J Electr Eng Technol.2015; 10(5): 2149-2154
http://dx.doi.org/10.5370/JEET.2015.10.5.2149

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Fragile Watermarking Scheme Based on Wavelet Edge Features

D.Vaishnavi† **and T.S.Subashini***

Abstract – This paper proposes a novel watermarking method to discover the tampers and localize it in digital image. The image which is to be used to generate a watermark is first wavelet decomposed and the edge feature from the sub bands of high frequency coefficients are retrieved to generate a watermark (Edge Feature Image) and which is to be embed on the cover image. Before embedding the watermark, the pixels of cover image are disordered through the Arnold Transform and this helps to upgrade the security of the watermark. The embedding of generated edge feature image is done only on the Least Significant Bit (LSB) of the cover image. The invisibleness and robustness of the proposed method is computed using Peak-Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) and it proves that the proposed method delivers good results and the proposed method also detects and localizes the tampers efficiently. The invisibleness of proposed method is compared with the existing method and it proves that the proposed method is better.

Keywords: DWT, Arnold Map, Fragile watermarking, Tamper detection, Edge Feature Image

1. Introduction

The images play an important role in news reporting, criminal investigation, insurance claiming, security assessment and military communications etc. Due to the advancement of technology, images are stored in digital form and can be transmitted over an internet medium. These images may be easily accessed and manipulated with the intension to collapse their integrity. As a consequence, it needs to be checked whether it is trustworthy. The digital image watermarking technique is one of the methods to check their integrity and it is consists of two methods: Robust method used to protect copy right of images [1] and Fragile method used to detect the tampers in the images [2-5]. A fragile watermarking scheme which is used to detect the tampers must follow the certain properties such as Invisibleness, Sensitivity and Security are very essential among them.

Invisibleness: The embedded mark should be perceptually unnoticeable to safeguard its shielding concealment.
Sensitivity: The embedded mark must be fragile to malicious tampering.
Security: The watermark must be hidden in a protected manner and it cannot be isolated illegally.

The modification or alteration on the watermarked image destroys the integrity of cover image and also content of the watermark image embedded on it. Therefore, verification process is required in watermarking system to detect and localize the tampered region. There are relative a number of fragile watermarking methods proposed in literature. The authors in [6], generated a watermark using the five Most Significant Bit (MSB) planes and embedded into the 3 Least Significant Bit (LSB) planes. The scheme in [7], uses the block-wise independence watermarking scheme using two Least Significant Bits in each image block of pixels. The method proposed in [15], utilizes logistic map to obtain the choatic pattern to generate the watermark and which is embedded in the LSB of each pixels. In [8], the authors detected the image modifications using a two-pass logistic map with Hamming code. Shivendra Shivani et al., [9] embedded the shuffled extensive ten bit recovery data and two bit authentication data of the image block into its Least Significant Bits (LSB) of its corresponding mapping block. The work in [10] uses the K-mean clustering algorithm on the watermarked image to calculate the number of one's and number of zero's in each layer separately. These clustered values are used as secret key and the tampered region in an image is mapped by comparing clustering values of watermarked image and tampered watermarked image. Sumalatha et al. [11] proposed a block based reversible watermarking using Discrete Wavelet Transform and the watermark is generated from the wavelet subbands. Bedi et al. [12] embedded a watermark either on the Discrete Hartley Transform (DHT) domain or in Discrete Cosine Transform (DCT) domain depending upon the number of edges in the block.

In this paper, a fragile watermarking scheme is proposed to detect the tampers using the Discrete Wavelet Transform (DWT). This paper consists of following sections. Section 2 furnishes the background study of the algorithms used in this paper, section 3 illustrates the proposed method, Section 4 discusses the experimental results and Section 5

† Corresponding Author: Dept. of Computer Science and Engineering Faculty of Engineering and Technology, Annamalai University, Tamilnadu, India. (vaishume11@gmail.com)
* Dept. of Computer Science and Engineering Faculty of Engineering and Technology, Annamalai University, Tamilnadu, India. (rtramsuba@gmail.com)

Received: December 21, 2014; Accepted: May 1, 2015

concludes the paper.

2. Algorithms

2.1 Discrete Wavelet Transform (DWT)

The 2D DWT is a linear transformation and is very commonly used tool in image processing and it decomposes the image into low frequency and high frequency coefficients. The low frequency coefficients give the approximation information and the high frequency coefficients (horizontal, vertical and detailed coefficients) give the detailed information such as edges, ridges and noise etc,. An edge provides the structural properties of objects in an image with reduced amount of information [13]. It aids to increase the invisibleness when watermark with less amount of information on the host image. Also these edge features controls the attacks caused by noise, edge strips and acuity.

2.2 Arnold map

It is very sensitive to initial conditions. So, it is mostly used in watermarking and encryption techniques. It is used as preprocessing step to embed the watermark, which reduces the spatial relationship between the pixels and makes the image as meaningless one [14]. The 2-dimentional Arnold scrambling algorithm is defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}\, N \quad x, y \in \{0,1,2,...,N-1\} \tag{1}$$

where, x, y is the pixel coordinates of the original space: x', y' is the pixel coordinates after iterative computation scrambling; N is the size of the image.

3. Proposed Method

The proposed fragile watermarking method consists of three phases. The first phase is generation of watermark, second phase is watermark embedding & extraction and third phase is tamper detection & localization which are explained in the following subsections.

3.1 Watermark generation

The edges are the major features which furnish the information about image content and the wavelet transform is marvelous way to detect the edge features, as, it increases the reliability of edge detection even when it is analyzed at different scales. However, a single level of decomposition is sufficient to obtain the edge features. Hence, the single level DWT is applied on the watermark image with 'haar' wavelet. Since, 'haar' wavelet is a simplest form of wavelet, computationally cheap, memory efficient and specifically it would be an optimal choice for finding the location of edges. DWT decomposes the image into one low frequency coefficients and high frequency coefficients. Low frequency coefficients contain signal information and high frequency coefficients contain excess details such as edge. In order to retrieve the edge details alone from the high frequency details, an adaptive threshold T is used. When applying a T on the high frequency coefficients, the resultant image of edge features is converted to binary and makes it easy to embed on the cover image. The value of the T is defined as sum value of mean and standard deviation of high frequency coefficients and the binary version of image is obtained using threshold is given in the Eq. (2).

$$w(i,j) = \begin{cases} 1 & if\ f(i,j) \geq T \\ 0 & if\ f(i,j) < T \end{cases} \tag{2}$$

where, $w(i,j)$ is binary edge image and $f(i,j)$ is high frequency coefficients matrix. Fig. 1 depicts the generation of watermark to embed on the cover image.

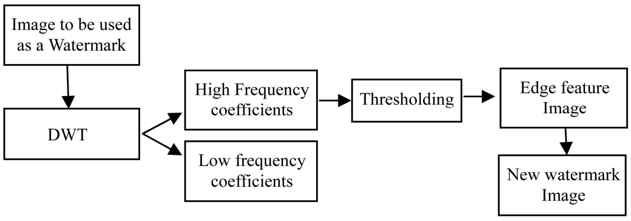


Image to be used as a Watermark
DWT
High Frequency coefficients
Low frequency coefficients
Thresholding
Edge feature Image
New watermark Image

Fig. 1. Watermark generation process

3.2 Watermark embedding and extraction

The watermarking method begins, only after the generation of watermark edge image was accomplished. Now the resolution of edge image is reduced to half as the host image. Hence the host image is divided into 2×2 non-overlapping blocks and watermark is embedded on the least significant bit of each block's first pixel element. In fragile watermarking method, watermark must be more sensitive and secure. Therefore, an Arnold scrambling is employed on the host image as a preliminary process. After embedding the edge image, watermarked image is constructed by the inverse Arnold scrambling.

In order to extract the watermark edge image embedded on host image, the Arnold scrambling is applied on watermarked image for number of iterations which is equal to the number of iterations done to embed the watermark edge image. Then it is segregated into 2×2 non-overlapping blocks and watermark is extracted from the least significant bit of first element of each block.

3.3 Tamper detection and localization

The tamper detection process begins after the extraction of watermark edge image. The original and extracted watermark edge images are subjected to XOR operation and it detects the difference among them and the image is decided as tampered or trustworthy based on the difference. Once the image is detected as tampered, the tampered region is localized by applying the inverse Arnold scrambling.

4. Results and Discussion

The experiment was done using the Mathworks MATLAB 12a. The sample images are gray scale image whose resolution is 256×256 pixels and the proposed method does not depending the resolution of an image but, the resolution of watermark and cover images must be equal and a square. The single level decomposition with 'Haar' wavelet scheme is utilized to get edge features from the wavelet sub-band and the watermark image is generated to embed on host image.

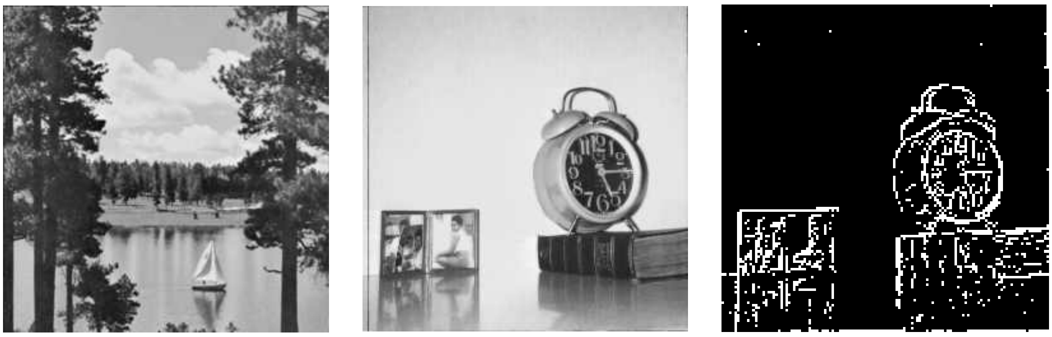
4.1 Results of watermarking scheme

The sample host image and the generated watermark image are shown in the Fig. 2. The watermark edge image is embedded on the host image to construct the watermarked image and the embedded watermark is extracted later to find whether an image was tampered or not. The watermarked and extracted watermark images are provided in Fig. 3(a) & Fig. 3(b). All the pixels values are zero in xor-ed output of embedded and extracted watermark and is given in the Fig. 3(c) It furnishes that the cover image is trustworthy.

In order to quantify the invisibleness and robustness of the proposed method when the images are not subjected to any attacks or alterations, the image quality metrics namely Peak-Signal-to Noise-Ratio (PSNR) and Normalized Correlation (NC) are computed. The performance of proposed method also validated by the various images which are taken from standard image processing database and its performances are given in Table 1. Fig. 4 provides the graphical representation about the performances of the proposed method using PSNR value. In order to carry out a performance comparison, the existing method [15] is

Table 1. Performances of proposed method using PSNR and NC values

Image	Invisibleness		Robustness (when image was not tampered)	
	PSNR	NC	PSNR	NC
Sail Boat	56.6433	0.9979	64.1851	0.9983
Lena	56.6935	0.9991	64.1892	0.9985
Cameraman	57.1370	0.9993	64.2026	0.9989
Barbara	57.2131	0.9994	64.2172	0.9989

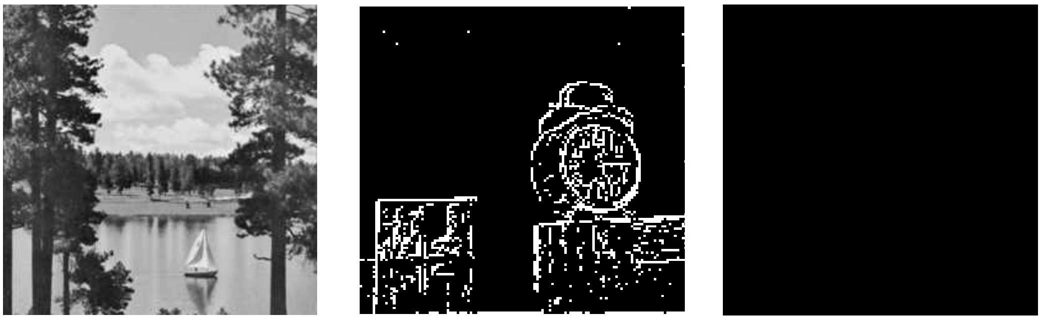


(a) Host Image (Sail boat)

(b) Watermark image (clock image)

(c) Generated watermark edge feature image

Fig. 2 sample test images and generated watermark image



(a) Watermarked image

(b) Extracted watermark

(c) XOR ed output

Fig. 3. Result of proposed method without tamper

implemented and its performances of PSNR values are given in the Table 2. It shows that the invisibleness of the proposed method is much better than the existing method [15].

4.2 Results of tamper detection and localization

The proposed method is examined to see how it detects and localizes the tampers namely copy & paste, text addition, image splice and object removal are introduced on the watermarked image. Then the watermark is extracted and results are demonstrated in the following subsections.

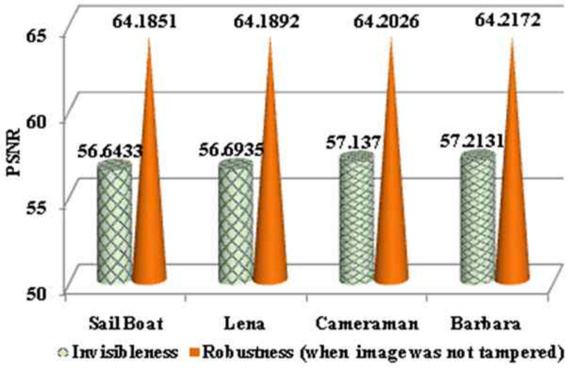


Fig. 4. Performances of proposed method using PSNR

Table 2. Performance comparison of invisibleness using PSNR

Images	Existing method [15]	Proposed method
Sail Boat	50.7261	56.6433
Lena	50.5683	56.6935
Cameraman	50.8637	57.1370
Barbara	50.7542	57.2131

4.2.1 Copy and paste attack

In the watermarked image, there is only one sailboat which is shown in the Fig. 3(a). In order to do this copy paste experiment, the sail boat is copied and pasted it near to the original sailboat, which is shown in the Fig. 5(a). Then the watermark is extracted and is displayed in the Fig. 5(b). The X-ored output in Fig. 5(c) shows some noise when compared the Xor-ed output of non-tampered image shown in Fig. 3(c). This indicates that watermarked image has been subjected to some kind of tampering and Fig. 5(d) shows the localized tampered region.

4.2.2 Text addition attack

To perform this experiment, the text ‘Sail Boat’ is merged in the watermarked image and is shown in the Fig. 6(a). Then the watermark is extracted from this manipulated image is shown in the Fig. 6(b). The X-ored output in Fig. 6(c) shows some noise when compared the Xor-ed output of non-tampered image shown in Fig. 3(c). This indicates that watermarked image has been subjected to some kind of tampering and Fig. 6(d) shows the localized tampered region.

4.2.3 Image splicing attack

To test the performance of proposed method, the object

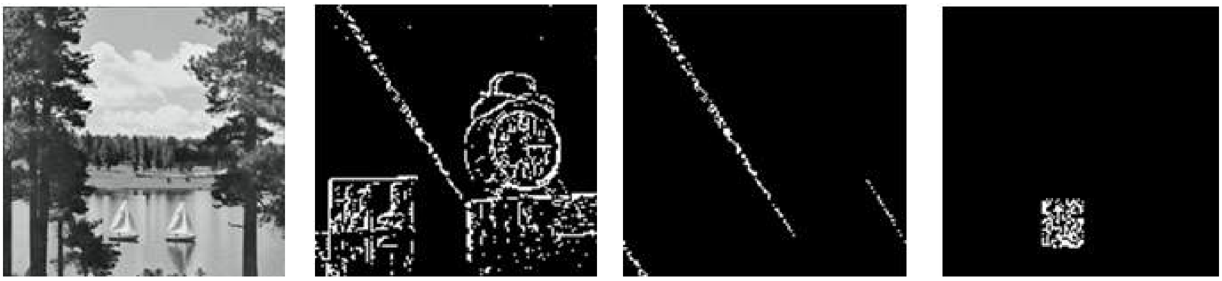
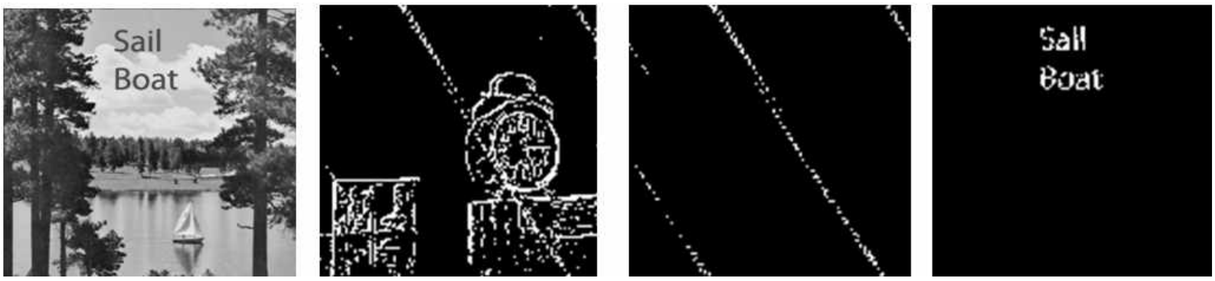
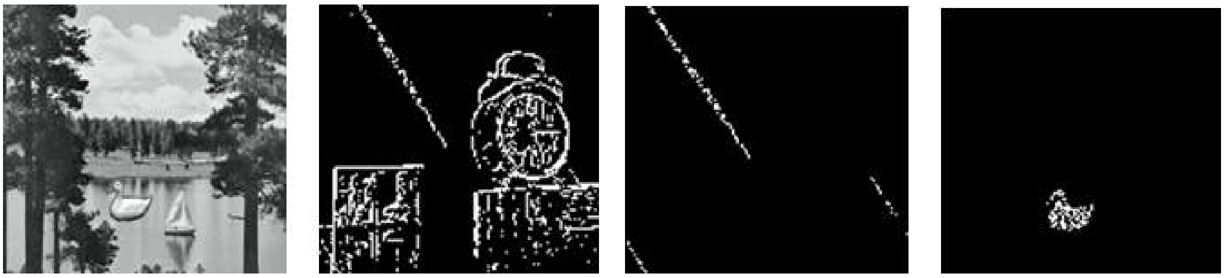

(a) Copy attack image (b) Extracted watermark (c) XOR ed output (d) Tampered region

Fig. 5. Result of copy move attack



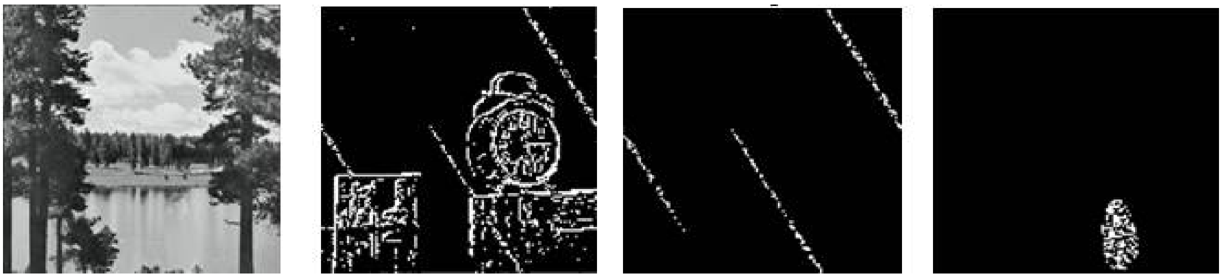
(a) Text addition attack image (b) Extracted watermark (c)Xor-ed output (d) Tampered region

Fig. 6. Result of text addition attack



(a) Image splic attacked image (b) Extracted watermark (c) Xor-ed output (d) Tampered region

Fig. 7. Result of image splicing attack



(a) Object removal attacked image (b) Extracted watermark (c) Xor-ed output (d) Tampered region

Fig. 8. Result of object removal attack

swan is combined in the watermarked image and is shown in the Fig. 7(a). Then the watermark is extracted from this manipulated image and which is displayed in the Fig. 7(b). The X-ored output in Fig. 7(c) shows some noise when compared the Xor-ed output of non-tampered image shown in Fig. 3(c). This indicates that watermarked image has been subjected to some kind of tampering and Fig. 7(d) shows the localized tampered region.

4.2.4 Object removal attack

To carry out this experiment, the object sailboat in the watermarked image is removed and is shown in the Fig. 8 (a). Then the watermark is extracted from this manipulated image and which is displayed in the Fig. 8(b). The X-ored output in Fig. 8(c) shows some noise when compared the Xor-ed output of non-tampered image shown in Fig. 3(c). This indicates that watermarked image has been subjected to some kind of tampering and Fig. 8(d) shows the localized tampered region.

5. Conclusion

A novel image watermarking method to discover and localize the tampers in an image was implemented successfully. The invisibleness and robustness of the proposed method were estimated using the PSNR and NC values and it provides the good values. The invisibleness and robustness (for non-tampered image) of proposed method were measured using PSNR and NC metrics. The invisibleness of proposed method is compared with the existing method[15] and it proves that the proposed method is better than the existing method. The proposed method is also examined to see how it detects and localizes the tampers subjecting to various tampers and its results shows that proposed method depicts that it efficiently detects and localizes the tampers where the region is altered.

