robustness & capacity are the two main aims which should be focused to achieve in digital watermarking scheme as a part of copyright protection.

There are mainly three types of digital watermarking techniques available in reality based on attacks on the watermark embedded multimedia object such as first based on fragile, second based on semi-fragile and finally based on robust. The embedded watermark which is going to be disappeared when the image is further processed for e.g. compression or resizing of a watermark embedded multimedia object is called more fragile. Similarly, the embedded watermark which is able to survive even though after attacking or by transformation using wide variety of attacking technique as well as the transformation technique is said to be highly robust.

The watermark which is less fragile but not completely robust is called semi-fragile watermark. The process of extraction of watermark might be cover image or embedded watermark dependent or independent. Based on required level information, this process is mainly categorized into blind and non-blind detection process. In non-blind watermarking, both cover data and embedded watermark is required for extraction. In blind watermarking, only watermarked data is required for extraction/detection of original cover data.

According to the section in which the watermark is embedded, the techniques are classified into two classes, i.e., spatial-domain and transform-domain methods. In spatial domain watermarking techniques, the watermark can be directly embedded within the image by modifying its pixel value.

The frequency domain technique for embedding watermark will follow the protocol initially by converting an image from spatial domain to equivalent frequency domain coefficients i.e transformation is applied in this case. These techniques includes as follows: first approach based on discrete cosine transform-(DCT), second approach based discrete Fourier transform-(DFT), third approach based on radon transform, fourth approach based on discrete wavelet transform (DWT), and so on. In the above said techniques, the digital image watermark is inserted the transformed co-efficient’s of a cover image image.

II. RELATED WORK

This section discuss about some previous work done on image watermarking.

Abdul R. Zubair presented the study about Digital watermarking in spatial domain[1]. Here the digital watermark in first stage is pre-processed by changing the image format from the rgb i.e. red-green-blue color space to an index image. Then the resulting index image usually carries a 2D matrix and an equivalent color map. This color map is preserved by storing it and it will be available as part of the watermark retrieval/extraction key. The 2D matrix of an index image is basically a kind of 2D gray-scale image which is in generally it is decomposed into a series/sequentially of binary i.e. 0 or 1 digital images using threshold decomposition technique such as stack filter's. Resulting output of binary digital images are then used to carry the implementation of multiple watermarking in the domain of spatial (pixels). Because of its higher dimensionality, robustness and copyright of ownership is achieved effectively by this multiple watermarking.

Vidyasagar M. Potdar, Song Han presented a Detailed survey of existing and newly proposed steganographic and watermarking techniques[2]. This paper provides classification of the watermarking techniques based on different domains in which data is embedded. Here author gave detailed analysis over 3 watermarking techniques, they are DCT, DWT and DFT. We also came to know about the requirements of digital watermarking like transparency, capacity and robustness. Applications of watermarking in several fields are also analyzed. Here we limit the survey to images only.

ShachiNatu, PrachiNatu presented, Digital image watermarking which is an improved Robust technique by using Singular Vector Decomposition - SVD and Hybrid Transform[3], which internally focuses on these two methodology of color image watermarking. Both the methodologies uses SVD as well as DCT as Walsh hybrid transform. The very beginning approach uses SVD on the hybrid transformation based on column of the host image or cover image and watermark images. And the next approach uses SVD on hybrid transform coefficients of column which is sorted in nature of host image and watermark images. In the said these two approaches, the coefficients of low frequency transform are used as a way of using middle frequency coefficients in dissimilarity.

Mauro Barni and Franco Bartolini presented a DCT-domain system for robust image watermarking[4] which is suitable for the marking of grey-level images. A pseudo-random sequence of real numbers having normal distribution with zero mean and variance of 1 is embedded in a selected set of DCT coefficients. This set is obtained by arranging the DCT coefficients in a zig-zag scan and by extracting the first L+M coefficients; then watermark is embedded in the following M coefficients, the L coefficients are skipped to preserve perceptual invisibility.

Ersin Elbasi and Volkan Kaya presented Robust Medical Image Watermarking using Frequency Domain and Least Significant Bits Algorithms[5]. Here both spatial domain (LSB) and frequency domain (DCT, DWT, DFT) watermarking techniques are used. The watermarking of images related to medical field has been by done using different methods like DWT, DFT, DCT and LSB algorithms. The calculations of peak to signal ratio (PSNR) and similarity ratio (SR) values on medical images via different algorithms is the main purpose of this study. In this work, logo images are inserted into the medical images using above mentioned methods and variety of attacks are carried out on the subsequent images. The best PSNR value could be found in the DFT method. The same kind of values would be found in DCT, DFT and LSB. As an output of hiding the data in MR images using coefficients of frequency domain is resist against a set of attack, and in the same way hiding the data using spatial domain resist against other set of attacks.

