



Fusion of Fractal Color Watermarking with RSA

Maninder Kaur¹, Manish Sachdeva²

Lecturer, Mehr Chand Polytechnic college, Electronics and Communication¹

Incharge, Mehr Chand Polytechnic college, Electronics and Communication²

Abstract: Now day's security is an important aspect of life. We require security in every part of communication to transmit our information safely. Here our main aim is to secure the important information hidden in the images, while communicating we are hiding watermark inside the image by using RSA algorithm. To obtain very high image quality we use Fractal color image watermarking. Firstly we encrypt the watermark using RSA and then this encrypted watermark is used to hide inside the image using Fractal color image watermarking. To achieve watermarking we convert RGB into space. Also we are trying to achieve better parameters like PSNR (power signal to noise ratio), BER (Bit error rate) and MSE (Mean square Error).

Keywords: DCT, DWT, HVS, CIE, SCDFD etc

I. INTRODUCTION

As the growth of internet is increasing these days so it is very important to keep the information from illegal distribution [2]. Data such as image, video, audio are readily produced again and distributed. For decades people strove to develop innovative methods for secret communication. The standard and concept of "What You See Is What You Get (WYSIWYG)" which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS), hence, they can convey more than merely 1000 words.

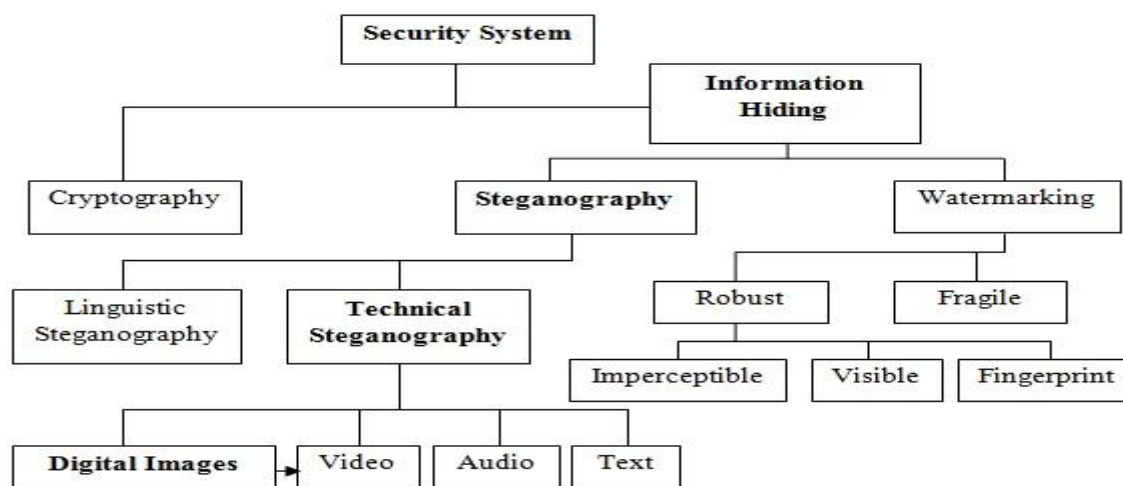


Fig. 1 The different embodiment disciplines of information hiding. The arrow indicates an extension and bold face indicates the focus of this study.

So cryptography technique is invented so to provide secrecy in communication and many other methods built to encrypt or decrypt the data. This technique is used to hide the contents of the message secret whereas a technique is invented to keep the existence of the message secret which is known as steganography. In steganography we hide data inside other data so to keep the secrecy of existence.

Depending on the domain in which watermark is embedded digital image watermarking algorithms classified into two categories that are spatial domain[3,4] and the transform domain which again have three types that is Discrete cosine transform(DCT)[5,6], Discrete fourier transform(DFT)[7], Discrete wavelet transform(DWT)[8,9]. By reorganizing a preselected set of pixels in the image we can insert watermark in spatial domain technique. Watermark is embedded into the image by modifying the transformed frequency coefficients in transform domain watermarking. We know that



HVS is more sensitive to low-frequency coefficients and less sensitive to high-frequency coefficients [10,11]. Advantage of watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral many methods are realized by embedding watermarks in the image luminance or by processing each color channel separately.

