ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

A High Integrity Approach to Digital Image Authentication

Rameeza Beevi N[1], Shanavaz K T[2]

PG Student [Signal Processing], Dept. of ECE, College of Engineering, Kallooppara, Kerala, India[1]

Associate Professor, Dept. of ECE, College of Engineering, Kallooppara, Kerala, India[2]

ABSTRACT: Watermarking techniques are widely used for image authentication and for protection of images from some unwanted modifications such as tampering in digital image processing applications. This watermarking algorithm helps to detect the tampered areas of received image and also to locate the tampered zones. These tasks can be accomplished with check bits and reference bits generated from the image respectively. This paper presents a watermarking method based on the source channel coding approach. Original image is source coded using the set partitioning in hierarchical trees (SPIHT) compression algorithm and the compressed image can be protected from tampering to a great extent with proper channel coding technique. Here Reed Solomon (RS) coding method is used as the channel coding technique. Also watermark is embedded into the Alpha channel of the host image here. At the receiver, decoder produces the encoder output bit stream if the tampering is below the certain limit. Decoder exploits the location of the erased blocks during decoding process which are known thanks to the embedded check bits. The output of the source decoder is then used to replace the tampered blocks at the tampered area. This source channel coding method can be used as an efficient approach with effective peak signal to noise ratio(PSNR) which helps to achieve high quality for both watermarked and reconstructed images and also high tolerable tampering rates(TTR) are affordable with this method.

KEYWORDS: Image watermarking, Set Partitioning in Hierarchical Trees(SPIHT),Reed Solomon(RS)coding.

I.INTRODUCTION

Digital Watermarking describes methods and technologies that embed hidden information, for example a string in digital media, such as images, video or any other kind of noise-tolerant digital signal such as multimedia data. Digital imaging has been rapidly developing in last two decades, and digital multimedia products are utilized in so many applications nowadays. As a consequence of this development, most image editing applications need the integrity of digital images. On the other hand, sophisticated techniques are required to the integrity of an image or protect it against malicious modifications. Watermarks are widely used for image authentication and for protecting images from unwanted modifications such as tampering in image editing applications.

In this work, a watermarking algorithm helps to achieve two purposes in case of image tampering is developed: First one is to detect the tampered area of the received image and second one for recovering the lost information in the tampered zones. We can accomplish these tasks using watermarks consisting of check bits and reference bits. In watermark embedding process, the original image is source coded and then the output bit stream is protected from tampering using appropriate channel encoder. Here the wavelet transform and set partitioning in hierarchical transforms (SPIHT) source encoding method is used to efficiently compress the original image. Also Reed- Solomon (RS) codes with large encoding blocks and over large Galva fields is used to solve the erasure problem. Therefore, the watermark consists of three parts in our algorithm: source code bits, channel code bits and check bits. Check bits are used at the receiver to determine the erasure location of the decoder. The output of channel decoder is source decoded to find the compressed version of the original image.

II.LITERATURE SURVEY

Image authentication techniques have great attention due to its importance for a large number of multimedia applications. Digital images are transmitted over non-secure channels such as the Internet. Therefore, military, medical

DOI:10.15662/IJAREEIE.2016.0506005

and quality control images must be protected from unwanted modifications. To protect the authenticity of multimedia images, several approaches have been developed. These approaches uses conventional cryptography, fragile watermarking and digital signatures that are based on the image content. It is well known that digital images can be manipulated with ease. Furthermore, it is generally impossible to tell whether a given image is authentic or has been manipulated subsequent to capture by some readily available digital image processing tools. This is an important issue in legal applications, news reporting and medical archiving, where we want to check that the digital image in question reflects what the scene looked like at the time of capture. Another need of authentication of images is in, for example, electronic commerce where the seller transmits a digital image to the buyer over the network. In this case the buyer needs to detect the authenticity that is he wants to be sure that the received image is indeed genuine. Here we not only want to verify the integrity of an image, but we also want to check for original ownership. Following are the image authentication techniques used previously.