Sumedh P. Ingale and Prof. C. A. Dhote proposed a study on Digital Watermarking Algorithm using DWT technique [6]. In his work, watermarking technique based on a 3-level discrete wavelet transform has been implemented. In which DWT transform is performed on both host and watermark image and watermark is embedded the host image with a scaling factor 'a'. Experiment results shows that the quality of the watermarked image and the recovered watermark are dependent on the scaling factor 'a'.

III. METHODOLOGY

In this scheme, DWT technique used for image decomposition, alpha blending algorithm used for embedding and extraction of a watermark and RSA is used for encryption of watermark and its decryption

A. Discrete Wavelet Transform (DWT)

A DWT is any wavelet transform for which the wavelets are discretely sampled in proper time interval. It is useful for processing of non-stationary signals. DWT is very suitable to identify the areas in the cover image where a watermark (logo) can be embedded effectively. This property allows the exploitation of the masking effect of the human visual system (HVS) such that if a DWT co-efficient is modified. Hence, it modifies only the region corresponding to that coefficient.

In this transform technique a small waves in generally it is called wavelets of frequency which will be varying with a the limited duration used as mother wavelet. These Wavelets are generated in nature by translations as well as by using dilations of a fixed

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

function which is said to be mother wavelet. This transform of wavelet provides in nature both frequency as well as spatial description of a digital image.

A function (signal) f(x) which implements DWT can be decomposed into a sum of scaling and wavelets functions shown in eq (1) :

$$f(x) = \frac{1}{\sqrt{M}} \sum_{k} W_{\phi}(j_0, k)\phi_{j_0,k}(x) + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_{k} W_{\psi}(j, k)\psi_{j,k}(x), \quad j, k \in \mathbb{Z}, \qquad (1)$$

Where j0 is the starting scale, M is the size or length of the signal, W(j,k) and W(j0,k) are details and approximation coefficients, respectively.

For image, the decomposition of signal f(x, y) of size MxN given in eq (2):

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{m} \sum_{n} W_{\phi}(j_0, m, n)\phi_{j_0,m,n}(x,y) + \frac{1}{\sqrt{MN}} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_{m} \sum_{n} W_{\psi}^{i}(j, m, n)\psi_{j,m,n}^{i}(x,y) \qquad (2)$$

The DWT generally divides the image signal into low and high frequency subsequent parts. the low frequency part is split again into high and low frequency parts and The high frequency part is very important because it contains information about the edge components. Then as usual high frequency components recommended for watermarking purpose because the human eye is very hard to detect changes in edges because human eye is less sensitive.

In 2-D applications, both cover image and watermark is first pre-processed by converting it from the rgb color image to a grey scale image. The 2D matrix are created which essentially a 2D gray-scale images which are decomposed. The resulting digital images are then used to implement multiple watermarking. With this decomposition, the 2D signal is filtered by the filter coefficients g(n) (low-pass filter) and h(n) (high-pass filter) that have two directions X and Y along with a down-sampling in each direction to produce the coefficients of the four sub bands(LL, LH, HL, HH).There are many classes of filters such as Haar, Daubechies, Orthogonal and Bi-orthogonal filters etc. These converts the given input into the series x_0, x_1....x_m having both series of High-pass wavelet coefficient as well as series of Low-pass wavelet coefficient. After decomposition of the image, the details coefficient and approximation coefficients are obtained which are used by inverse DWT to recompose the original image.[7-8]

Soon completing the decomposition of first level, we are able to get 4 sub-bands such as 1) LL1, 2) LH1, 3) HL1, and 4) HH1 which are depicted in the figure 2.1.

LL_1	HL_1
LH_1	HH_1

Figure 2.1: One-level decomposition of an image

B. Watermark Embedding and Extraction using Alpha-Blending Algorithm

1) Embedding Algorithm

a) For this process first we need to apply one-level DWT decomposition on host image. This decomposes the image into 4 sub-images, 3 details parts and 1 approximation part. The approximate part appears to be like the original.

b) In the same manner one-level DWT is also applied to the watermark image. For this process Haar wavelets is used.

c) Then the technique of alpha blending is implemented for insertion the watermark in the host image. In this technique the decomposed components of the host image and the watermark are multiplied by a scaling factor and are added.