Kutter et al. [12] proposed a method for embedding a watermark in the blue component because the change in blue component is insensitive to human eyes. Barni et al. [13] introduced a color image watermarking scheme. Where host image contains a subset of full frame DCT coefficient of each color channel which is modified to embed watermark in it. Tsai et al. [14] introduced a scheme where in quantized color image they embed a watermark in it. Tsui et al. [15] provided a solution where by using the spatio chromatic discrete fourier transform (SCDFT) they embed a watermark in the frequency domain of the chromatic channels. Whereas Tsui's introduced a method, in which achromatic content is encoded as *CIE L* tristimulus value and chromatic content of a color image is encoded into *CIE a*b** chromaticity coordinates. Kuo and Cheng [16] introduced a color watermarking method in which by using principal axes analysis in 3-D color space they combine color edge detection and color quantization. Chou and Liu [17] presented a color image watermarking plan that shrouds watermark motions in most contortion mediocre signs inside of three color channels of the host image without coming about in recognizable distortion in wavelet domain. Vahedi et al. [18] proposed a watermarking scheme where with the aid of the visual characteristics of the host image and so forth controls strength of the embedded watermark locally.

Actually the idea of fractal image coding (FIC) was originally introduced by Barnsley and Demko [19]. And the first practical fractal image coding method is achieved by Jacquin in 1992 [20]. Davern and Scott [21] described a steganographic method for inserting secret information into images using fractal image coding for studying gray level image watermarking. The method permitted a client to indicate a visual key when concealing the mystery data. The visual key must then be utilized when recovering the covered up information.

Here in our work we are hiding a grayscale watermark image inside color image into the range block means by converting the watermark into pseudorandom binary sequence and to identify the procedure we used to calculate the correlation between the original watermark and extracted watermark. Before embedding we encode RSA algorithm inside watermark image where RSA generate public and private key as shown in Figure 1. Then for measuring the quality of image we are using PSNR. To measure the difference between original watermark image and extracted watermark image we are using MSE. To check the robustness of image we are using BER.

II. FRACTAL COLOR WATERMARKING

Fractal image coding involves as a self similarity in images which are use to compress the image data. In these image compression methods, the picture is divided into blocks. As per the property of self-comparability, for every block, a fractal change can be obtained, which is determined by some fractal parameters. Like in Fractal color watermarking we consider a color pixel as 3D vector in RGB space than a luminance offset vector is substituted by the range block mean vector. Then we hide watermark in range block mean vector which is explained below. There are two sorts of methods for inserting a predefined watermark into a picture. First one is pseudorandom sequence utilized for objective recognition; the other one is gray image or binary picture utilized for subjective recognition [2]. In this paper, keeping in mind the end goal to subjectively confirm the responsibility for picture with the guide of separating a watermark, a grayscale image is utilized which is further converted into binary form, the watermark bit is either 1 or 0. One of the main difficulties of the watermarking is to accomplish a trade-off in the middle of perceptivity and good robustness. As a rule, expanding the quality of the installed watermark can accomplish robustness, yet it would prompt an increment in the visible contortion too, and the other way around [22]. Well the orthogonalized fractal decoding is a mean-invariant cycle, the range block mean is a decent strong spot to hide a watermark, as examined. Then after fractal decoding, the inserted watermark diffuses all through the recreated image.

So as to increase high robustness and in addition low sensitivity in color image watermarking, the information of human visual impression of color boosts must be all around used in embedding algorithm for outlining. It is well realized that the human visual system (HVS) is not immaculate sensor of seeing color visual data. Despite the fact that the HVS is especially delicate to changes in picture hue, it is less delicate to the yellow-blue segment. *CIE La*b** is the most finish color model ordinarily used to depict the greater part of the hues that are noticeable to the human eye [10].

