An Image Steganography Algorithm using Fractional Discrete Wavelet Transform with Advanced Encryption System

Satyaki Sarkar, Dipanshu Dey, Shweta Singh, M Jasmine Pemeena Priyadarsini, Jabeena A

Abstract*: The research constitutes a distinctive technique of steganography of image. The procedure used for the study is Fractional Random Wavelet Transform (FRWT). The contrast between wavelet transform and the aforementioned FRWT is that it comprises of all the benefits and features of the wavelet transform but with additional highlights like randomness and partial fractional value put up into it. As a consequence of the fractional value and the randomness, the algorithm will give power and a rise in the surveillance layers for steganography. The stegano image will be acquired after administrating the algorithm which contains not only the coated image but also the concealed image. Despite the overlapping of two images, any diminution in the grade of the image is not perceived. Through this steganographic process, we endeavor for expansion in surveillance and magnitude as well. After running the algorithm, various variables like Mean Square Error (MSE) and Peak Signal to Noise ratio (PSNR) are deliberated. Through the intended algorithm, a rise in the power and imperceptibility is perceived and it can also support diverse modification such as scaling, translation and rotation with algorithms which previously prevailed. The irrefutable outcome demonstrated that the algorithm which is being suggested is indeed efficacious.

Keywords*: Fractional random wavelet transform, Wavelet transform, image steganography, surveillance.

I. INTRODUCTION

The steganography of image is fundamentally nothing unusual from image encryption. A confidential image is concealed in such a manner that nobody except the person who is transmitter and the person who is the recipient of the image will identify that there is concealed data [15]. The operation of concealing the confidential image into a contrasting image known as the coated image is known as steganography. The image secured as an outcome of concealing the two images is called stegano image. Since the procedure of transmitting digital information is expanding, we obligate a rise in surveillance, especially on technology networks which are susceptible to hacking. Since the number of information being transmitted on the web is expanding, surveillance of networks has become a very key matter [12]. Therefore, to avert unsanctioned ingress and avail of confidential files, data integrity is of utmost significance [5]. As a result, there has been an expansion in the zone of concealing data and surveillance. Various procedure of steganography has expanded with respect to spatial transformation and they are useful in areas of complication and operation [19]. The indicated procedure keeps the confidential concealed. In order to preserve the information, randomness is very important because an unauthorized person will not be able to understand the information. Only the authorized recipient will be able to understand it [9].

Here, we work on a modern procedure of steganography which is related to Fractional Random Wavelet Transform (FRWT). It belongs to an extended relation of the wavelet transform [7]. It inherits the brilliant arithmetic features of both Wavelet Transform (WT) and the Fractional Random Transform (FRT) [1].

The information is described in not only frequency but also spatial domain with some added randomness, which is a result of the time frequency plane being rotated [3]. We use the qualities of FRWT for hiding the image here in steganography [20]. The procedure of transmitting the concealed image to the desired recipient without getting perceived in an unguarded channel is a very challenging task. Some available images are used as concealed image to transmit data and after applying them to digital image steganography, its robustness was justified [6].

Image steganography using transform domain method embeds the secret image into the coated image. To strengthen them and make them more robust for attacks, they are concealed within the frequency regions of the coated image [18]. This also assembles much further suitable for exchange of confidential information. There are four sub-levels: LL (low-low), LH (low-high), HL (high-low) and HH (high-high). Here, the confidential image is concealed in the LL sub-band parameters of FRWT of the coated image. Succeeding this inverse transform (IFRWT) is applied and the stegano image is obtained by the recipient.

Revised Manuscript Received on July 22, 2020.
*Correspondence Author
Satyaki Sarkar*, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. Email: satyaki2020@gmail.com
Dipanshu Dey, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.Email: dipanshudey1407@gmail.com
Shweta Singh, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, IndiaEmail: shwetasingh2498@gmail.com
M. Jasmine Pemeena Priyadarsini, Higher Academic Grade, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, IndiaEmail: jasmin@vit.ac.in
JABEENA A, Associate Professor Grade 1, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
Email: ajabeena@vit.ac.in

Then we move ahead with the extraction procedure to separate the concealed image from the stegano image. Various features of FRWT are explored like the fractional sequence of transform, the embedding coefficient, the arbitrary matrix generated which consists of unconstraint variable.

