Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130209

Dual Tree Complex Wavelet Transform-based Image Security Using Steganography

T. Yuvaraja[1,*] *and R. S. Sabeenian*[2]

[1] Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy, India
[2] Department of Electronics and Communication Engineering, Sona College of Technology, Salem, India

Received: 30 Oct. 2018, Revised: 23 Dec. 2018, Accepted: 28 Dec. 2018
Published online: 1 Mar. 2019

Abstract: Modern communication media requires high level of protection system for securing the multimedia data from hackers. The most important objective of this manuscript is to develop a simple and efficient methodology for protecting the information from hackers. In this paper, the level of image security is improved by integrating the steganography and cryptography techniques in order to produce the secured image. In this manuscript, secured image is produced by applying Dual Tree Complex Wavelet Transform (DT-CWT). Further, cryptography algorithm is applied on the steganography image if the level of information entropy lies beyond the threshold value. Mean Square Error (MSE),Peak Signal to Noise Ratio (PSNR) and Mean Absolute Error (MAE) are the metrics which are used to evaluate the performance of the proposed method in this manuscript. The proposed image security methodology achieves 47.04 dB of PSNR, 165.86 of MSE and 31.66% of MAE on bone image dataset.

Keywords: Security, steganography, cryptography,DT-CWT

1 Introduction

The modern world transfers lot of multimedia information through internet which contains videos, audios and data files. This information can be accessed only by the destination end users. But, the hackers between sender and receiver hack on these information and they can be used by unauthorized works [1]. Hence, this information should be protected in order to overcome such limitations on data protection. This requires high level of multimedia data security on data transmission from one source user to destination user. The information hacking may be categorized into internal hacking and external hacking. In internal hacking, the data is hacked when they are in static mode of operation [5]. In external hacking, the data is hacked during the transmission of information from one user end to another user end.

These two types of hacking should be avoided in order to prevent data from unauthorized users [6]. In this paper, the images are protected from unauthorized persons using a technique called Steganography. This insets the secret information into main or source image for protecting or hiding the information from hacker's direct sight. This manuscript suggests an methodology for hiding the information within source image. In order to evaluate the performance of the proposed security methodology, the standard benchmark secret images are used. Fig. 1 shows the general process flow of the steganography methodology.

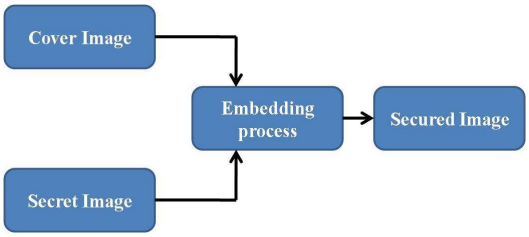


Fig. 1: Generic flow of steganography for image security

This work is ordered as follows. Section 2 deals with the conventional methodologies for image security using various steganography and cryptography techniques. Section 3 proposes a novel methodology for image security using the integration of image steganography and cryptography. Section 4 discusses the simulation results and Section 5 concludes the manuscript by depicting the main findings.

* Corresponding author e-mail: kstyuvaraja@mail.com

2 Literature Survey

Emad et al. (2018) used least significant approach for securing the data within the source image which was based on the wavelet transform techniques. The authors tested their proposed approach on real time benchmark images to validate their methods. Ma et al. (2018) developed an error-resilient approach for protecting the data from un-authorized users in static and random environments. Soria-Lorente et al. (2017) applied frequency domain-based bit mapping technique on source cover and secret images to hide the secret image information into cover image. The authors obtained low PSNR value due to the errors in the secured image. Suchitra Sinha et al. (2016) proposed a method to increase the level of image security using de-synchronization method. The authors applied their proposed methodology on different text, audio and video images by implementing the transformation techniques on rows and columns. The main limitation of this work is that it was not able to detect dynamic attacks from the outside environment. Shikha Mohan et al. (2015) developed less complex image security algorithm using matrix transformation techniques. The authors classified the various objects in image and then the steganography was applied over the secret image for protecting the image from hackers. The authors checked their proposed method with various types of attacks from indoor and outdoor environments.