Formula of the alpha blending embedding for watermarked image is given in eq (3)

$$WI=k*(LL1) +q*(WM1) \qquad (3)$$

Where, WM1 = low frequency approximation of Watermark, LL1 = low frequency approximation of the original image, WI=Watermarked image, k, q- Scaling factors

After embedding the watermark Image within host image Inverse DWT is applied to obtained watermarked image coefficient to generate the final secure watermarked image (WI).

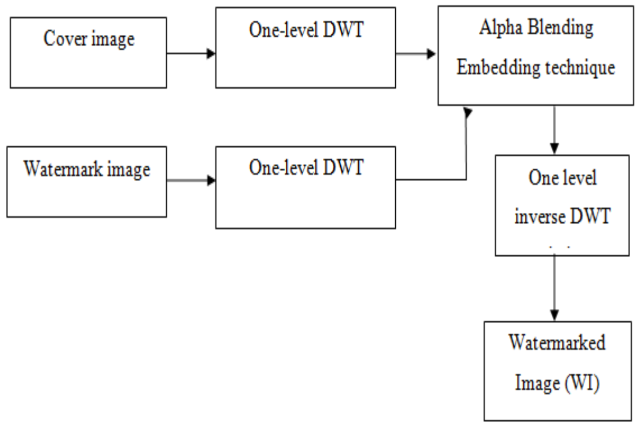


Figure 2.2: Watermark embedding process using Alpha-Blending

2) *Extraction Algorithm*

a) For extraction first we applied 1 level DWT to watermarked image (WI) and cover image which decomposed the image in sub-bands.

b) After this we implement alpha blending method on low frequency components.

Formula of the alpha blending extraction for Recover watermark is given by is given in eq (4)

$$\mathbf{RWI = (WMI - k*LL1) / q} \qquad (4)$$

RWI= is the recovered watermark approximation in Low frequency, LL1=Low frequency approximation of the cover image, and also WMI= watermarked image low frequency approximation..

After extraction process, Inverse DWT is applied to the watermark image coefficient to generate the final watermark extracted image.

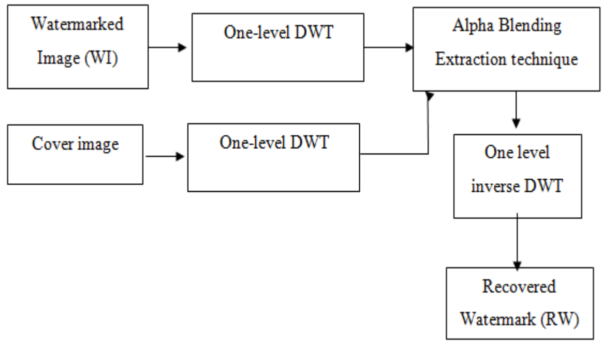


Figure 2.3: Watermark extraction process using Alpha-Blending

C. RSA Encryption and Decryption

RSA algorithm meant for transmitting the data securely and is very initial practiced public-key cryptosystems which is very rigorously used. In encryption processes is public in nature by encryption public key and in the same way the decryption is private in nature by using private decryption key in the entire cryptosystem. In RSA, this kind of asymmetry approach is based on the system of factoring the product of two very large prime numbers which is said to be factoring problem. [4].

In this scheme RSA is used to encrypt and decrypt watermark (logo).

It involves mainly three different steps as shown below:

1) First - Key Generation

2) Second – Encryption

3) Third - Decryption

a) Choose two large distinct primes p and q**.** Prime numbers should be chosen at random, and bit-length must be of similar.

b) Compute n = pq, in which the product will be used as modulus (%) operator for both kind of keys such as the private and public.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

c) Then, Compute $f(n) = (p - 1)*(q - 1)$, in which f meant for Euler's totient function.
d) Choose public exponent e to be co-prime to f(n). with $1 < e < f(n)$ and gcd (e, f(n)) = 1;
e) Next The pair (n, e) which is the public key.
f) The next key is said to be private key is the unique numeric integral value $1 < d < f(n)$ such that e mod d = 1
g) Encryption: Lets treat $M_1, M_2, \ldots, M_i$ be the coefficient of image block in frequency domain. where each and every M_i satisfies $0 \leq M_i < n$. Then these blocks will be encrypted by using equation 5.

$$\mathbf{C \equiv E(M) \equiv M\hat{}e \ (mod\ n)} \qquad (5)$$

h) *Decryption:* In this stage a given private key d and the generated cipher text C.
The function of decryption is shown in equation 6.

$$\mathbf{D(C) \equiv C\hat{}d \ (mod\ n)} \qquad (6)$$

Thus the encryption key is a positive integer pair (e; n). in the same way, the pair of positive integers (d; n) is a decryption key. Each user makes his own encryption key public, and in the same way keeps the corresponding generated decryption key privately.