a) HASH GENERATION

An image hash is an essential component of any signature based approach to check the authenticity of protected query images. It is a short signature of an image that is robust to some modifications such as small rotations, compression, scaling, addition of noise etc and sensitive to distinct queries and illegal tampering [2]. For verification, given the hash of the original and the query, the hash verification algorithm verifies the authenticity of the query. Only allowably modified images such as slightly rotated, cropped, JPEG compressed etc are detected as authentic. Tampered or distinct images are declared non-authentic. For non-authentic images, the application may also require the method to be able to localize any tampering in the image. To generate a multimedia hash, a secret key is used to get certain features from the data. These features are further processed to form the hash[3].The hash is transmitted along with the media data either by appending or embedding it to the primary data. At the receiver , the authenticator uses the same key which is used in the transmitter section to generate the hash values, which are compared with the ones transmitted along with the data for verifying its authenticity. The limitation of this integrity verification technique is that it requires a secure channel that must be reused for each image transmission.

b) FRAGILE WATERMARKING

Fragile watermarking is a technique for inserting the watermark into an image, which can be later extracted for a variety of purposes including identification and/or authentication purposes. Fragile watermarking system which embeds a watermark in the discrete wavelet domain of the image by quantizing the corresponding coefficients[4]. Tamper detection can be achieve in localized spatial and frequency regions. This approach provided information on specific frequencies of the image that have been modified. Fragile watermarks are of two types, *public key* and *private key* methods[5].Fragile watermarking techniques aim only to check the integrity of image or locate the tampered area with little robustness against image processing modifications[6].

c) SELF RECOVERY METHOD

The idea of self-embedding a form of image into itself enables not only detection of areas that have been tampered or manipulated, but also recovering the missing information. This class of watermarking techniques aims to achieve both tasks of tampering localization and error concealment via a single watermark[7]. The problem of image self recovery can be approached in numerous ways. In conventional error control coding schemes are used for restoration. Several methods embed a form of representation of the original image into itself for the sake of self-recovery. In discrete cosine transform (DCT) coefficients or reduced color-depth form of the host image is embedded in the least significant bits (LSB) of the original image[8]. Watermark bits in self-recovery methods are fallen into two categories, namely check bits and reference bits where check bits are used to localize the tampered zones, whereas the reference bits are employed to restore the original image in the tampered area. The drawback of self recovery method is that when one block is marked as tampered, all its carrying reference bits are missed.

d) ZHANG'S METHOD OF IMAGE SELF RECOVERY

Later Zhang proposed a self embedding method based on DCT coefficients of the image [9].Similar to some previous methods, the watermark data in this scheme are also made up of two parts that will be respectively used for tampered area detection and content recovery, and the original image data in the five MSB-layers are kept unchanged while the three LSB of all pixels are replaced with the watermark data. But the mechanism for generating the reference data used for content recovery is indeed different. In this scheme, the reference data are generated from a non uniform quantization of a linear representation of original DCT coefficients and does not contain any additional redundancy.

e)KORUS METHOD OF IMAGE SELF RECOVERY

This method is based on an alternative approach to spread the reference information over the whole image. Instead of using a combined approach with locally applied random projection and globally-applied scattering, here uses a spreading mechanism which uses the whole image in the process. Unlike in scattering, each image block uniformly contributes to the entire embedded watermark[10].As a result, every pixel carries information about the whole image . In this scheme also the reference data in is generated by the least square quantization of the DCT coefficients. This information is then channel coded with a particular rate λ and embedded as the watermark data. Therefore, the λ parameter determines the trade-off between the quality of the restored image and TTR for a certain embedding capacity. Here, the Foundain coding method is used as the channel coding mechanism. The limitation of Foundain coding is that when one block is detected as tampered ,all its carrying reference bits are missed. Another limitation is that, this method provides constant quality of reconstruction for tampering up to a certain limit and thereafter failed to reconstruct beyond that limit.