As a stranger, which is extremely cumbersome to realize that there is a concealed image within the coated image [16]. Due to the arbitrary matrix, it is very difficult to frame it. Predicting the fractional order is also very difficult, therefore this method provides very high network security [11].

II. OVERVIEW

A. Input Random Fractional Wavelet Transform for A 2-D Wave

A colored coated image of measurement 512x512 is taken and a random matrix of the same size is taken. Through Fig 1 we can visually assess and compare Wavelet Transform (WT) with Fractional Random Wavelet Transform (FRWT) for the original image which has a size of 512x512. An image after undergoing Discrete Wavelet Transform (DWT) possesses multiresolution property whereas FRWT has a property where it illustrates the details in domains with respect to frequency and spatial but with arbitrary coefficient [7]. Since FRWT has a unique feature in which the time-fractional-frequency plane can be rotated about an arbitrary angle, it gives uniform randomness and also maintains the components of an image which have low frequency. This property was used in encryption and decryption of image [14]. Here we bring forward different implementation of FRWT which is steganography of image.

(a)Real Image (b)Level-1 WT (c)Level-1 FRWT

Fig 1: Visual assessment of WT and FRWT

III. METHODOLOGY

A colour image is basically represented by three planes: Red, Green and Blue planes. In the proposed algorithm of image steganography, we embed the image such that it is concealed in the level-1 of LL (low-low) frequency sub-band in the FRWT of the coated image's green plane. The green plane provides good results and it is also in line with the requirements of the International Telecommunication Union (ITU), 1992 [12]. After applying inverse FRWT(IFRWT), the stegano image is obtained which carries the hidden image. The stegano image does not provide any signs or information that there is a confidential image within it. The coated image and concealed image are acquired separately after the segregation procedure is implemented. Image steganography will be successful only if we find a suitable method to embed the secret image and create the stegano image. We need to know which algorithm provides highest security hence it is important to rank them so that we can know how successful the embedding process will be. The most important aim of steganography is to develop a function of embedding parameter which is not detectable mathematically and which is able to communicate large payloads.

A. Input

A colored coated image of measurement 512x512 is taken and a random matrix of the same size is taken. The secret image is a gray scale image of size 256x256. A value of fractional order with coefficient of embedding is also taken.

B. Output Before Segregation

The image for steganography, which is a colored image of measurement 512x512 is obtained.

C. Output After Segregation

The coated image of measurement 512x512 and the segregated concealed image of size 256x256 is obtained.

D. Embedding Process

- The color image is divided into three color planes, i.e Red, Blue and Green.
- The FRWT is computed by functioning on the coated image of Green plane.
- The result of FRWT is decomposed to four wavelet sub-levels, i.e LL, LH, HL and HH.
- Encryption performed by shuffling the coefficients of LL, LH, HL and HH multiple times by using Arnold Cat Map (ACM) method.
- The confidential image along with LL sub-level in FRWT are divided into blocks of equal size which are non-overlapping.
- The confidential image is embedded into sub-level of LL by using (1):

$$(1-\rho) * \beta 1 + \rho * \beta 2 \qquad -(1)$$

- $\beta 1$ represents the LL sub-level blocks of FRWT of the coated image, $\beta 2$ represents the confidential image block and ρ represents the coefficient embedding parameter. This is how the confidential image is concealed in the coated image.

E. Extraction Process

- FRWT is computed for the stegano image. Extraction is performed by the receiver by using (2):

$$(\gamma\gamma 1 - ((1-\rho) * \gamma\gamma 2)) . / \rho \qquad -(2)$$

- $\gamma\gamma 1$, $\gamma\gamma 2$ and ρ represent the LL sub-level blocks of image steganography, confidential image and coefficient embedding parameter.
- The confidential image is retrieved from the stegano image.
- Finally, MSE and PSNR values are computed for the stegano and confidential image.

IV. ABBREVIATION AND FLOWCHART

A. Abbreviations and Acronyms

I.**MSR:** Mean Square Error. It calculates the mean of the squared error between desired value and calculated value

II. **PSNR:** Peak Signal-to-noise ratio. It is ratio of signal power to that of noise

B. Equations

FRWT is two dimensional. It has a feature of separability as a result of which FRWT is acquired by taking the single-dimension of transformation along vertical and horizontal axis [17].

$$W_{a_x,a_y}(u,v,a1,b1,a2,b2) = FRWT_{a_y}^{t_y \to v} x \left\{ FRWT_{a_x}^{t_x \to u} \{ f(t_x,t_y) \} \right\}$$

- -(3)

Where a1, a2 are scaling and translation parameters along x direction and b1, b2 are scaling and translational constants on y direction.