D. Overall System Design

Using RSA, DWT and Alpha-Blending techniques a complete system design is implemented.

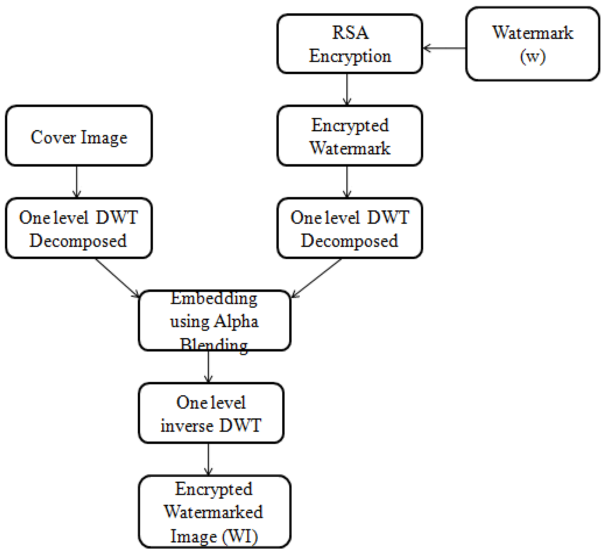


Figure 2.4: Phase of Embedding watermark

Figure 2.4 depicts the complete phase of embedding in this scheme.

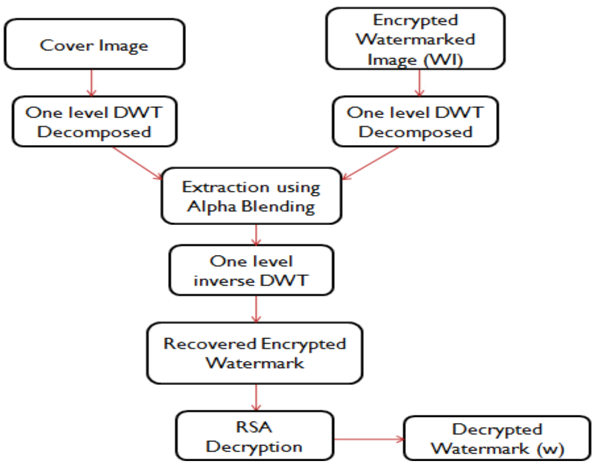


Figure 2.5: Watermark Extraction Phase

Figure 2.5 shows complete watermark extraction phase of this scheme.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

IV. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

In order to evaluate the performance of the watermarking algorithm, the Imperceptibility, the Peak Signal-to-Noise Ratio (PSNR), and Mean Square Error (MSE) must be evaluated.

A. Imperceptibility

Imperceptibility is one of the important requirements of digital watermarking. Imperceptibility depends on human visual system which intern points to the quality of the multimedia object which is watermarked in nature which noticed visually. This, the approach of digital watermarking inserts the watermark into an original image and its not visible directly for observing in sense. Usually distortion will be introduced when an embedding process has been carried out. Hence, we are supposed to use proper embedding approach in order to have very less or minimal distortion in the original image multimedia content.

B. Mean Squared Error - MSE

MSE is a basic methodology in order to check the distortions usually between the cover image as well as the watermarked image. By analyzing the value of MSE one can determine the changes in the watermarked image. The Equation -7 will elaborates about the MSE operation, in which MxN is the said to be the size or length of the host image or watermarked image and MSE is the mean square error between these two images.