III.PROPOSED METHOD

In this work, an efficient method of watermarking is introduced for image authentication with high integrity for images. The watermark consists of three parts in this algorithm: source code output bits, channel code parity bits and check bits. Source code bits which are the reference bits in this work are the bit stream of the SPIHT-compressed original image at a desired rate[11]. In order to survive tampering, the reference bits are channel coded using RS coding to produce channel code bits[12]. The channel coded data along with the hash value generated from the image using MD5 algorithm is inserted as the watermark data to the Alpha channel of the host image. For this, the host image is converted to a PNG format with an appended alpha channel. Assume the number of image pixels are $N = N1 \times N2$, where $N1$ and $N2$ stand for numbers of rows and columns of the original image. We compress the original image into $Ns = N \times ns$ bits using proper source coding algorithm (SPIHT here). A channel coding algorithm (RS code here) is applied to permuted compressed image bit stream. Channel coded bits are permuted and spread over the whole image. The permutation for channel coding are generated using a secret key K, which is known to both embedding phase (transmitter end) and image reconstruction phase (receiver end), to guarantee the security of our algorithm. The original image is also divided into blocks of size $B \times B$, thus each block will host channel code bits. These bits are basically belonged to some other blocks, whose rows and indices are turned into a binary stream of bits called position bits. These position bits along with MSB bits of each block are inputted to a hash generator algorithm (MD5 here), to produce hash bits. A random binary key of length bh fixed for the whole image is generated at the embedding phase. This key is *XOR*ed with hash bits to produce bh check bits. These bh check bits along with bc channel code bits of the corresponding blocks are spread over the block which results in embedding this watermark data and thus watermarked image is created.

At the reconstruction part of this work, the watermarked data is read out from the Alpha channel and thereafter this Alpha channel is discarded. Later, the received image tampered to some percentage is generated. Then the received image is watermark decomposed to generate channel coded bits and hash bits. Also the block decomposition of the received image generate position bits. This position bits and the MSB bits are embedded to produce the hash bits. The XOR of calculated hash bits and the extracted check bits is calculated for each block , this value is equal to the random binary key used in the algorithm. This way the tampered blocks can be detected.

The list of tampered blocks determines erasure locations and also helps the channel erasure decoder to find the compressed image bit stream despite the erasure. Then source encoded image would be later decoded and the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

estimation of the original image is recovered. The process of tampering detection and image recovery schemes are shown in Fig. 1 and 2 respectively.

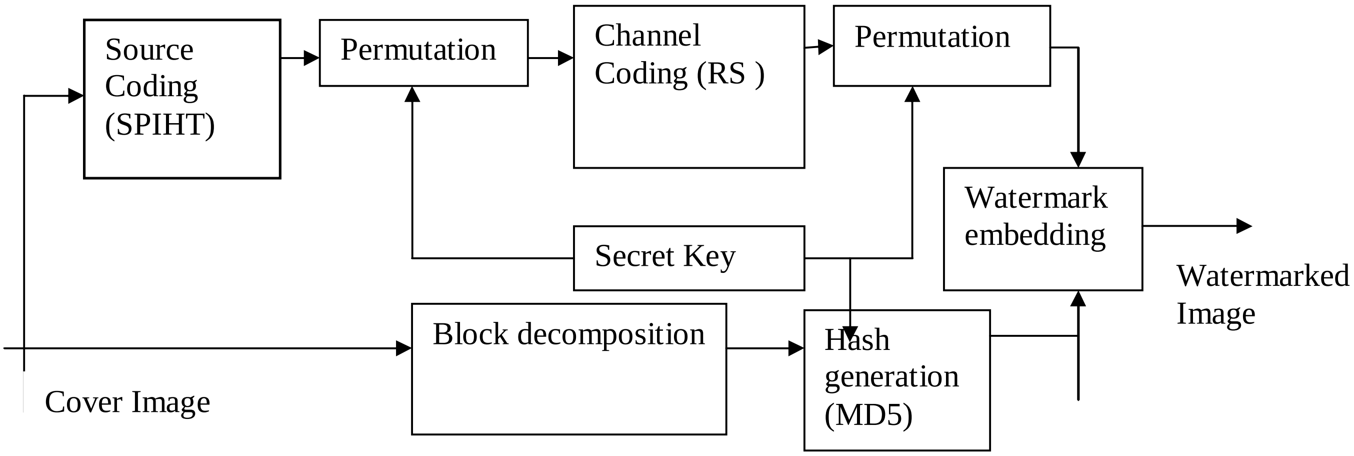

Fig 1.Block diagram of Watermark embedding

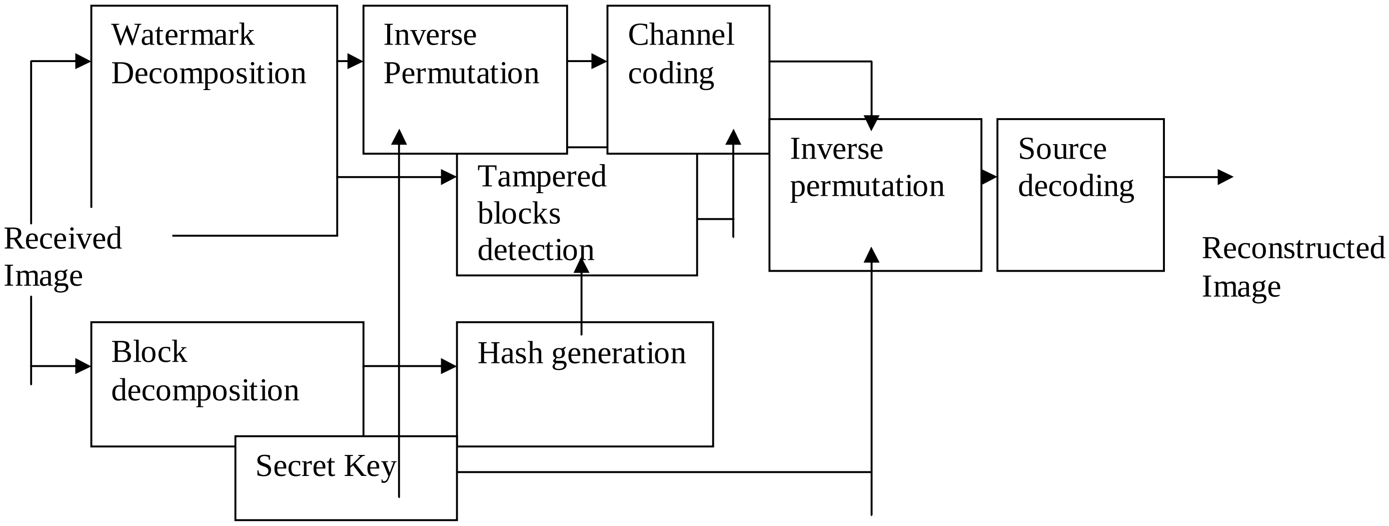

Fig 2.Block diagram of tampering detection and image recovery scheme.

IV .DESIGN AND ANALYSIS

In this section, the parameter design of this algorithm is discussed .Here the 8-bit gray scale Cameraman image of size 512 × 512 is taken as the input image for protecting it from tampering. Also the wavelet transform and Set Partitioning in Hierarchical Trees (SPIHT) Compression algorithm is used as the source coding method. Also Reed Solomon coding is applied as channel coding method to protect source encoded image from tampering to a great extend. The MD5 algorithm is used for hash value calculation. Also set the block size as B = 8. That is, the image is divided into 8×8 blocks in block decomposition process .

The average energy of distortion imposed by watermarking measured by MSE (Mean Square Error) equals:

MSE= sum(sum((Image-original Image)).^2))/nRow/nColumn (1)

Where nRow and nColumn denote the number of rows and columns of the original image.
Therefore, the average peak signal to noise ratio (PSNR) is calculated as:

$$\text{PSNR}=10\ log_{10}(\frac{255^2}{MSE}) \quad (2)$$

For image recovery, the PSNR of more than 40 dB at the recovered tampered region is acceptable in scenario. Simulations also show that the Cameraman photo can be compressed at the rate of 1 bpp with PSNR of 44.9 dB utilizing SPIHT.

V. RESULT AND DISCUSSION

Original cameraman input image of size 512×512 is source coded using SPIHT compression algorithm. The input image is shown as Fig 3.

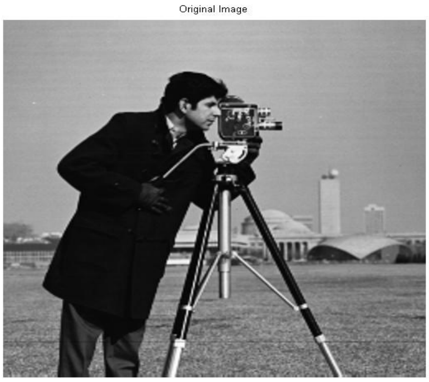

Fig 3.Input Image

The SPIHT compressed bit stream is generated thereafter. The compressed bit stream produced is later channel coded with RS coding technique and the channel coded data is generated. The hash value of the image is also generated using the MD5 algorithm. This channel coded data along with the hash value data are embedded to the alpha channel as watermark data and the watermarked image is generated. The watermarked image generated by alpha channel method is shown in Fig 4.

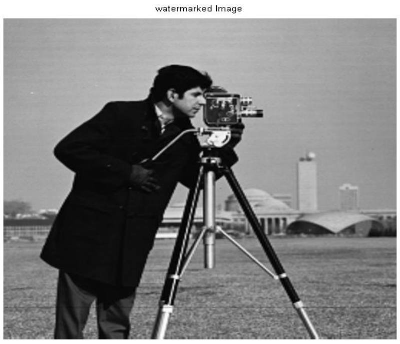

Fig 4.Watermarked Image

The watermarked image tampered to some percentage is later generated. This image is received at the tampering detection and image recovery part. The tampered image generated for about 2% tampering is shown in Fig 5.

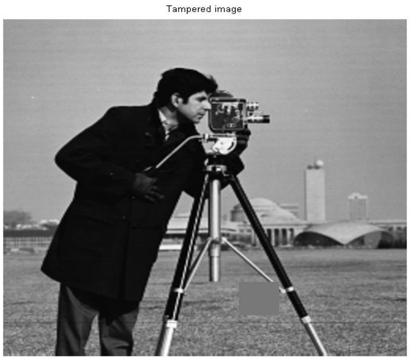

Fig 5.Tampered Image

The tampered area detected by check bit examination and the detected tampered area is shown in the Fig 6.

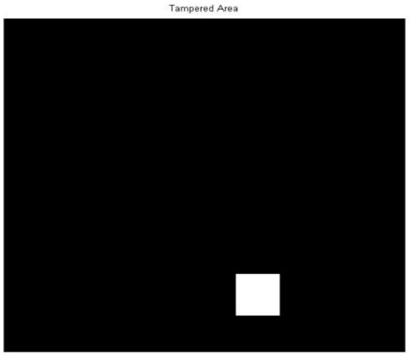

Fig 6.Tampered area

After locating the tampered blocks, the channel coded data is channel decoded using RS decoding technique and thereafter source decoded using SPIHT decoding technique and thus the reconstructed image is generated with aPSNR value of 46.95 dB.The reconstructed image is shown in Fig 7.

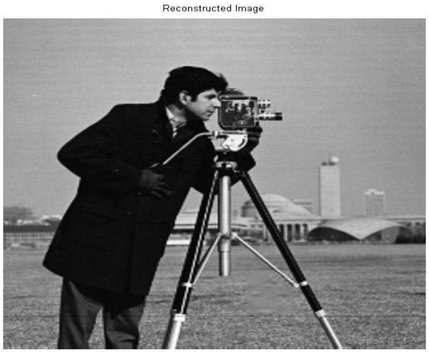

Fig 7 Reconstructed Image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

The graph showing the relation between Tolerable Tampering Rate (TTR) and PSNR values for the proposed method is shown below in Fig 8 .Here tampering of rate 95% can be tolerable with this method.