Li and Wang (2007) used particle swarm optimization algorithm for improving the security of the system by hiding the secret image within source image. Here, the transformed messages were embedded in the 36 coefficients during the decomposition of cover image into multi-level coefficient metrics.. Chang et al. (2002) proposed a new steganography scheme-based on JPEG and modification of quantization table. In this case, the secret message is first encrypted and then embedded in the 26 coefficients located in the cover image.

The following points are observed from the conventional methods of image security.

- The image security was improved using either steganography or cryptography technique only.
- No hybrid technique was implemented to improve the image security.

Hence, this paper proposes the methodology which integrates the steganography technique with cryptography method-based on information entropy.

3 Proposed Method

In this paper, DT-CWT transform-based image security is proposed. The proposed image security methodology has two modules as module 1 is image steganography module 2 is image cryptography.

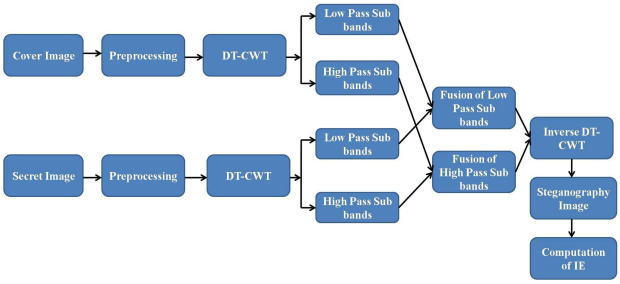


Fig. 2: Proposed image security methodology using steganography

In case of module 1, the secret image is embedded into cover image using DT-CWT transform by fusing its coefficients. Then, module 2 is applied on steganography image-based on the computation of Information Entropy (IE).

3.1 Preprocessing

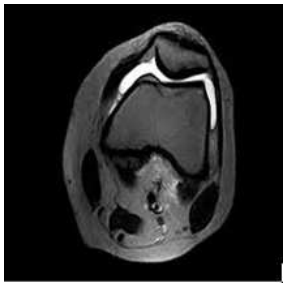
In this paper, the cover image could be either gray-scale or RGB format [10]. This RGB cover image is transformed into gray-scale image format if the source cover image is in RGB format. The secret image is allowed to be only in gray-scale image format. Because, the secret image used in this paper are medical images.

In this paper, brain and bone Magnetic Resonance Image (MRI) are used as secret images which can be obtained from open-access dataset [11]. Both gray scale cover and secret images are now resized into 256×256 sizes as width and height of the images. Now, normalization (threshold is found using histogram method [3] and the images are converted into binary-based on threshold value) is applied on both secret and cover images in order to produce binary images. Fig. 3(a) and Fig. 3(b) illustrate the source cover and gray-scale secret image respectively. Fig. 3(c) and Fig. 3(d) illustrates the preprocessed normalized cover and secret image, respectively.

3.2 DT-CWT

The normalized cover and secret images [9] are spatial images which cannot be decomposed into different levels. These spatial domain images are converted into frequency domain images [12]. In this paper, DT-CWT is used which transforms the spatial normalized cover and secret images into frequency domain images in order to obtain multi-level decomposition coefficients. This DT-CWT transform [13] has two inbuilt filter banks as LPF banks and HPF banks. In this paper, two levels of decompositions are applied on both normalized cover image and secret image respectively. The wavelet and scale design factors are the two important design factors

(a) Source cover image (lena)



(b) Secret image (bone)

(c) Normalized cover image

(d) Normalized secret image

Fig. 3: Cover(lena) and Secret (bone) images

of DT-CWT to decompose the image into number of subbands.

The wavelet design factor of the DT-CWT is described in the expression as stated below.

$$\psi_c(t) = \psi_r(t) + j\psi_i(t)$$

The scale design factor of the DT-CWT is described in the expression as stated below.

$$\phi_c(t) = \phi_r(t) + j\phi_i(t)$$

where, the real part of the wavelet design factor is represented by $\psi_r(t)$ and the imaginary part of the wavelet design factor is represented by $\psi_i(t)$ respectively.