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x(i,j) - y(i,j))^2, \qquad (7)$$

C. Peak Signal to Noise Ratio (PSNR)

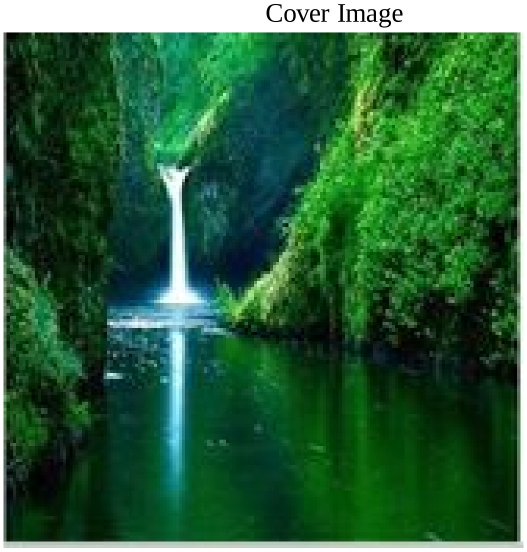
This PSNR, strategy is mainly used to estimate the embedded quality with reference to imperceptibility i.e . Visibility, and its criteria is meant to evaluate original/cover image and the watermarked image similarity. This in generally a better test in order to check distortions usually between watermarked image as well as cover image because mean squared error is also used in this process. Equation – 8 used to estimate the PSNR of the two images.

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{\mathrm{Max}(x(i,j))^2}{\mathrm{MSE}} \right), \qquad (8)$$

A high PSNR refers watermarked image has good imperceptibility and it is highly similar to the host image. The nature of lossy image is checked usually by this PSNR. Thus, basically image for this kind of situation is the information, and in the same way noise is the error. The human view of reconstruction or reproduction quality will be estimated by this PSNR. The 39 dB is the least acceptable PSNR value .

In figure 2.6 cover image and watermark to be embed are selected both of size 512X512.

Cover Image



Watermark

Figure 2.6 Cover Image and Watermark of size 512X512

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

Watermark is encrypted using RSA encryption which is shown in figure 2.7.

Figure 2.7: Encrypted Watermark using RSA

After applying one-level decomposition on both cover image and encrypted watermark image and embedding them using alpha blending embedding, encrypted Watermarked image is obtained which is shown in figure 2.8.

Figure 2.8: Encrypted Watermarked Image

To extract the watermark again we need to apply one-level decomposition on cover image and encrypted watermarked image and extract encrypted watermark using alpha blending extraction which is shown in figure 2.9.

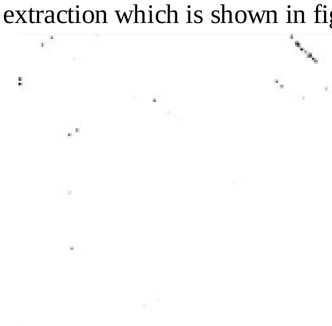


Figure 2.9: Encrypted Watermark

After applying RSA decryption, finally watermark is recovered shown in figure 2.10.