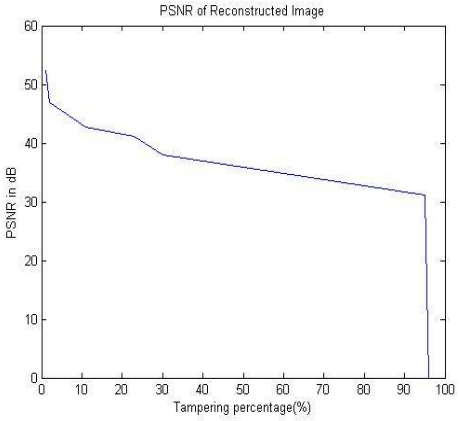

Fig 8 Graph between PSNR and TTR

V1. CONCLUSION

In this work, a watermarking method based on source channel coding approach is introduced. This method of self recovery is an efficient approach for image authentication with high integrity for digital images. The watermark bit-budget in this scheme falls into three parts: Hash bits, source encoder output bits and channel encoder parity bits. The original image is source encoded using SPIHT compression algorithm and the output compressed bit stream is later channel coded using RS coding technique .The hash bits generated from the image along with the channel coded data is inserted as the watermark data in alpha channel the watermarked image is generated. The alpha channel masking algorithm is used improve the robustness and protection along with security. Alpha channel is an additional channel which contains the information regarding the image transparency and its various level. It is an extra 8bit channel which controls the transparency of watermarking. The channel coding technique applied after the source coding technique helps to avoid the tampering problem to a great extend. At the receiver ,the decoder reveals the encoder output bit stream if the tampering is below the certain limit. Here the method of watermarking can be flexibly adapted to different applications with different purposes, with the help of capability of applied source and channel codes. The tampered area of the image is also detected by checking the hash bits. The reconstructed image is generated after tampered blocks detection with a greater PSNR value of 46.95 dB for about 2% tampering. Also this method is tolerable for about 95% about tampering. So this method of watermarking outperforms other methods in terms of image quality of reconstructed image as well as for TTR.

.

REFERENCES

[1] Saeed Sarreshtedari, Mohammad Ali Akhaee, “A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery,” IEEE Trans.on Image Processing, vol. 24, no. 7, July. 2015.

[2] A. Swaminathan, Y. Mao, and M. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[3] S. Roy and Q. Sun, “Robust hash for detecting and localizing image tampering,” in Proc. IEEE Int. Conf. Image Process. (ICIP), vol. 6. Sep./Oct. 2007, pp. VI-117–VI-120.

[4] P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[5] J. Fridrich, “Image watermarking for tamper detection,” in Proc. Int. Conf. Image Process. (ICIP), vol. 2. Oct. 1998, pp. 404–408.

[6] D. Kundur and D. Hatzinakos, “Digital watermarking for telltale tamper proofing and authentication,” Proc. IEEE, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[7] J. Fridrich and M. Goljan, “Images with self-correcting capabilities,” in Proc. Int. Conf. Image Process. (ICIP), vol. 3. 1999, pp. 792–796.

[8] H.-J. He, J.-S. Zhang, and F. Chen, “Adjacent-block based statistical detection method for self-embedding watermarking techniques,” Signal Process., vol. 89, no. 8, pp. 1557–1566, 2009.

[9] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self recovery quality based on compressive sensing and compositive reconstruction," IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.

[10] P. Korus and A. Dziech, "Efficient method for content reconstruction with self-embedding," IEEE Trans. Image Process., vol. 22, no. 3,pp. 1134–1147, Mar.2013.

[11] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," IEEE Trans. Circuits Syst. Video Technol., vol. 6, no. 3, pp. 243–250, Jun. 1996.

[12] S. B. Wicker, Reed–Solomon Codes and Their Applications. Piscataway, NJ, USA: IEEE Press, 1994.

BIOGRAPHY

Rameeza Beevi N is currently pursuing M.Tech in electronics with specialisation in Signal Processing from College Of Engineering, Kallooppara (CUSAT University), Kerala, India. She received her B.Tech degree in Electronics and Communication from University college of Engineering, Kariavattom,Trivandrum, Kerala, India. Her areas of interest are Digital Image Processing, Digital Communication, Wavelet and Embedded Design.

Shanavaz K T is currently working as Associate Professor in College Of Engineering, Kallooppara, Kerala, India. He received his Phd in Image Processing , M.Tech on Digital System Communication Engineering from NIT Calicut and B.Tech degree on Electronics and communication Engineerig from College of Engineering ,Trivandrum, Kerala, India. His areas of interest are Digital Image Processing, Digital Communication, Wavelet and EmbeddedDesign.