These real and imaginary parts are depicted in the following equations as,

$$\psi_r(t) = \sqrt{2}\sum_n H_a(n)\cdot\phi_r(t)(2t-n)$$
$$\psi_i(t) = \sqrt{2}\sum_n H_b(n)\cdot\phi_i(t)(2t-n)$$

Fig. 4 shows the decomposition architecture of DT-CWT which consists of low- and high-pass filter banks and its corresponding decimators. In this paper, the decimating factor is set to two for obtaining the loss less sub-band coefficients in DT-CWT. In this paper, six low-pass and six high-pass sub bands are obtained by applying an image into DT-CWT.

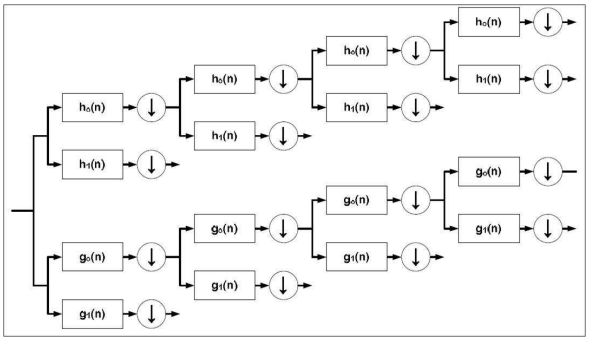


Fig. 4: Decomposition of image into subbands in DT-CWT

(a) Fused image

(b) Secured image

Fig. 5: Fused and Secured(cameraman) image

3.3 Subband fusion

The subband coefficients from low-pass and high-pass filters are represented in matrix format. The following steps are followed for producing fused image.

Step 1: Eigen values are computed for each low-subband coefficient matrix individually as el1, el2 and el3.
Step 2: Determine the maximum Eigen value from the computed Eigen values and noted as $E1_{\max}$.
Step 3: Eigen values are computed for each high-subband coefficient matrix individually as eh1, eh2 and eh3.
Step 4: Determine the maximum Eigen value from the computed Eigen values and noted as $E2_{\max}$.
Step 5: The following fusion rule is adopted for fusing the subband coefficients.

$$E = E1_{\max} + k \times E2_{\max}$$

where E represents the fused coefficient matrix.

Then, inverse DT-CWT transform is applied on the fused coefficient matrix image Fig. 5(a) in order to produce the image as depicted in Fig. 5(b).

3.4 Determination of IE

The strength of the proposed security methodology stated in this paper is analyzed using IE. IE is computed due to determine the level of security in steganography-applied source image. The value of IE is equal to eight for strong image security methodology. The attackers or hackers fail

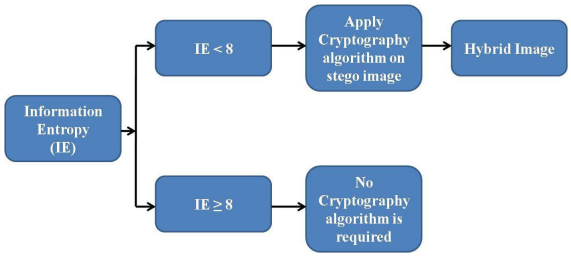


Fig. 6: Proposed image security methodology using cryptography

to attack the stegonography image. Hence, the evaluation factor IE is used for evaluating the strength of the image and it is given in the following equation as,

$$IE = \sum_{i=1}^{N} p(m_i) \times \log_2[1/p(m_i)]$$

The pixel in the secured image may present many number of times in the image and its probability value is noted by $p(m_i)$ and the number of repeated pixels is noted by N.

In many practical applications such as patient-scanned images security, the value of IE may vary 7 to 8 due to various modalities of the medical scanned images. If the IE value of the fused image which is obtained from the proposed methodology stated in this paper is equal to or greater than 8, then there is no further requirement for improving image security. If IE value of the fused image obtained in this paper is less than 8, then there is a requirement for strengthening the image security. In this paper, cryptography algorithm is applied on the fused image if the value of IE less than 8.

Fig. 6 shows the proposed image security methodology using cryptography algorithm which is explained in the following steps.

3.5 Cryptography Algorithm

The following procedure is the proposed cryptography algorithm which is applied on the steganography image if the image security is at either low or risk.

Step 1: Matrix A is created by filling the elements with pixels of steganography image.

Step 2: Matrix B is created by changing the rows and columns of Matrix A.

Step 3: Apply Singular Value Decomposition (SVD) transform on Matrix B and Matrix A using the following equations,

$$[S_1\ V_1\ D_1] = SVD(\text{Matrix } A)$$
$$[S_2\ V_2\ D_2] = SVD(\text{Matrix } B)$$

SVD transform decomposes the image into three-matrix components as S, V and D. The edges are preserving in V components than the other components (A and D). Hence, the V component is used for generating the encryption key. The encryption key is generated by integrating the elements of V_1 and V_2 in an array.

Step 4: The integer elements in Matrix S_1 is transformed to Matrix X and the fractional elements in Matrix S_2 is transformed to Matrix Y.

Step 5: Generate encrypted image (Fig. 7) using the following equation as,

$$E = A \wedge X;$$

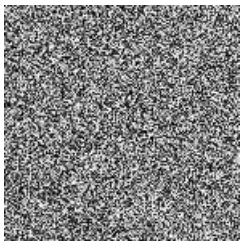


Fig. 7: Encrypted image

4 Results and Discussion

The proposed hybrid image security methodology is applied on various set of benchmarked images and medical images. The brain MRI images used in this manuscript are obtained from 'BrainWeb' open-access dataset. In this paper, 72 brain MRI brain images are acquired from this dataset and the proposed methodology is evaluated on these images. The bone images (36 images) are obtained from 'ISBWEB' dataset.

The cameraman cover image and secret-brain image are shown in Fig. 8(a) and Fig. 8(b) respectively. Fig. 8(c) shows the secret bone image. Fig. 9(a) shows the secured brain secret image and Fig. 9(b) shows the secured bone secret image.

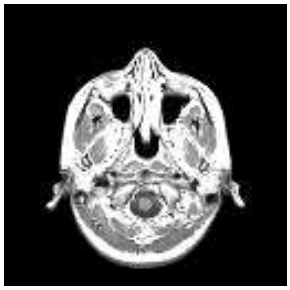
Table 1 analyses the impact of k value in fusion on secured images. From Table 2, it is clear that the IE value is high for high value in k, which does not require further cryptography process.

In this paper, MATLAB R2014 software is used to calculate the performance of the proposed image security algorithms on both brain and bone images. The performance evaluation parameters PSNR,MAE and MSE are used to calculate the parameters of the proposed system. The pixel difference between source secret image and its recovered image is represented by PSNR and it is represented in dB as computed as follows.

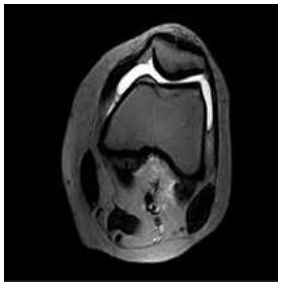
$$PSNR = 20\log_{10}\frac{255_f}{\sqrt{MSE}}$$

The maximum pixel value in secret image is 255 and the error between source and retrieved secret image is noted

(a) Cover image (Cameraman image)



(b) Secret image-1 (Brain image)



(c) Secret image-2 (Bone image)

Fig. 8: Cover and Secret images

Table 1: Impact of k value in fusion on secured images

Brain image sequences	K value in fusion rule	IE	Bone image sequences	K value in fusion rule	IE
Brain image 1	1.1	8	Bone image 1	0.02	7.8
Brain image 2	0.02	6.5	Bone image 2	0.01	7.1
Brain image 3	0.01	6.4	Bone image 3	0.04	6.7
Brain image 4	0.03	7.1	Bone image 4	1.1	8.2
Brain image 5	1.2	8.1	Bone image 5	0.03	7.9