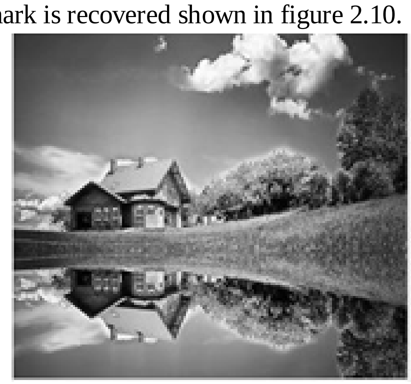


Figure 2.10: Decrypted Watermark

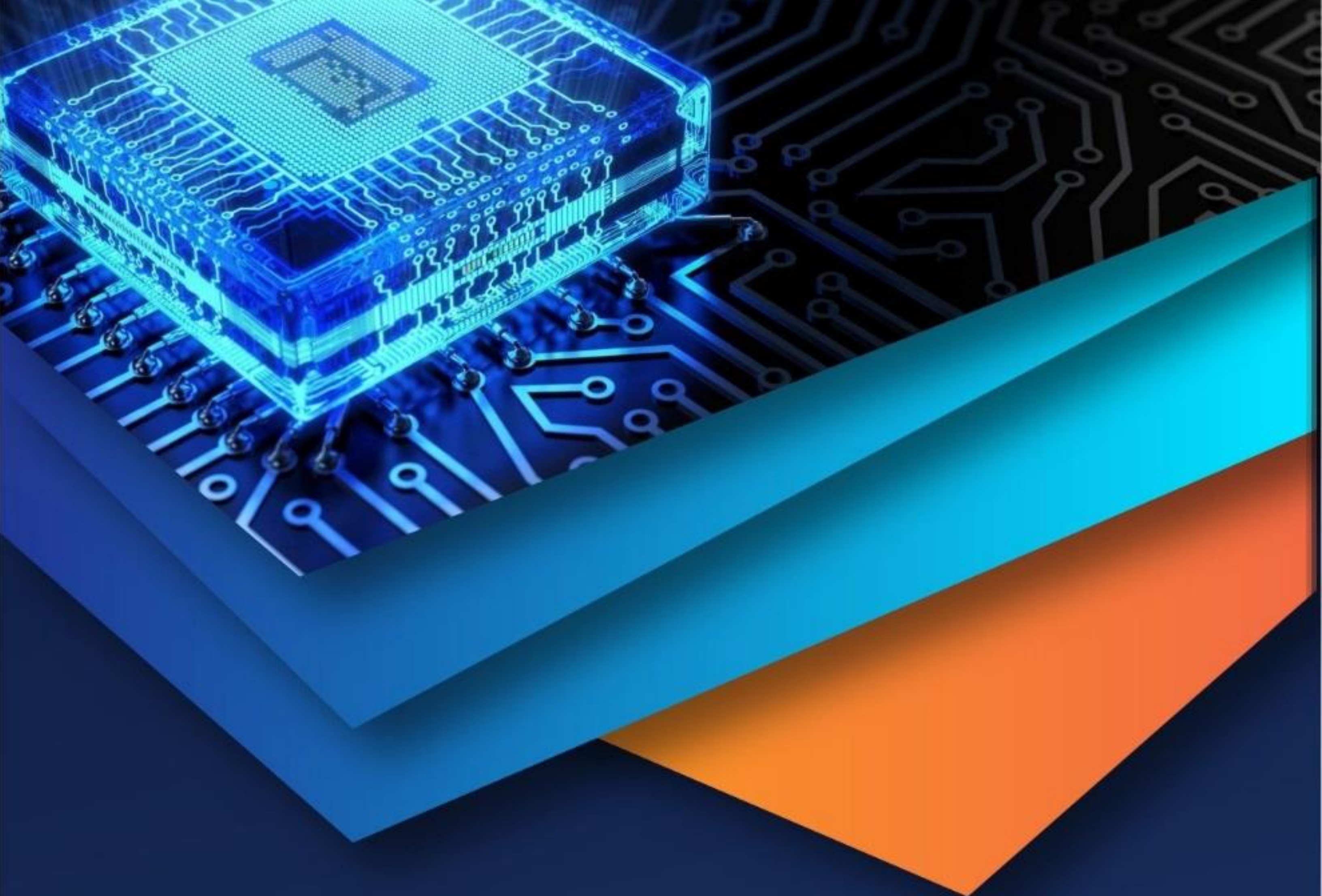
V. CONCLUTION AND FUTURE SCOPE

A novel robust digital image watermarking technique based on DWT is introduced. Here DWT properties are mainely focused to accomplish the watermarking requirements. These properties are detection of an in the cover image and also the perfect reconstruction of the DWT as an original cover image. This scheme also uses RSA public-key encryption for more secure transmission of watermark. The executed results which are shown above proves that the proposed scheme is very imperceptable with PSNR having good value and good resistant towards variety of cryptographic attacks.

In future work we can include embedding of multiple watermarks within a single cover image. The DWT technique for decomposition can be extended to include 3-level decomposition. Considering robustness criteria, extraction process can be extended to blind technique to produce more robust digital watermarked image.

REFERENCES

[1] Abdul R. Zubair, Olasebikan A. Fakolujo, Periasamy K. Rajan: Digital watermarking of still images with color digital watermarks, IEEE EUROCON (2009)
[2] Vidyasagar M. Potdar, Song Han, Elizabeth Chang: A Survey of Digital Image Watermarking Techniques. 2005 3rd IEEE International Conference on Industrial Informatics.
[3] ShachiNatu, PrachiNatu, TanujaSarode: Improved Robust Digital Image Watermarking with SVD and Hybrid Transform. International Conference on Intelligent Communication and Computational Techniques (ICCT), IEEE (2017).
[4] Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva: A DCT-domain system for robust image watermarking. Dipartimento di Inegneria Elettronica, Universita. Firenze, Italy. (1997)
[5] Ersin Elbasi,Volkan Kaya: Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms. IEEE (2018).
[6] Sumedh P. Ingale, Prof. C. A. Dhote: Digital Watermarking Algorithm using DWT technique.International Journal of Computer Science and Mobile Computing. IJCSMC, Vol. 5, Issue. 5, May 2016, pg. 01 – 09.
[7] E.Najafi: A robust embedding and blind extraction of image watermarking based on discrete wavelet transform.MathSci (2017) 11:307–318
[8] P. K. Sharma, Rajni, "Analysis of Image Watermarking Using Least Significant Bit Algorithm International" Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY