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. 2, Special Issue 1, December 2013

Watermarking Technique for Self Authentication and Recovery

Augustus P P[1], David Solomon George[2]

M.Tech Student, Department of ECE, Rajiv Gandhi Institute of Technology, Kottayam, India[1,]

Asst. Prof, Department of ECE, Rajiv Gandhi Institute of Technology, Kottayam, India[2]

Abstract: In this paper, an algorithm for invisible watermarking of digital images has been proposed. This scheme provides self authentication and recovery of watermarked image. The tampered regions in an image, if any, are detected and the recovery of those altered regions are facilitated by the proposed scheme. Image authentication is performed in 4×4 sub-block level. Self recovery is accomplished through descriptors, which enable in reconstructing the altered regions with acceptable quality. The descriptor details corresponding to each region are spatially separated from region of impact. Discrete Wavelet Transform (DWT) and Inverse Discrete Wavelet Transform (IDWT) are employed for the transformations within the image for block based retrieval. The proposed algorithm is experimentally verified and the results are presented.

Keywords: Authentication, descriptor, digest, watermarking

I. INTRODUCTION

Advances in computing hardware, software and networks have created threats to copyright protection and content integrity. Nowadays, softwares are available in market to fruitfully modify the image. With the advent of social networking sites, uploading and sharing of photos became an inevitable need. User community of such sites comprise of people around the globe. However, no measures are currently incorporated in the present day social networking sites to provide reliability of their multimedia content [1]. Therefore, now it is easy to copy, modify and distribute images. Malicious persons can acquire images from the internet and use versatile digital image processing tools to modify them without leaving a trace [2], [3]. The truthfulness of the images shared on the Internet is therefore questionable. These tools are capable of creating ambiguity to pick the original image in midst of spoofed ones. Images, thus uploaded in social networking sites are very much prone to such alterations. The alterations may be casual in some scenario, while harmful in others. Therefore, the need arises to ensure the authentication of digital images. It would be pleasing if the original image details are retrieved from the altered image. Prime concern lies in ensuring the authenticity of target image. Image authentication involves confirmation of the authenticity of image content and the detection of localized alterations, if any. The authentication watermark employed may be visible or invisible. Visibility is formulated based on whether it is perceivable to human eye or not. Many robust, fragile and semi-fragile techniques are available to provide authentication to digital images [4]. Robust watermarks could resist non-malicious distortions [1], [4]. Fragile watermarks are highly sensitive to alterations [1], [4]. They can accurately detect the changes made in the marked image. The underlying idea behind fragile technique is to insert a watermark in such a way that any attempt to alter the content of an image will also alter the watermark itself. Therefore, fragile watermark can be used in all the applications for which no modification on the original content is tolerated. To verify the authenticity of marked image, the watermark is retrieved from the same and is compared with the re-evaluated watermark [1], [5].

Many methods for image authentication have been found in the literature. Image authentication based on set of pseudorandom numbers is proposed in [6]. For the purpose of image recovery, descriptors are needed for the reconstruction of tampered region. A self recovery/embedding block based authentication technique for JPEG image has been described in [5], [7]. Here, an image is divided into non-overlapping blocks. A transformation is applied to every block so as to obtain descriptors which are spatially embedded in distant blocks. Altered blocks are recovered with the help of these block descriptors. A common transformation method employed in the evaluation of descriptor is through the Discrete Cosine Transform (DCT). Performing DCT in an image block, results in a transformed block with one DC coefficient and many AC coefficients. For each block, only a few DCT coefficients have significant amplitude and are embedded in distant blocks, neglecting other coefficients with low amplitude [8]. The image block can be approximately recovered by inverse DCT of embedded coefficients. These coefficients can be used as descriptors. A JPEG compressed

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. 2, Special Issue 1, December 2013

version of each block is inserted into the LSBs of a distant block. The distance of this distant block may be approximately chosen as one-third of image size in any chosen direction.

Different scheme have been proposed for authentication as well as localization of the tampering of images by dividing image in 8×8 block size [8], [9]. By reducing the block size, better localization with respect to alterations can be provided. Further, it reduces the artefacts incurred during process of reconstruction. In this context, an algorithm which provides detection of tampering and recovery in a 4×4 block size is proposed. Method for reconstruction using descriptors based on quantized DCT coefficients is suggested in [10]. Here, the reconstruction is achieved through descriptors which are evaluated by a combined technique employing DWT and DCT based approaches. These descriptor values are stored at distant locations to ensure that the descriptors are intact.

II. PROPOSED SCHEME

A watermarked image is formed from the original image through self-embedding process. It concerns with embedding of digest and descriptor in two least significant bits of each pixel in image. The digest is embedded for authentication and the descriptor for purpose of recovery. Digest is evaluated for each 4×4 sub-block by multiplying each pixel in it by one of the 16 pseudorandom numbers generated from a secret key. An overall schematic diagram for the proposed algorithm is shown in Fig. 1.

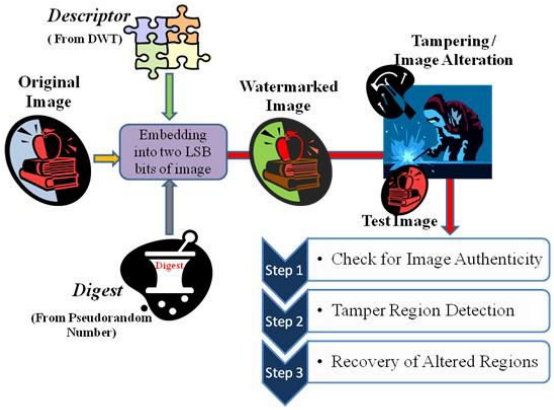

Fig. 1. Overall schematic of proposed watermarking algorithm

Simple method for the generation pseudorandom sequence from an integer is hereby discussed. A 16 bit random binary number is chosen. The binary sequence is rotated/ shifted by one place. This shifted sequence is XOR-ed with the previous sequence. Convert this binary sequence to decimal number. Repeat this to form 16 pseudorandom numbers. The check sum is evaluated by the product of pseudorandom numbers with pixel values of 4×4 sub-block. The sum of these products undergo modulo operation to generate the digest. This is shown in Fig. 2. The storage of digest is shown in Fig. 3. The recovered quality of the tampered regions in the image increases as the number of bits allotted for recovery increase. But, as the number of bits for recovery increase, the quality of watermarked image degrades. Therefore, the embedding is confined within two least significant bits. Due to the limitation in the embedding capacity, it is necessary to apply a transformation so as to have a compressed representation that can reconstruct the original image within the storage size constraint. However, during compression of the image content, it has to be ensured that the recovered image is of acceptable quality, considering the embedding capacity of the original image. Descriptor is evaluated through a series of transformation. DWT transformation of entire image is followed by block based DCT transformation of the LL part of the DWT transformed image and its quantization. Fig. 4 describes the descriptor evaluation and embedding process. The watermarked image can undergo tampering/ alteration to form a test image. The obtained test image undergoes check for authenticity. The altered regions in an unauthentic image are detected and further the recovery of those altered regions is done.

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. 2, Special Issue 1, December 2013

A. Self- Embedding Algorithm for Watermarking

The self-embedding process concerns with embedding of digest and descriptor into two least significant bits of the original image. In the proposed algorithm, all pixels in image will undergo this transformation. The self-embedding steps are as follows:

1) Generate 16 pseudorandom sequences using a secret key.
2) Reset the two least significant bits (LSBs) of the original image to zero.
3) Divide the modified image into blocks of size 8×8 and each 8×8 block into four 4×4 sub-blocks.
4) *Checksum formation*: Based on the 5 most significant bits of each pixel in 4×4 sub-blocks and 16 pseudorandom sequences, evaluate a checksum value corresponding to each sub-block. The block number and image properties, i.e. image dimensions, are also incorporated in evaluation process of checksum.
5) *Digest evaluation for image authentication*: A modulo operation is done with the obtained checksum, so as to limit the digest to 8 bit value. An integer N is chosen such that the digest is always 8 bit long. Choice of N should be such that it is an odd value less than 255.
6) *Storage of digest information:* These digest bits are stored in those 4×4 sub-block where the digest was evaluated as their 7^{th} least significant bit of each pixels. The storage is based on selection of 8 pixels from group of 16 pixels in each 4×4 blocks based on relative average luminance. This will help in checking the authentication of each 4×4 sub-block. Embedding o f digest is shown in Fig. 3.
7) *Descriptor evaluation:* Evaluate the first level DWT transformation for the image to obtain LL, LH, HL, HH components. Choose the entire LL matrix and divide it into four non overlapping parts.
8) Each of one of these four parts of LL is further divided into non-overlapping blocks having 8x8 size.
9) Subtract 128 from each element of the matrix to reduce the dynamic range. Apply DCT transformation to each of these 8x8 blocks.
10) Divide each of these transformed matrices with a constant truncation matrix.
11) Quantize the resulting matrix coefficients and store the coefficients in binary form. Also store mean values of HL, LH, HH to forms the descriptor for one LL part of the image.
12) The descriptor details for each part of LL component is stored at 8^{th} least significant bit (LSB) in pixels, but at complement LL component sections, i.e. part one descriptor details is stored at part four of image and part four descriptor being stored at part one of image.
13) Perform this transform operation on remaining three LL components of the image.

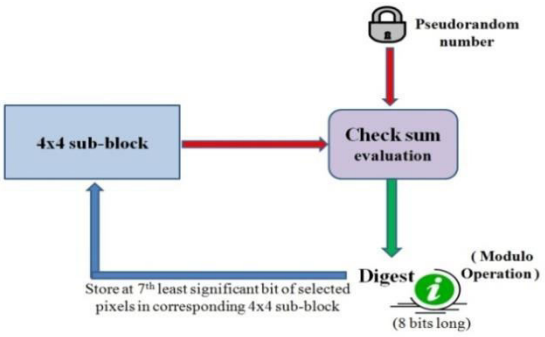

Fig. 2. The digest embedding process.

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. 2, Special Issue 1, December 2013

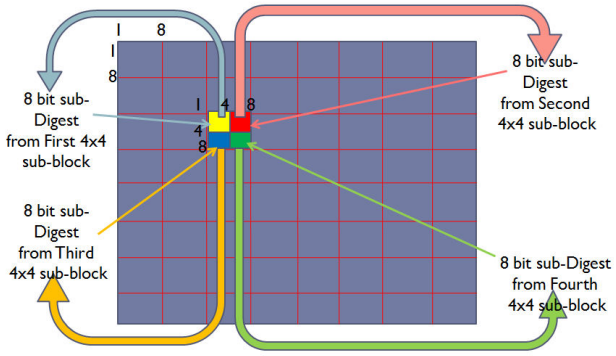

Fig. 3. Overall embedding process of digest.

The embedding of descriptors is shown in Fig. 4 and the formation of digest is shown in Fig. 5.

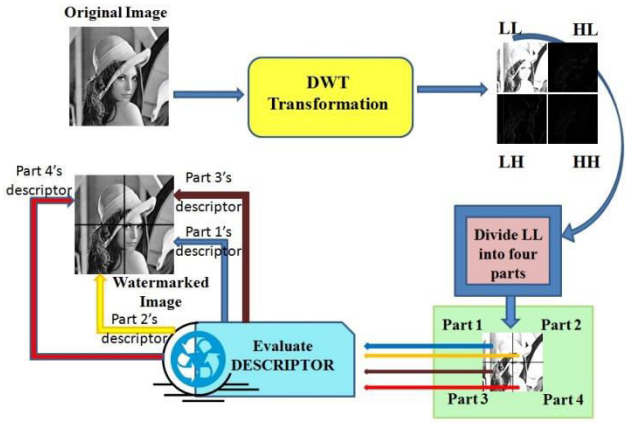

Fig. 4. DWT based descriptor evaluation and its embedding process.

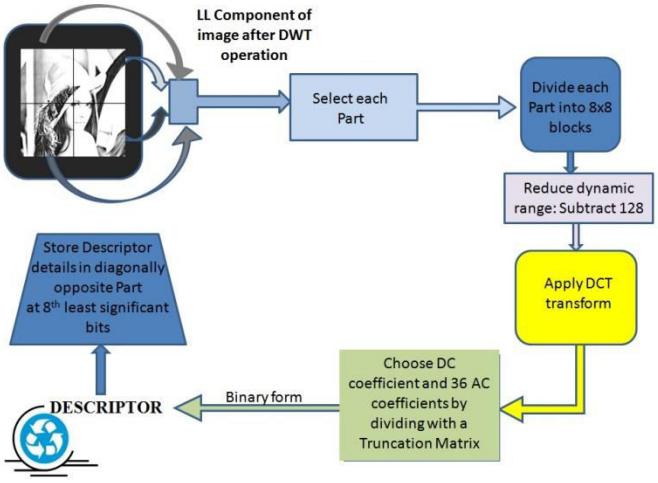

Fig.5. Formation of descriptors for DWT technique

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. 2, Special Issue 1, December 2013

B. Algorithm for Tamper detection and Self-Recovery

Watermark extraction is the inverse process of embedding. The crucial part of recovery process is to precisely locate the tampered regions and to extract the embedded watermark from the remaining image to fill tampering regions. An over view of image authentication detection and recovery is shown in Fig. 6. First the obtained watermarked image is checked for authenticity by comparison between extracted digest and calculated digest. After checking for the authenticity, if the image is found unauthentic, then locate the tampered regions. The tampered regions are detected with an accuracy of 4×4 size. Steps for retrieval are further done using inverse discrete wavelet transform.

The retrieval steps are listed as follows:

1) Upon receiving a test watermarked image, extract the least significant bit information per sub-block from the watermarked image by embedding rules.
2) Detect the tampered sub-blocks by a comparison between the digest embedded in watermarked image and recalculated digest from the watermarked image. Since the authentication is being done in 4x4 block level, precise localization of tampering is possible.
3) From those descriptor details stored in the least significant bits, reconstruct the DWT coefficient *LL* by employing the reverse operations used for embedding, i.e. by multiplying with truncation matrix and calculating inverse discrete cosine transform in 8x8 block size.
4) Add 128 from each element of the matrix to obtain the *LL* component of the image.
5) From the *LL* component, obtain *HL*, *LH*, *HH* by finding the horizontal, vertical and diagonal edges of *LL* and weighing each edge accordingly by its mean value.
6) Evaluate the inverse discrete wavelet transform and replace those regions with the reconstructed regions from the descriptor, where the alterations are detected.

The recovery of tampered regions from the descriptor is done through the inverse process involved to formulate the descriptors. This is shown in Fig. 7.

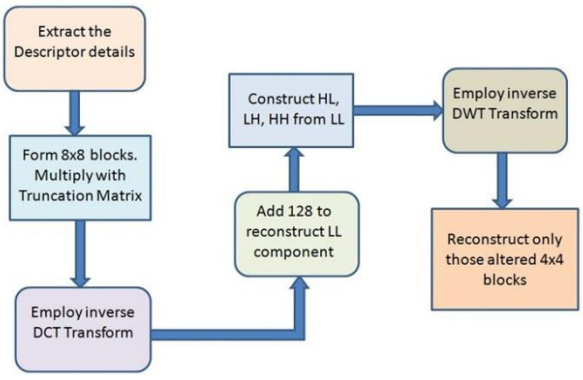

Fig. 7. Recovery process from descriptors

III. EXPERIMENTAL RESULTS AND VERIFICATION

The proposed watermark does not significantly affect the quality of the image. This is visually evident on comparing the original image and the watermarked image which are shown in Fig. 8 (a) and 8 (b) respectively. Since the watermarking is being done in the last two least significant bits, the maximum difference in magnitude of pixel value that occurs between the original and watermarked image is three.

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. 2, Special Issue 1, December 2013

(a) (b)

Fig.8.(a) Original Lena image, (b) Watermarked Lena image.

For evaluating the quantitative degradation of the image introduced by the proposed algorithm, MSE (mean square error) and PSNR (Peak Signal to Noise Ratio) are calculated.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)dB \tag{1}$$

$$MSE = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(\frac{\left(a_{i,j} - b_{i,j}\right)^2}{m \times n}\right) \tag{2}$$

where, $m \times n$ is the image size and $a_{i,j}$ and $b_{i,j}$ are the corresponding pixel values of original and watermarked images. The MSE and PSNR of the watermarked Lena image are calculated and obtained as 0.9705 and 48.2608 respectively. These values are quite reasonable. PSNR value above 35dB is appreciable for watermarked images. Table 1. shows a comparison between the MSE and PSNR of various standard images.