The 2-D DWT of DFRT in the form of X (n1, n2):

$$W_\Phi(j_0,k_1,k_2) = \frac{1}{\sqrt{MN}} \sum_{n1=0}^{M-1} \sum_{n2=0}^{N-1} X(n1,n2) \Phi_{j_0,k_1,k_2}(n1,n2)$$

-(4)

$$W_\Psi^i(j,k_1,k_2) = \frac{1}{\sqrt{MN}} \sum_{n1=0}^{M-1} \sum_{n2=0}^{N-1} X(n1,n2) \Psi_{j,k_1,k_2}^i(n1,n2)$$

- (5)

Here, i= {H, V, D}, j_0 represents some arbitrary scale. k_1 and k_2 are translation parameters [10].

Equation (4) gives us an approximate value of coefficients at scale j_0 and (5) gives us detailed coefficients at a scale $j > j_0$ of X (n1, n2). Therefore, the 2D-FRWT which is obtained is incorporated with all the properties of both DWT and FRT.

The Inverse transformation of wavelet is acquired by the following expression:

$$X(n1,n2) = \frac{1}{\sqrt{MN}} \sum_{k_1} \sum_{k_2} W_\Phi(j_0,k_1,k_2) \Phi_{j_0,k_1,k_2}(n1,n2) + \frac{1}{\sqrt{MN}} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_{k_1} \sum_{k_2} W_\Psi^i(j,k_1,k_2) \Psi_{j,k_1,k_2}^i(n1,n2)$$

- (6)

After the application of IFRT to X (n1, n2), the images are extracted.

C. **Flowchart**

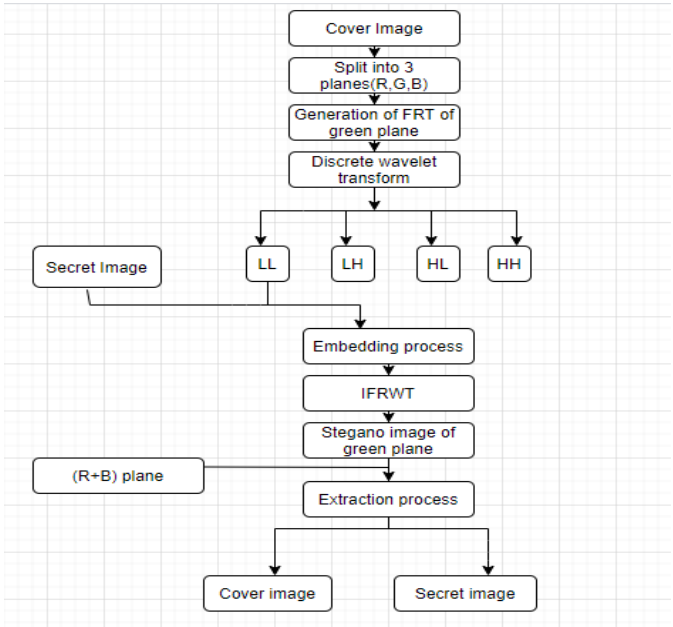


Fig 2: Flowchart of Suggested Algorithm

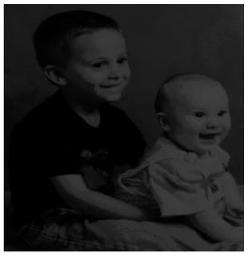
V. RESULT AND DISCUSSION

We need to assess the result of the suggested methodology. For that, a football image of measurement 512x512 is taken as a coated image with kid's greyscale image of measurement 256x256 is taken as confidential image. They are shown in Fig. 3(a) and (b).

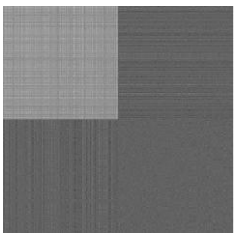
Level-1 of FRWT is processed for the coated image's green plane and displayed in Fig. 3(c). Since almost all the energy is focused in the LL level, it is selected for embedding. The LL level of FRWT is displayed in Fig. 3(d). LL level formed after decomposition of DWT and the confidential image are split into blocks which are non-overlapping. The confidential image which has been divided is concealed into the LL level of FRWT's coated image using (1) and later using IFRWT. The stegano image which is acquired contains the confidential as well as the coated image. It is shown in Fig. 4(a). The confidential image cannot be identified by unauthorized personnel. The surveillance of the stegano image is of very huge strength and the changes in the images are not noticed.

In order to acquire the confidential image from the stegano image, segregation method is utilized and the image is reconstructed. The extracted image is displayed in Fig. 4b. The images of steganography are obtained not only with fractional coefficient but also with integer coefficient, so that the importance of fractional order could be determined. Upon usage of integer order, the stegano image has a blurred look and it might lead to notion that there is some concealed data in it. But when using fractional parameter, the stegano image is exactly alike to the coated image. The performance values have been calculated later which also proves the superiority of the fractional order, which is displayed in Fig. 5.

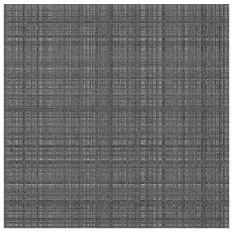
(a)Coated image of 512 x 512-dimension



(b)Confidential image of 256 x 256-dimension

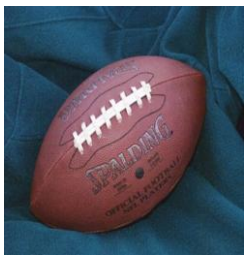


(c)Level-1 FRWT of Coated image



(d) LL level of FRWT Confidential image

Fig 3: Mathematical simulation of 2D-FRWT with coated and confidential image



(a)Stegano Image

(b)Segregated confidential Image

Fig 4: Mathematical values of FRWT after extraction process

(a)Stegano image with Integer parameter

(b)Stegano image with Fractional parameter

Fig 5: Mathematical values of stegano image

A. *Performance Measures*

The result of the suggested procedure is computed using frequently used metrics like PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error).

B. *Performance between Integer and Fractional Order*

The performance measures of both integer and fractional order are evaluated and they have been displayed in Table-I. It can be concluded that fractional method of steganography performance is better than the integer method of steganography.

Table-I: Numerical values of Stegano and Segregated Confidential Image

	Stegano Image		Segregated Confidential Image	
Order Type	**PSNR**	**MSE**	**PSNR**	**MSE**
Fractional	37.90	2.79	277.02	1.07e-023
Integer	14.12	3.62e+003	23.87	8.59e+006

C. *Comparison of various frequency level*

In the algorithm used here, the confidential image has been concealed in the LL sub-level of FRWT and it has been proved that the other sub-bands do not give good results as they the magnitude of their coefficients is less. The performance measures of the stegano image for various sub-bands has been tabulated and shown in Table-II.

Table-II: Numerical values for stegano image in different frequency bands

Frequency Band	PSNR	MSE
LL	37.90	2.79
LH	9.49	1.16e+004
HL	8.53	1.05e+004
HH	6.87	1.34e+004

D. *Comparison with DWT*

Image steganography using FRWT is a very promising field. Searching a random matrix which is encrypted and is equally scattered with arbitrary value is not possible. Similarly, it is very difficult to identify the presence of a confidential image in the stegano image without calculating the value of the coefficient of embedding factor and the fractional parameter. The problem of DWT with respect to various factors like PSNR, MSE and efficiency of FRWT for different regions of decomposition are given in Table-III.

To analyze efficiency of this suggested methodology, it is assessed on images of various types and it is discovered to be non-sensitive on many image types. We executed the procedure with MATLAB software (2019b) and analyzed it by finding various performance measures such as PSNR and MSE. We used numerous images of various types and they have been shown in Table-IV. If an embedded image is detected, it defeats the main goal of steganography of hiding information. The subjective tests are carried out and the success percentage is 81% and can be deduced that the data is not visible. These standards and suggestions are explained by the ITU.

Table-III: MSE and PSNR for FRWT and DWT

Level of Decomposition	PSNR	MSE	Surveillance
Level-1 DWT	33.87	4.19	Medium
Level-1 DWT	32.69	7.43	
Level-1 DWT	32.14	5.84	
Level-1 FRWT	37.90	2.71	Extreme

Level-2 FRWT	36.53	3.18	
Level-3 FRWT	35.22	3.67	

Table-IV: Contrast in PSNR and MSE for Various Test Images

Coated Image	Confidential Image	PSNR	MSE
Football.jpg	Kids.tif	37.90	2.79
Saturn.png	Shadow.tif	39.43	7.99
Rose.jpg	Mandi.tif	35.28	5.59
Lena.png	X-ray.jpg	34.42	4.16
Peppers.jpg	Fingerprint.bmp	38.68	6.27

VI. CONCLUSION

Due to increase in digital technologies and the emergence of various networks, communication has increased and files are transferred in electronic format. Hence, it is necessary to hide information. None of the spectator should guess the order of the fractional value or the various values in the uniformly distributed random matrix. Therefore, it is very difficult to recognize the presence of a confidential image in the coated image. FRWT is performed by combining the coefficient of embedding parameter, fractional value and formation of arbitrary matrix. Randomness is a key component here and as a result of that FRWT provides better results. We have also compared our proposed algorithm with already existing methods. Various performance measures like PSNR and MSE are used to compare the various algorithms and FRWT provided better results. Hence, we conclude that Random Fractional Wavelet Transform gives a favorable, resilient and durable steganography. This implementation has prospective fortune in medical zones and we can conceal various data such as CT scan images, MRI, etc.

ACKNOWLEDGMENT

We are grateful to School of Electronics Engineering VIT University Vellore and our guides Dr. M. JASMINE PEMEENA PRIYADARSINI, Higher Academic Grade, and Dr. A. JABEENA, Associate Professor, VIT University, Vellore, Tamil Nadu for guiding and assisting us in completing the project.

REFERENCES

1. Ghosh, P. and S.N. Mondal, 2012. A steganographic method for color image authentication (SMCIA). Proceeding of 2012 International Conference on Recent Trends in Medical Technology, pp: 816-821.
2. Chedhud, M., J. Coswell, K. Kurien and N.P. Kevin, 2011. Digital image steganography, Signal Process., 90(3): 627-652.
3. Vamsin, V., 1983. The fractional order laplace transform and implementation of quantum mechanics. J. Inst. Physics Appl., 25(3): 221-245
4. Hemalat P, K. Dinesh Achary,Devi A,Priyamani R Kamath,2012. A Secure Image Steganography Procedure Using Integer Wavelet Transform: 248-255.
5. Neda Raftar, Ameer Masod Eftekar Mogadham,2014. Digital Image Steganography with Fourier Transform and Assignment Algorithm:458-468.
6. Mizu, M., H. Ciao and S. Miu, 2009. A discrete integer random transform. Optical Communication, February, 2009.
7. SS Zang, W. and X. Lee, 2013. Data content weighting for perceptual image quality evaluation. IEEE T. Image Process., 20(5): 1156-1179.
8. El Shazl Yemad, Abdel Wahab Safey,2018. Image steganography using least significant bit and integer wavelet transform:265-273.
9. Anitha Gnana selvi. J, Maria kalavathy. G,2019. Probing Video and Image Steganography based On Discrete Wavelet and Discrete Fourier Transform:589-595.
10. P. Narsingham, Pastor Xavier.R, Optimized Fractional Wavelet Transform based Steganography,2012
11. M.A. Lakshmi, Usha B A, Sangeeta K N,2018. Security Enhancement in Image Steganography Using Neural Networks and Deep Learning:105-109
12. International Telecommunication Union (ITU), 1994. Technology-Digital Compression and Encoding of Discrete-Tone Still Images- T.81. ITU Sept., 1994.
13. Agarwal, G., LPK. Zu and W. Raman, 2013. A new discrete wavelet transforms for fingerprint security. IEEE T. Syst. Cybersecurity, Humans, 42(1): 262-275.
14. Mina Sharma, S.N., S.N..Barik and S. Mohanty, 2013. Hybrid Domain in LSB Steganography. Int. J. Computer. Application., 15(2), (2475-8752).
15. Md Syed Kabeer, Prashan Premaratne, Peter James Vial,2017. Secure Image Steganography Using Dual-Tree Block Matching Complex Wavelet Transform, 398-415.
16. S.Thenmozhi , Dr.M.Chandrasekaran,2012. Novel Approach for Image Stenography Based on Integer Wavelet Transform:456-469.
17. Sallat, C.G., 1991. A process for multiresolution signal decomposition: IEEE T. Sequence Anal. Mach. Intell., 31(5): 276-912.
18. Mohamed Elhoseny, Gustavo Ramirez-Gonzalez, Osama M. Abu-ElNasr, Shihab A. Shawkat, Secure Medical Data Transmission Model for IoT-Based Healthcare Systems:89-115.
19. Leontiev V.V., Saragishvilli S. E, 2017.Steganography Based on the Hadamard Transform and Modification of the DEMD:487-505.
20. Velamurthy, B.J. and K. Sreyoshi, 2008. Steganim-a novel data hiding process using animations. Eng. Seth., 79: 9.