Table 2: IE values for different set of secured images

Brain image sequences	IE	Cryptography required or not	Bone image sequences	IE	Cryptography required or not
Brain image 1	8	Not required	Bone image 1	7.8	Required
Brain image 2	6.5	Required	Bone image 2	7.1	Required
Brain image 3	6.4	Required	Bone image 3	6.7	Required
Brain image 4	7.1	Required	Bone image 4	8.2	Not required
Brain image 5	8.1	Not required	Bone image 5	7.9	Required

(a) Secured image (Cover image: Cameraman; secret image: Brain image)

(b) Secured image (Cover image: Cameraman; secret image: Bone image)

Fig. 9: Secured images

as MSE, which is described in the following equation as stated below.

$$MSE = \frac{1}{P \times Q} \sum_{0}^{X} \sum_{0}^{Y} \|(S_1 - S_2)\|^2$$

where, the image size is represented by its width and height, P and Q respectively. The source secret image is S_1 and retrieved secret image is S_2. X is the maximum pixel value in source secret image and Y is the maximum pixel value in retrieved secret image.

Table 3 illustrates the performance analysis of the proposed methodology in terms of PSNR.

The Mean Absolute Error (MAE) of the proposed methodology can be computed using the equation as stated below.

$$MAE = \frac{1}{P \times Q} \sum_{0}^{X} \sum_{0}^{Y} \|(S_1 - S_2)\|$$

Table 4 illustrates the proposed image security methodology on brain MRI image dataset with respect to the conventional methodology Emad et al. (2018).

The proposed methodology achieves 47.45 dB of PSNR, 169.84 MSE and 41.58% of MAE on brain-image dataset as depicted in Table 4. Fig. 10 shows the graphical analysis of the proposed method for brain images

The proposed image security methodology achieves 47.04 dB of PSNR, 165.86 MSE and 31.66% of MAE on bone image dataset, while the conventional methodology. Emad et al.(2018) achieves 40.78 dB of PSNR, 183.56

Table 3: Performance analysis in terms of PSNR

Methodology	Year	PSNR (dB)
Proposed work	2018	48.75
Emad et al.	2018	41.71
Rejani et al.,	2015	45.49
Odai M. Al-Shatanawi et al.	2015	43.39
Manjula and AjitDanti	2015	42.42

Table 4: Analysis of proposed methodology on brain MRI image dataset

Image Sequences	Emad et al.(2018)			Proposed Algorithm		
	PSNR	MSE	MAE	PSNR	MSE	MAE
Brain image 1	40.8	181.6	32.7	48.75	167.8	39.79
Brain image 2	41.7	182.5	33.6	47.1	172.6	41.85
Brain image 3	40.1	181.2	31.8	48.81	165.2	37.74
Brain image 4	41.8	182.7	35.7	46.84	171.5	43.75
Brain image 5	39.7	181.3	36.9	45.75	172.1	44.79
Average	40.82	181.86	34.14	47.45	169.84	41.58

Table 5: Analysis of proposed methodology on bone MRI image dataset

Image Sequences	Emad et al.(2018)			Proposed Algorithm		
	PSNR	MSE	MAE	PSNR	MSE	MAE
Bone image 1	40.1	182.6	33.7	44.7	165.7	32.1
Bone image 2	41.2	183.8	34.1	46.9	163.9	30.8
Bone image 3	41.3	182.7	32.1	45.8	171.8	32.7
Bone image 4	42.8	186.1	34.9	49.1	161.7	31.9
Bone image 5	38.5	182.6	37.9	48.7	166.2	30.8
Average	40.78	183.56	34.54	47.04	165.86	31.66