TABLE I
COMPARISON OF MSE AND PSNR FOR VARIOUS IMAGES

Name of Figure	Mean Square Error	PSNR (dB)
Autumn	1.0582	47.8851
Cameraman	0.9933	48.1601
Coins	1.0278	48.0118
Lenna	0.9705	48.2608
Spine	0.6758	49.8324

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. 2, Special Issue 1, December 2013

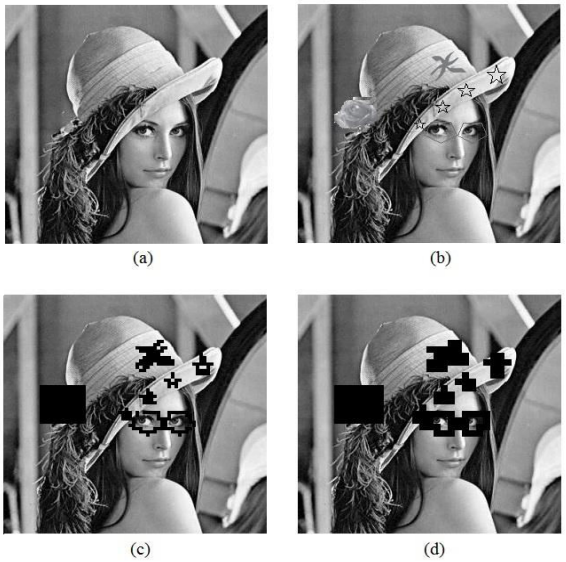

Fig. 9. (a) Watermarked Lena image, (b) Tampered image, (c) Image with tamper region being detected in 4×4 block size , (d) Image with tamper region being detected in 8×8 block size.

Image authentication with a block size of 4×4 is proposed in this paper. Smaller block size results in more localized tamper detection and better reconstruction of the image. Fig. 9 shows comparative results while employing the two different block sizes, 4×4 and 8×8. Watermarked Lena image is shown in Fig. 9 (a). Fig. 9 (b) shows the tampered version of Lena image. Fig. 9 (c) and Fig. 9 (d) show the detection of tampered regions in the image with block size of 4×4 and 8×8 respectively. More accurate detection of tampered region for 4×4 block size is evident by comparing Fig. 9 (c) and 9 (d). Here better localization for tampered regions is obtained in 4x4 based techniques. Better localization helps to reduce the amount of incurred artifacts during reconstruction.

Employing descriptors based on DCT and DWT techniques have varying perceptual performances. Fig. 10 shows the recovered output image based DCT and DWT descriptors.

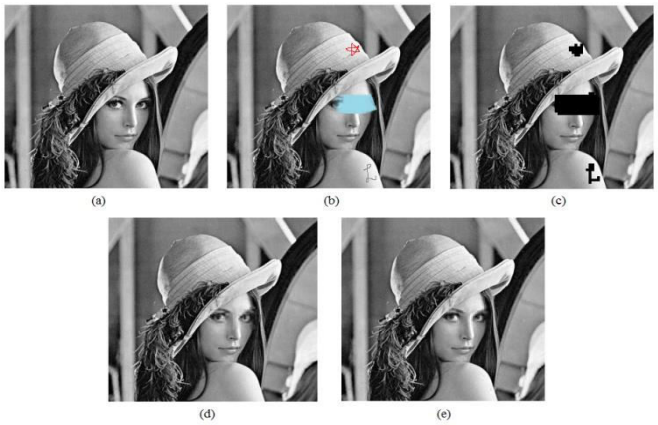

Fig. 10. (a) Watermarked Lena image, (b) Tampered image, (c) Image with tamper region being detected in 4×4 block size , (d) Reconstructed image using DCT based descriptors, (e) Reconstructed image using DWT based descriptors.

The quality of DWT based recovery shows significant improvement over the DCT method. The region near the left eye is poor and blurred in DCT technique, in contrast to DWT technique. DWT method provides better reconstruction

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. 2, Special Issue 1, December 2013

quality for high frequency regions. The reconstructed version of the complete image using the descriptors based on DCT and DWT are shown in Fig. 11. This shows significant improvement in visual perception for DWT based descriptor technique.

(a) DCT descriptor based recovered Lenna image

(b) DWT descriptor based recovered Lenna image

(c) DCT descriptor based recovered cameraman image

(d) DWT descriptor based recovered cameraman image

Fig.11. A comparison of the recovered images based on DCT and DWT based descriptor.

The effectiveness of the proposed technique is verified in cameraman and Lena images and the results are presented. Fig. 12 (b) shows the tampered version of Fig. 12 (a) in which the structure of a building is erased and an aero plane is added. The proposed technique detects the altered regions by comparing the stored digest and the recalculated digest as discussed in section II. Fig. 12 (c) shows the image with the detection of the altered regions, and Fig. 12 (d) shows the altered regions which are reconstructed from the altered image using the descriptors.