References

[1] D. Vaishnavi and T. S. Subashini, “Robust and Invisible Image Watermarking in RGB Color Space Using SVD,” *Procedia Computer Science*, vol. 46, pp. 1770-1777, 2015.

[2] D. Vaishnavi and T. S. Subashini, “Image Tamper Detection based on Edge Image and Chaotic Arnold Map,” *Indian Journal of Science and Technology*, vol. 8, pp. 548-555, Mar. 2015.

[3] F. Di Martino and S. Sessa, “Fragile Watermarking Tamper Detection with Images Compressed by Fuzzy Transform,” *Inf. Sci.*, vol. 195, pp. 62-90, Jul. 2012.

[4] D. Xiao and F. Y. Shih, “An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing,” *Optics Communications*, vol. 285, pp. 2596-2606, 2012.

[5] R. C.-W. Phan, “Tampering with a watermarking-based image authentication scheme,” *Pattern Recognition*, vol. 41, pp. 3493-3496, 2008.

[6] S. Shan, “Logistic map-based fragile watermarking

for pixel level tamper detection and resistance," *EURASIP Journal on Information Security*, vol. 2010, 2010.

[7] W.-C. Chen and M.-S. Wang, "A fuzzy c-means clustering-based fragile watermarking scheme for image authentication," *Expert Systems with Applications*, vol. 36, pp. 1300-1307, 2009.

[8] C.-C. Chang, K.-N. Chen, C.-F. Lee, and L.-J. Liu, "A secure fragile watermarking scheme based on chaos-and-hamming code," *Journal of Systems and Software*, vol. 84, pp. 1462-1470, 2011.

[9] S. Shivani, D. Singh, and S. Agarwal, "DCT Based Approach for Tampered Image Detection and Recovery Using Block Wise Fragile Watermarking Scheme," in *Pattern Recognition and Image Analysis*, Springer, 2013, pp. 640-647.

[10] D. M. N. G. P. Dr.S.A.K.Jilani Manickam.L, "A Novel Fragile Watermarking Scheme For Image Tamper Detection Using K Mean Clustering," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, pp. 3380-3385, 2013.

[11] L. Sumalatha, V. V. Krishna, and A. V. Babu, "Image Content Authentication based on Wavelet Edge Features," *International Journal of Computer Applications*, vol. 50, 2012.

[12] S. S. Bedi, G. S. Tomar, and S. Verma, "Robust watermarking of image in the transform domain using edge detection," in *Computer Modelling and Simulation, 2009. UKSIM'09. 11th International Conference on*, 2009, pp. 233-238.

[13] D. Zhang, Z. Pan, and H. Li, "A contour-based semi-fragile image watermarking algorithm in DWT domain," in *Education Technology and Computer Science (ETCS), 2010 Second International Workshop on*, 2010, vol. 3, pp. 228-231.

[14] M. Sui and J. Li, "The medical volume data watermarking using arnold scrambling and 3D-DWT," in *Mechatronic Sciences, Electric Engineering and Computer* (*MEC*), *Proceedings 2013 International Conference on*, 2013, pp. 1120-1124.

[15] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *AEU-International Journal of Electronics and Communications*, vol. 65, pp. 840-847, 2011.

D.Vaishnavi She has received her BE (IT) degree in the year 2009 and ME (CSE) degree in the year 2011 from Annamalai University. She has worked as Assistant Professor at Anjalai Ammal Mahalingam Engineering College, Thiruvarur District, Tamil nadu, India. Currently, she is pursuing Doctor of Philosophy in Annamalai University. She has published 11 papers in International Journals and conferences. Her area of research is Image Processing, Image watermarking and Digital Forensics.

T.S. Subashini She has received her B.E (CSE) degree in the year 1991 from Bharath Engineering College, Chennai. In the same year she was appointed as Hardware Service Engineer in Sterling Computers Chennai and in 1996 she joined Annamalai University. She was sponsored by the University under Quality Improvement Programme (QIP), to pursue ME (CSE) at Anna University, Chennai 2001. She gained her doctoral degree in Computer Science and Engineering from Annamalai University in 2011. Her area of doctoral research is Medical Image Analysis. She has published over 35 research papers in international journals and conferences. She is now working on UGC sanctioned research project worth Rs. 11.4 lakhs on Breast Cancer. Her research interests include Image and Video processing, Computer Vision and Pattern Classification.