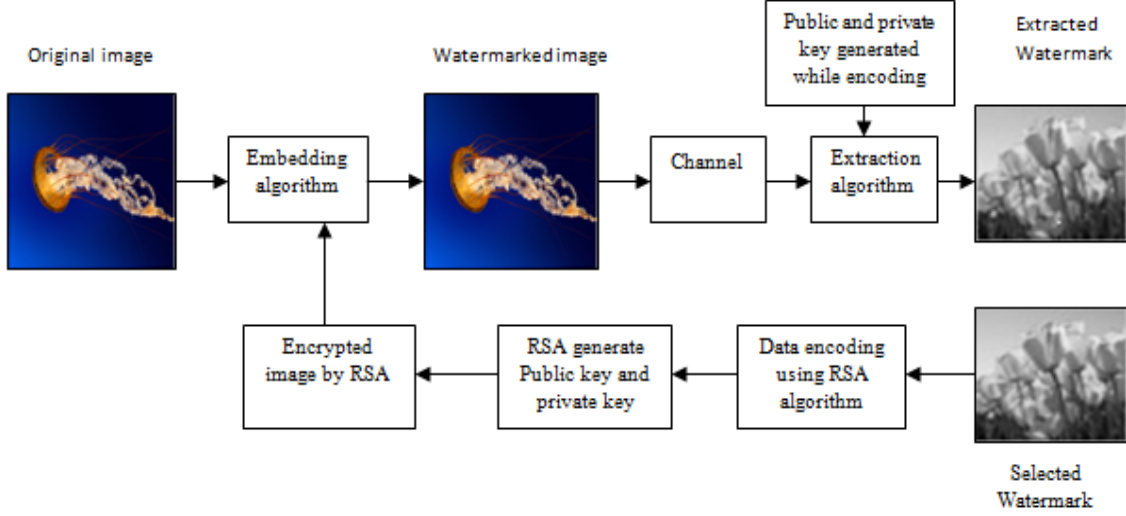


Fig. 2 Insertion and Extraction procedure of Watermark using RSA

The parameter L speaks to the softness of the color, while a^* , b^* are chromatic data. Furthermore, a^* is constantly named magenta- green pivot and b^* is named yellow-blue pivot. In view of the perceptions, in the method here, we will change over the r , g , and b estimations of the range block means $\{R_u\}_{u=1}^n$ to La^*b^* space before they are embedded watermark $\{w_u\}_{u=1}^n$. The change from RGB space to the $CIE La^*b^*$ space is through the XYZ space. Firstly by linear transformation we can convert RGB space into XYZ space.

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.490 & 0.310 & 0.200 \\ 0.177 & 0.813 & 0.011 \\ 0.000 & 0.010 & 0.990 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

And then through a non linear transformation we convert XYZ space into $CIE-La^*b^*$ space

$$L = 166f\left(\frac{Y}{Y_0}\right) - 16,$$

$$a^* = 500 \left[f\left(\frac{X}{X_0}\right) - f\left(\frac{Y}{Y_0}\right) \right] \quad (2)$$

$$b^* = 200 \left[f\left(\frac{Y}{Y_0}\right) - f\left(\frac{Z}{Z_0}\right) \right]$$

Where

$$f(t) = \begin{cases} t^{1/3}, & \text{if } t > 0.008856 \\ 7.787x + \frac{16}{116}, & \text{otherwise} \end{cases} \quad (3)$$

And reference white color is represented by X_0 , Y_0 , Z_0 . Alternately, the reverse change is effectively communicated by utilizing the inverse of the function f :

$$Y = Y_0 f^{-1}\left(\frac{(L + 16)}{116}\right),$$

$$X = X_0 f^{-1}\left(\frac{(L+16)}{116} + \frac{a^*}{500}\right), \quad (4)$$

$$Z = Z_0 f^{-1}\left(\frac{(L + 16)}{116} - \frac{b^*}{200}\right)$$



Where

$$f^{-1}(t) = \begin{cases} t^3, & \text{if } t > 0.2069 \\ 0.1284 \left(t - \frac{4}{29}\right), & \text{otherwise} \end{cases} \quad (5)$$

The color contrast ΔE at each pixel is characterized by

$$\Delta E = \sqrt{(\Delta L)^2 + (\Delta a^*)^2 + (\Delta b^*)^2}. \quad (6)$$

In particular review condition, there leaves a certain measure of data that is not distinguishable by the human eyes. Tests have demonstrated that $\Delta E < 1$ is not distinguishable by the HVS, and $\Delta E < 3$ is not clear. When $\Delta E = 3$ it is called as the uniform just noticeable color difference (UJNCD). Since the affectability of the HVS to the yellow-blue segment is roughly 1/5 contrasted with the luminance segment, we can set $\Delta L = \Delta a^* = 1/5 \Delta b^*$. Along these lines, in the event that we set $\Delta b^* = 1.5$, then $\Delta L = \Delta a^* = 0.3$ what's more, $\Delta E \approx 1.56 \ll 3$. Let's take haphazardly scrambled watermark which is represented by $\{W_u\}_{u=1}^n$ the procedure for inserting a watermark is shown in Figure 3 and incorporates the accompanying steps.

- (1) Using full pursuit plan Fractally encode the original image to deliver the fractal codes $\{\bar{R}_u, A_u, \vec{x}_u\}_{u=1}^n$ in RGB space, where the position of the optimal domain block is represented by $\vec{x}_u = (x_u, y_u)$.
- (2) After fractally encoding convert the range block means $\{\bar{R}_u\}_{u=1}^n$ from RGB space to $L a^* b^*$ space and indicate them by $\{\bar{R}'_u\}_{u=1}^n$
- (3) Embed the grayscale watermark $\{w_u\}_{u=1}^n$ into $\{\bar{R}'_u\}_{u=1}^n$
 - i. Replace $\bar{R}'_u$ with $\bar{R}_u^* = \bar{R}'_u + \zeta$, where $\zeta = [0.3, 0.3, 1.5]^T$ if the message which is to be inserted is $w_u = 1$.
 - ii. else, if $w_u = 0$, replace $\bar{R}'_u$ with $\bar{R}_u^* = \bar{R}'_u - \zeta$.
- (4) Convert $\{\bar{R}_u^*\}_{u=1}^n$ back to RGB space and indicate them by $\{\bar{R}_u^*\}_{u=1}^n$
- (5) Hide the watermark by performing fractal interpreting utilizing $\{\bar{R}_u, A_u, \vec{x}_u\}_{u=1}^n$.