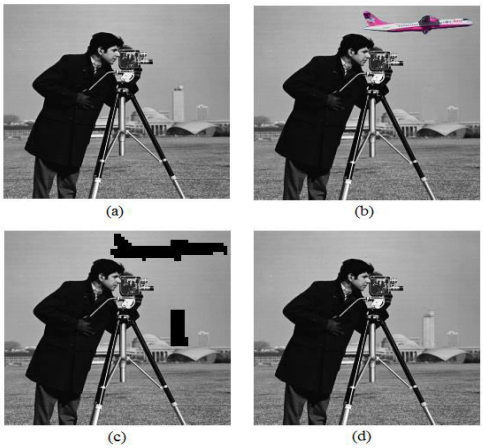

Fig.12. (a) Original image of cameraman, (b) Tampered image, (c) Image with tamper region being detected, (d) Recovered image.

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. 2, Special Issue 1, December 2013

IV. CONCLUSION

A simple but effective algorithm for image tamper detection and self recovery is done. This scheme can detect the alteration/tampering done on the watermarked image with localization in level of 4×4 block size. The advantage of the proposed 4×4 block based algorithm is that, it induces fewer artifacts during the reconstruction than 8×8 block scheme. Utilization of DWT based technique will improve the reconstruction quality in comparison to DCT method. Although the distortion made in large area and tampering done in multiple regions degrade the quality of recovered regions, their detection will never go un-noticed. This algorithm can effectively thwart collage attack.

REFERENCES

[1] Athanasios Zigomitros, Achilleas Papageorgiou, "Social network content management through watermarking", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1381-1386, 2012.
[2] Chun-Shien Lu, Liao, H.-Y.M., "Multipurpose watermarking for image authentication and protection", IEEE Transactions on Image Processing, pp. 579-1592, 2001.
[3] Mirza Hanane, Thai Hien, Nakao Zensho, "Color image watermarking and self-recovery based on independent component analysis", Artificial Intelligence and Soft Computing - ICAISC 2008, 9th International Conference, pp. 839-849, 2008.
[4] J. Fridrich and M. Goljan," Images with self-correction capabilities", Proc. ICIP 99, Japan, pp. 792-796, 1999.
[5] Ammar M. Hassan, Ayoub Al-Hamadi and Yassin M. Y. Hasan, "Secure self-recovery image authentication using randomly-sized blocks", 2010 International Conference on Pattern Recognition, pp.1445- 1448, 2010.
[6] L. Sumalatha, G. Roseline Nesa Kumari, V. Vijaya Kumar, "A simple block based content watermarking scheme for image authentication and tamper detection", International Journal of Soft Computing and Engineering (IJSCE), pp. 113-117, 2012.
[7] M. Hamad Hassan and S.A.M. Gilani, "A semi-fragile watermarking scheme for color image authentication", World Academy of Science, Engineering and Technology, pp. 34-38, 2006.
[8] Christian Rey, Jean Luc Dugelay, "A survey of watermarking algorithms for image authentication", EURASIP Journal on Applied Signal Processing, pp. 613-621, 2002.
[9] Kuo-Ming Hung, Ting-Wen Chen, "Automatic image authentication and recovery using multiple watermarks", Information Science and Digital Content Technology, pp. 730-735, 2012.
[10] Augustus P P, David Solomon George, "Digital Image Authentication and Self-Image Recovery", Proceedings of the 1st National Conference on Systems, Energy & Environment (NCSEE '13), pp. 395- 399, 2013.

BIOGRAPHY

David Solomon George received the B. Tech. degree in Electronics and Communication engineering from NSS College of Engineering, Palakkad, India in 1992 and the M. Tech. in Electronics from the Department of Electronics, Cochin University of Science and Technology, India, in 1999. Since 1991, he has been working as a member of faculty in various Engineering Colleges in Kerala, India. At present he is with Rajiv Gandhi Institute of Technology, Kottayam, India as an Associate Professor in the Department of Electronics and Communication.

Augustus P P received the B. Tech. degree in Electronics and Communication engineering from Adi Shankara Institute of Engineering and Technology, Kalady, India in 2010 and the M. Tech. in Electronics from the Department of Electronics, Rajiv Gandhi Institute of Technology, Kottayam, India, in 2013.