AUTHORS PROFILE

Satyaki Sarkar has pursued his education from. SBOA School & Junior College, Chennai which is affiliated to CBSE. Before that he studied in Etasi Timpany School, Vishakhapatnam and Bharatiya Vidya Bhavan, Kolkata. He is currently pursuing under-graduation in B.Tech from Vellore Institute Of Technology, Vellore, Tamil Nadu. He is doing major in Electronics and Communications Engineering. He started pursuing this degree from 2016 and will be completing it in 2020. He has done a few internships and trainings in his respective field. He did internship in the field of Computer Networks from BSNL. He has done various projects using Microcontrollers, Arduino, Java, MySQL, Tableau and used multiple softwares such as, Cadence and Netsim.

Dipanshu Dey has pursued his education from Loyola School, Jamshedpur from 2005-2015. It is affiliated to ICSE curriculum. He was distinguished for securing cent per cent marks in the ISC (12th board) examinations in Mathematics. He is currently pursuing under-graduation in B. Tech from Vellore Institute of Technology, Vellore, Tamil Nadu. He is majoring in Electronics and Communication Engineering. He started pursuing this degree in 2016 and will be completing it in 2020. He has done internships in reputed companies like Tata Power. He has also interned in Ericsson which specializes in the field of communication. He has done various projects using microcontrollers, Java, Arduino, and used multiple softwares such as MATLAB, Keil, Tableau and Netsim.

Shweta Singh has pursued her secondary education in 2014 from Saint pauls Sr. Sec. School, Kota, Rajasthan. She pursued her higher secondary education from Mittal international school, kota, Rajasthan was affiliated with CBSE curriculum. She is currently pursuing under-graduation in B-Tech from Vellore Institute of Technology, Vellore, Tamil Nadu. She is doing majors in electronics and communication engineering. She started pursuing this degree from 2016 and will be completing it in 2020. She has done her internship from western railways in her respective field. She has done projects on Travel salesman problems using Genetic Algorithm, Brute force, Greedy Algorithm (DSA), Automatic railway gate control system using 8051 microcontrollers with the help of keil IDE.

Dr. M. Jasmine Pemeena Priyadarsini obtained B.E. degree from Madras University in 1992 and M.E. degrees from Madurai Kamaraj University, Madurai in 1995. She earned his Ph.D. from Vellore Institute of Technology, Vellore, INDIA in 2014. She has published more than 45 research papers in National and International journals and reputed conferences. She has a teaching experience of about 25 years in Vellore Institute of Technology, Vellore in India. Presently, she is serving as Professor at Vellore Institute of Technology, India. She is a life member of Indian Society for Technical Education, IEEE society Membership, Fellow of Institution of Engineers, Fellow of Institution Electronics and Telecommunication Engineers. She has authored about four technical books. His research areas include Digital Image Processing, Digital signal processing, Optical Signal Processing, Light wave Communication Systems, Optical Coding Theory and Biometric Image Processing. She is a reviewer of several international conferences and journals.

Dr. A. Jabeena is an Associate Professor in School of Electronics Engineering, VIT University, Vellore. She has completed her B.E [Electronics and Communication Engineering in Bhrathiar University, Coimbatore, M.E., in Applied Electronics and received her PhD in Optical communication, Vellore Institute of Technology, Vellore. She has more than 25 years of teaching experience and her Research Interest includes application of Evolutionary algorithms to optimization problems in Wireless Optical Communication, Satellite communication, Optical Sensors and visible light communication. She is a member of Indian Society for Technical Education, IEEE, Institution of Engineers and Indian Science Congress Association. She has published more than 60 of her contributions in Scopus indexed journals and IEEE conferences. She is also reviewer of several international conferences and International journals