Now to extract the implanted watermark, we need original image and watermarked image so that we can compute $\bar{R}'_u + \zeta$ and $\bar{R}'_u - \zeta$ from the original image in $L a^* b^*$ space, trailed by a separation correlation of $\bar{R}'_u$ with the watermarked picture. In the event here outcome is 1 if extracted $\bar{R}'_u$ is closer to $\bar{R}'_u + \zeta$, otherwise "0" was inserted. The watermark extraction digram is illustrated in figure 3

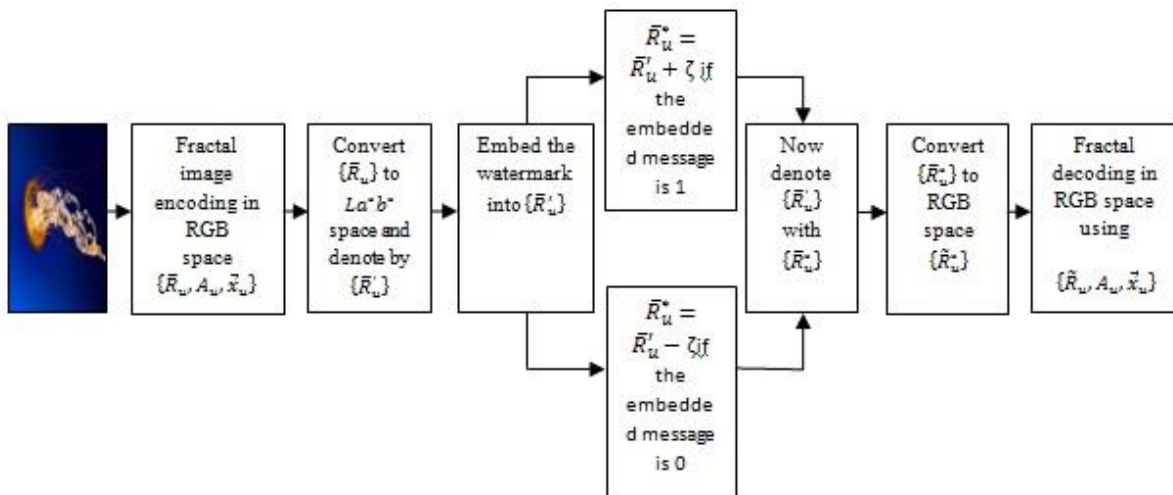


Fig. 3 Watermark embedding using Fractal color image watermarking procedure

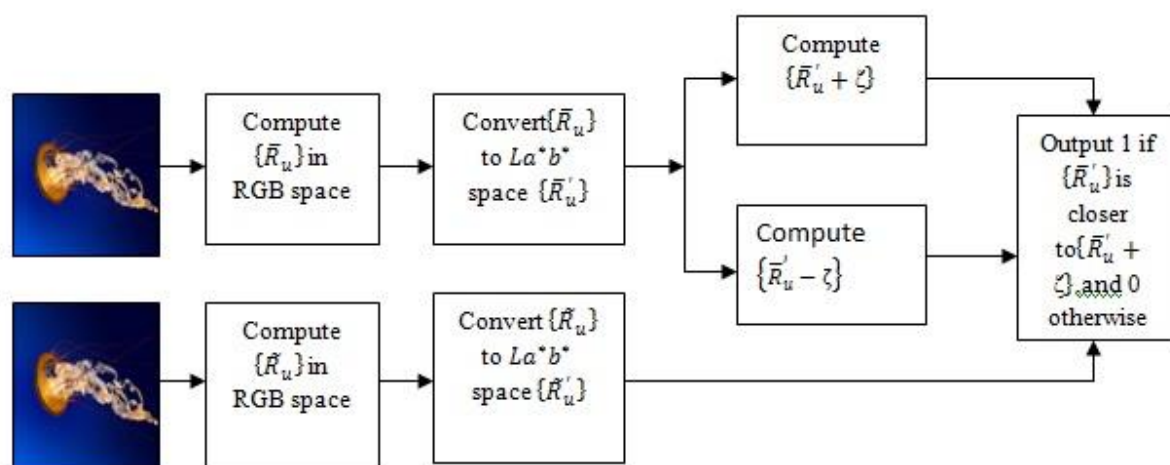


Fig. 4 Procedure for extracting Watermark

III. RSA ALGORITHM

The RSA algorithm is named after Ron Rivest, Adi Shamir, and Leonard Adleman developed in 1977 — is based on a property of positive integers that we portray underneath RSA includes an public key and private key. In general public key can be known to all, it is utilized to encrypt messages. Messages encrypted utilizing public key must be decoded using reasonable amount of time with the private key. The keys for the RSA algorithm are produced the accompanying way:

- (1) Pick two distinct prime numbers p and q . For security purposes, the whole numbers p and q ought to be picked indiscriminately, and ought to be of comparable bit-length. Prime whole numbers can be effectively discovered utilizing a primality test.
- (2) Calculate $n=pq$. Where n is utilized as the modulus for both public and private keys. Its length, typically expressed in bit.
- (3) Calculate $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = n - (p+q-1)$, where ϕ is Euler's totient function. This value used to keep private.
- (4) Pick a whole number e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; i.e., e and $\phi(n)$ are coprime. e is used as public key type.
- (5) Calculate d as $d = e^{-1}(\text{mod } \phi(n))$; i.e., d is the modular multiplicative reverse of $e(\text{modulo } \phi(n))$. d is kept as the private key example.

In general public key comprises of the modulus n and public exponent e . The private key comprises of the modulus n and the private key d , which must be kept secret. p , q , and $\phi(n)$ should likewise be kept mystery in light of the fact that they can be used to calculate d . Following we are explaining encryption and decryption of the watermarked image in a flow chart.

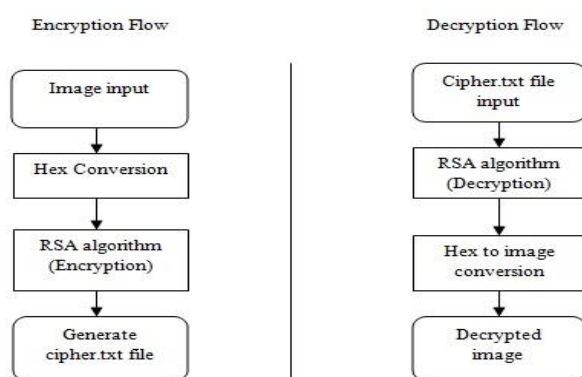


Fig. 5 Encryption and Decryption process of grayscale watermarked image using RSA algorithm



IV. EXPERIMENTAL RESULTS

To confirm the proposed work that is improving security using RSA algorithm with Fractal image watermarking technique and finding PSNR, BER, MSE. We have taken the image of jellyfish 256×256 and encode the gray scale watermark 50×50 with RSA algorithm then the resulting watermark is been embedded inside the jellyfish image and we obtain the watermarked image. To extract image we need public and private key which is generated by RSA algorithm. Only user who have the key can decrypt the image, thus improves security. Figure shows Watermarked image and Extracted watermark which is been through various attacks before it is extracted.



(a)



(b)

Fig. 6 (a) Watermarking image. (b) Extracted watermark.

If an unauthorized user tried to extract the watermark but they require private key. So if we enter the wrong key than decrypted image will be like randomly scrambled image shown in figure



Fig. 7 Randomly scrambled image

We have generated Public key and private key using RSA algorithm during encryption in watermarking



Fig. 8 This figure is made in GUI(Graphical user interface) in Matlab. In this figure we are showing all images like original image, Original watermark image, Grayscale watermark image, Watermarked image and Decrypted image. Also entered public key (N) and private key.

MSE is defined as

$$MSE = \frac{1}{3f_H \times f_W} \sum_{i=1}^{f_H} \sum_{j=1}^{f_W} \|f(i,j) - \tilde{f}(i,j)\|_2^2. \quad (7)$$



Here, f_H and f_W are the height and width of image, respectively. Where $f(i, j)$ and $\tilde{f}(i, j)$ are the values located at (i, j) coordinates of the original image and attacked image. Here we find MSE of the attacked image which also vary with the quality factor 'Q'. Where 'Q' is determined as Quality factor of image and the values are (5, 55, 105, 155, 205, 255).

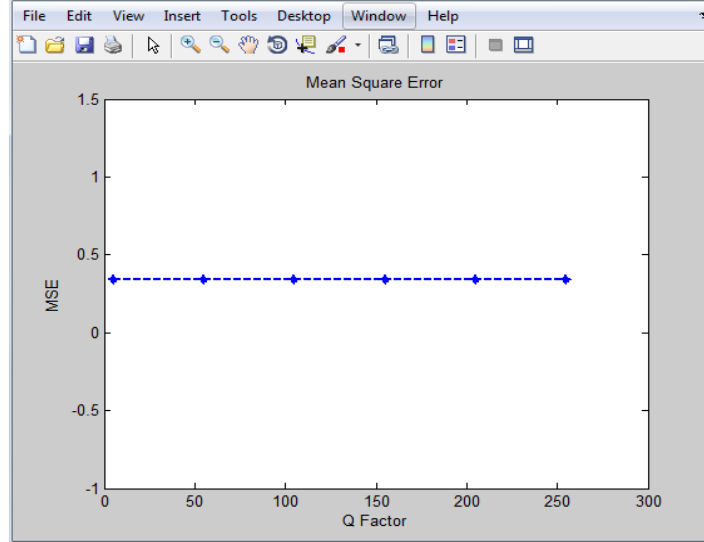


Fig. 9 MSE value varying with the Quality factor of image jellyfish.

The attacked watermarked image quality is measured by Peak signal to noise ratio (PSNR)

$$PSNR = 10 \log_{10} \frac{Q^2}{MSE} \quad (8)$$

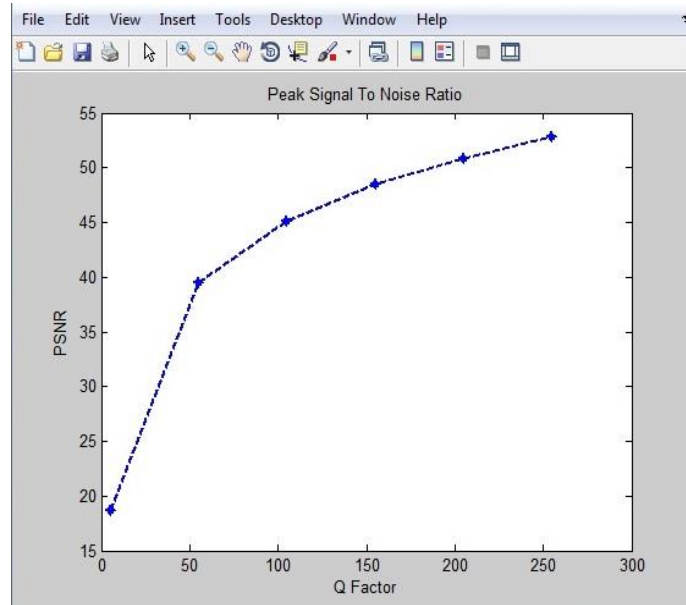


Fig. 10 PSNR value varying with the Quality factor of image jellyfish.

BER is the number of bit errors per unit time and it is also defined as the inverse of PSNR. We also find BER which also vary according to the Quality factor

$$ZBER = \frac{1}{PSNR} \quad (9)$$

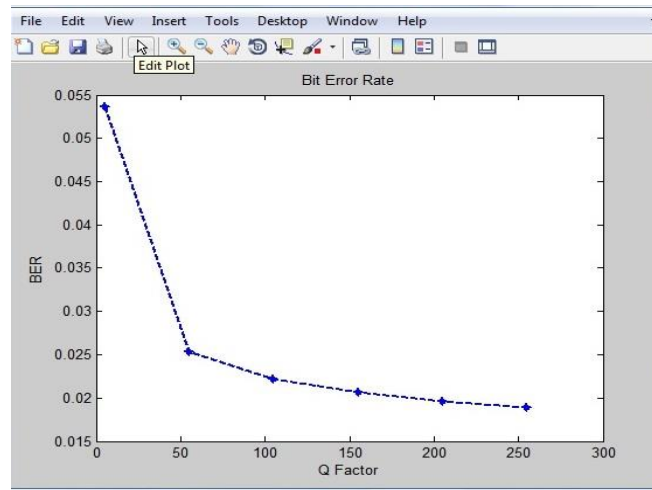


Fig. 11 BER value varying with the Quality factor of image jellyfish.

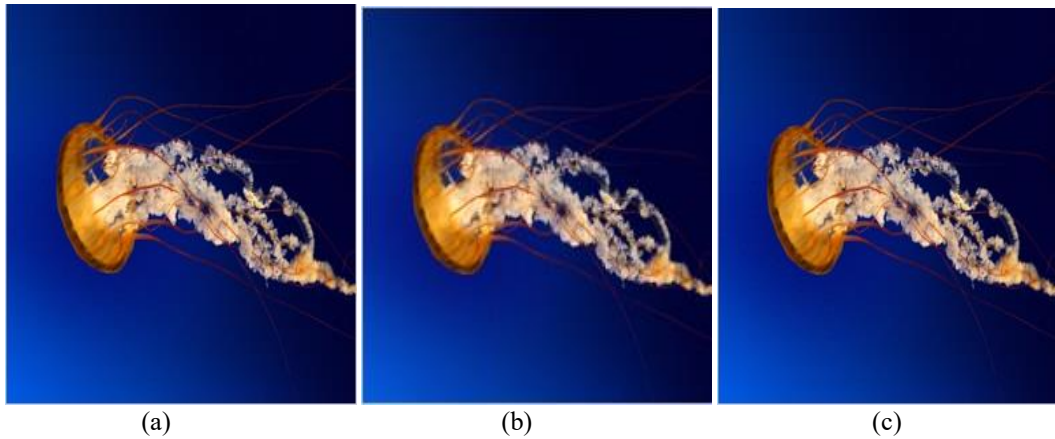


Fig. 12 (a) Original image (b) Watermarked image of classic method (c) Watermarked image of Proposed method.

TABLE I COMPARISON BETWEEN THE PARAMETERS OF WATERMARKED IMAGES OF BOTH CLASSIC AND PROPOSED METHOD.

Image	PSNR	MSE	BER
Watermarked image of classic method	50.2261	0.6173	0.0199
Watermarked image of Proposed method	52.8013	0.3412	0.0189

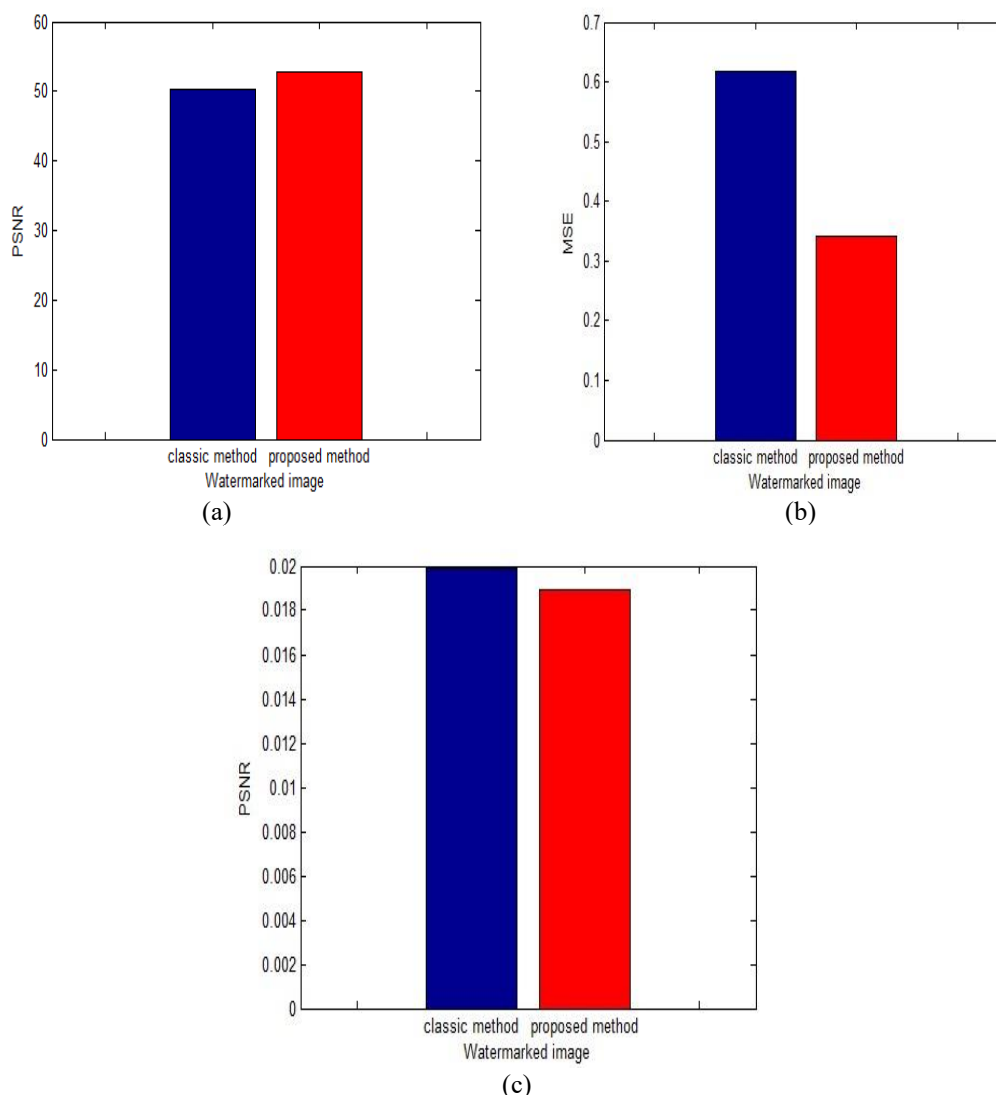


Fig. 13 Comparison between the parameters of watermarked images of both classic and proposed method where (a) shows comparison in PSNR, (b) shows comparison in MSE and (c) shows comparison in BER.