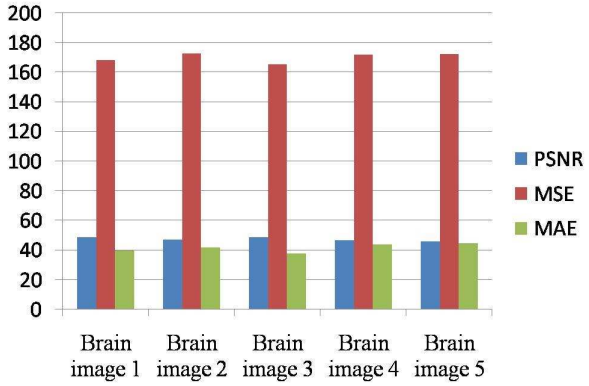


Fig. 10: Graphical analysis for brain images

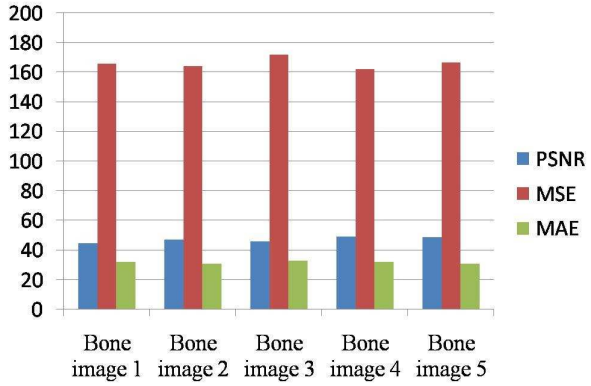


Fig. 11: Graphical analysis for bone images

MSE and 34.54% of MAE on bone image dataset, as depicted in Table 5. Fig. 11 shows the graphical analysis of the proposed method for bone images.

5 Conclusion

In this manuscript, the level of image security is improved by integrating the steganography and cryptography techniques in order to produce the secured image. DT-CWT is used in this paper to produce secured image. Further, cryptography algorithm is applied on the steganography image if the level of information entropy lies beyond the threshold value. In future, this methodology can be improved for protecting the audio and video data into image file.

References

[1] Suchitra Sinha, Prateek Gupta, Image Steganography using desynchronization, International Journal of Computer Science and Mobile Computing, vol. 5, no. 2, pp. 55–61 (2016).

[2] Shikha Mohan and Satnam Singh, Image Steganography: Classification, Application and Algorithms, International Journal of Core Engineering & Management (IJCEM), vol. 1, no. 10 (2015).
[3] Soria-Lorente and S. Berres, A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information, Security and Communication Networks, Article ID 5397082, 14 pages, (2017).
[4] C. Chang, T. Chen and L. Chung, A steganographic method based upon JPEG and quantization table modification, Information Sciences, vol. 141, no. 1–2, pp. 123–138, (2002).
[5] X. Li and J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences, vol. 177, no. 15, pp. 3099–3109, (2007).
[6] Odai M. Al-Shatanawi1 and Nameer N. El. Emam, A new image steganography algorithm based on MLSB method with random pixels selection, International Journal of Network Security & Its Applications (IJNSA), vol. 7, no. 2, (2015).
[7] G.R. Manjula and AjitDanti, A novel hash based least significant bit (2–3-3) image steganography in spatial domain, International Journal of Security, Privacy and Trust Management, vol. 4, no. 1, pp. 11–20, (2015).
[8] R. Rejani, D. Murugan and Deepu V. Krishnan, Pixel pattern based steganography on images, ICTACT Journal on Image and Video Processing, vol. 5, no. 3, (2015).
[9] Amitesh Kumar, Ashish Kr. Luhach and Dhermendra Pal, Robust Digital Image Watermarking Technique using Image Normalization and Discrete Cosine Transformation, International Journal of Computer Applications, vol. 65, no. 18, pp.5-13, (2013).
[10] Kamaldeep Joshi, Swati Gill and Rajkumar Yadav, A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the gray-scale Image, Journal of Computer Networks and Communications, vol. 2018, Article ID 9475142, 10 pages, (2018).
[11] K.H. Jung, Dual image based reversible data hiding method using neighboring pixel value differencing, Imaging Science Journal, vol. 63, no. 7, pp. 398–407, (2015).
[12] S. Batra and R. Rishi, Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels, International Journal of Security and Its Applications, vol. 4, no. 3, pp. 1–10, (2010).
[13] A.A.-A. Gutub, Pixel indicator technique for RGB image steganography, Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 1, (2010).
[14] K. Joshi and R. Yadav, A new LSB-S image steganography method blend with cryptography for secret communication, in Proceedings of the Third International Conference on Image Information Processing (ICIIP), pp. 86–90, Waknaghat, India, (2015).
[15] K. Joshi and R. Yadav, New approach toward data hiding using XOR for image steganography, in Proceedings of the Ninth International Conference on Contemporary Computing (IC3), pp. 1–6, IEEE, Noida, India, August (2016).
[16] M. Khan, S. Muhammad, M. Irfan, R. Seungmin and B.W. Sung, A Novel Magic LSB Substitution Method (M-LSB-SM) Using Multilevel Encryption and Achromatic Component of an Image, Springer, (2015).
[17] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, A secure image steganography algorithm based on least significant bit and integer wavelet transform, in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639–649, (2018).
[18] P.Y. Ma, B. Wu, B.J. Shastri, A.N. Tait, P. Mittal and P.R. Prucnal, Steganographic Communication via Spread Optical Noise: A Link-Level Eavesdropping Resilient System, in Journal of Lightwave Technology, vol. 36, no. 23, pp. 5344–5357, (2018).