V. CONCLUSION

In our work we tried to develop double security by combining two techniques i.e. Fractal image watermarking with RSA algorithm and then assessed its performance. Our motive is also to achieve good robustness and high image quality. Here we encrypted the watermark with RSA algorithm which generates two keys i.e. public key and private key. These keys again used during decryption of Watermark. Here we take image as 3D vector and hide the watermark in range block mean by converting first RGB vector into La^*b^* space. Then we tried to access its performances and our PSNR, MSE and BER shown better performances because in our technique we are hiding grayscale watermark which gives better performances than hiding a black and white watermark.

VI. FUTURE SCOPE

In future we try to secure it more by using RSA algorithm with more than 2 prime numbers. And by that we try to achieve better robustness of watermarked image and better PSNR, MSE, BER value of image. Also we will try to extract watermark which will be the same copy of original.



REFERENCES

- [1]. Lu, J., Zou, Y., Yang, C., & Wang, L. (2014). A robust fractal color image watermarking algorithm. *Mathematical Problems in Engineering*, 2014.
- [2]. V.M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *Proceedings of the 3rd IEEE International Conference on Industrial Informatics (INDIN '05)*, pp. 709–716, Perth, Australia, August 2005.
- [3]. B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," *Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 27, no. 1-2, pp. 7–33, 2001.
- [4]. R. Ye and S. Wu, "Application of chaotic ergodicity in image encryption and watermarking," in *Proceedings of the 2nd International Conference on Mechanic Automation and Control Engineering (MACE '11)*, pp. 7196–7199, Inner Mongolia, China, July 2011.
- [5]. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.
- [6]. N. Ahmadi and R. Safabakhsh, "A novel DCT-based approach for secure color image watermarking," in *Proceedings of the International Conference on Information Technology: Coding Computing (ITCC '04)*, vol. 2, pp. 709–713, Las Vegas, Nev, USA, April 2004.
- [7]. V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, 2001.
- [8]. W.-H. Lin, Y.-R. Wang, S.-J. Horng, T.-W. Kao, and Y. Pan, "A blind watermarking method using maximum wavelet coefficient quantization," *Expert Systems with Applications*, vol. 36, no. 9, pp. 11509–11516, 2009.
- [9]. H. A. Al-Otun and A. O. Al-Taba'a, "Adaptive color image watermarking based on a modified improved pixel-wise masking technique," *Computers and Electrical Engineering*, vol. 35, no. 5, pp. 673–695, 2009.
- [10]. B. A. Wandell, *Foundations of Vision*, Sinauer Associates, Sunderland, Mass, USA, 1995.
- [11]. C. P. Li, Y. J. Wu, and R. S. Ye, Eds., *Recent Advances in Applied Nonlinear Dynamics with Numerical Analysis*, World Scientific Publishing, Singapore, 2013.
- [12]. M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326–332, 1998.
- [13]. M. Barni, F. Bartolini, and A. Piva, "Multichannel watermarking of color images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, no. 3, pp. 142–156, 2002.
- [14]. P. Tsai, Y.-C. Hu, and C.-C. Chang, "A color image watermarking scheme based on color quantization," *Signal Processing*, vol. 84, no. 1, pp. 95–106, 2004.
- [15]. T. K. Tsui, X.-P. Zhang, and D. Androutsos, "Color image watermarking using the spatio-chromatic fourier transform," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '06)*, pp. 305–308, Toulouse, France, May 2006.
- [16]. C.-T. Kuo and S.-C. Cheng, "Fusion of color edge detection and color quantization for color image watermarking using principal axes analysis," *Pattern Recognition*, vol. 40, no. 12, pp. 3691–3704, 2007.
- [17]. C.-H. Chou and K.-C. Liu, "A perceptually tuned watermarking scheme for color images," *IEEE Transactions on Image Processing*, vol. 19, no. 11, pp. 2966–2982, 2010.
- [18]. E. Vahedi, R. A. Zoroofi, and M. Shiva, "Toward a new wavelet based watermarking approach for color images using bioinspired optimization principles," *Digital Signal Processing*, vol. 22, no. 1, pp. 153–162, 2012.
- [19]. M. F. Barnsley and S. Demko, "Iterated function systems and the global construction of fractals," *Proceedings of the Royal Society A*, vol. 399, no. 1817, pp. 243–275, 1985.
- [20]. A. E. Jacquin, "Image coding based on a fractal theory of iterated contractive image transformations," *IEEE Transactions on Image Processing*, vol. 1, no. 1, pp. 18–30, 1992.
- [21]. P. Davern and M. Scott, "Fractal based image steganography," in *Information Hiding*, vol. 1174 of *Lecture Notes in Computer Science*, pp. 279–294, Springer, Berlin, Germany, 1996.
- [22]. M.H. Pi, C. H. Li, and H. Li, "A novel fractal image watermarking," *IEEE Transactions on Multimedia*, vol. 8, no. 3, pp. 488–498, 2006.