T. Yuvaraja is currently is working as Assistant Professorin Department of ECE, Kongunadu college of Engineering and Technology, Trichy, Tamilnadu,India. He received his B.E. degree in Electronics and communication Engineering from Anna University, Chennai in the year 2005 and M.E. degree in Applied Electronics from Anna University, Chennai in the year 2008. He has more than 10 years of teaching experience in ECE. He has published more than 7 papers in international Journals and presented 8 papers in national and international conferences. His research areas of interest are Image Processing,Cryptography and steganography.

R. S. Sabeenian is currently working as Professor and Head in ECE Department in Sona College of Technology, Salem, Tamil Nadu, India. He has more than 17 years of teaching experience. He received his B.E from Madras University and his M.E in Communication Systems from Madurai Kamaraj University. He received his Ph.D. Degree from Anna University, Chennai in the year 2009 in the area of Digital Image processing. He is currently heading the research group named Sona SIPRO (SONA Signal and Image PROcessing Research Centre) centre located at the Advanced Research Centre in Sona College of Technology, Salem. He has published more than 85 research papers in various International, National Journals and Conferences. He has also published around seven books nationally and one book internationally. He is a Reviewer for the journals of IET, UK and ACTA Press Singapore. He received the Best Faculty Award for the year 2009 given by the Nehru Group of Institutions, Coimbatore and the Best Innovative Project Award from the Indian National Academy of Engineering, New Delhi for the year 2009 and ISTE Rajarambapu Patil National Award for Promising Engineering Teacher for Creative Work done in Technical Education for the year 2010 from ISTE. He has also received a Project Grant from the All India Council for Technical Education, DST, TNAU and Tamil Nadu State Council for Science and Technology for carrying out research. He received two Best Research Paper Awards from Springer International Conference and IEEE International Conference in the year 2010. He was also awarded the IETE Biman Behari Sen Memorial National Award for outstanding contributions in the emerging areas of Electronics and Telecommunication with emphasis on R& D for the year 2011. The Award was given by Institution of Electronics and Telecommunication Engineers (IETE), New Delhi. He is the Editor of six International Research Journals. He is also associated with the Image Processing Payload of the PESIT Pico Satellite Project. He was the Honorary Treasurer of IETE Salem Sub Centre from 2010 to 2014. He is the Coordinator for AICTE-INAE DVP Scheme. His areas of interest include texture analysis, texture classification and pattern recognition. He delivered more than 50 guest lectures and chaired more than 25 national and international conferences. He received ISTE Periyar Award for Best Engineering College Teacher for the year 2012. He received more than 97 lakhs research grants from various funding agencies like AICTE, DST, TNSCST, TNAU, INAE, IETE, ISTE, IEEE Anna University and various industries. He also received AICTE Career Award for Young Teacher (CAYT) for carrying out the Project 'Development of Digital Encoding System for Tamil Characters in Palm Leaf Manuscripts' from 2015 to 2018. Recently he received Best Faculty Award Senior Category under ECE stream for the year 2015–2016 from Nehru Group of Institutions.