I.J. Image, Graphics and Signal Processing, **2012, 9, 30-36**
Published Online September 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2012.09.05

Local Content Based Image Authentication for Tamper Localization

L. Sumalatha
Associate Professor
Department of Computer Science and Engineering, University College of Engineering
Jawaharlal Nehru Technological University Kakinada
Kakinada, AP, India.
E-mail:sumapriyatham@gmail.com

V. Venkata Krishna
Professor and Principal
Department of Computer Science and Engineering, Chaitanya Institute of Science and Technology
Rajahmundry, AP, India.
E-mail:vakula_krishna@yahoo.co.in

V. Vijaya Kumar
Professor & Dean, Department of Computer Sciences
Head, Srinivasa Ramanujan Research Forum (SRRF)
Godavari Institute of Engineering and Technology
Rajahmundry, A.P. India
E-mail:vijayvakula@yahoo.com

Abstract**—** Digital images make up a large component in the multimedia information. Hence Image authentication has attained a great importance and lead to the development of several image authentication algorithms. This paper proposes a block based watermarking scheme for image authentication based on the edge information extracted from each block. A signature is calculated from each edge block of the image using simple hash function and inserted in the same block. The proposed local edge based content hash (LECH) scheme extracts the original image without any distortion from the marked image after the hidden data have been extracted. It can also detect and localize tampered areas of the watermarked image. Experimental results demonstrate the validity of the proposed scheme.

Index Terms— Image authentication, Simple hash, Tamper Localization

I. INTRODUCTION

Digital multimedia plays a vital role in applications such as broadcast monitoring, gathering of intelligence information, criminal investigation, security, and medical care. This data can be vulnerable to several malicious modifications during its transfer over public network like internet and trustworthiness could no longer be guaranteed. Any tamper to an image could change the decisions based on that image. Recently, digital watermarking techniques have been considered as one of the promising techniques for multimedia authentication. It is the best way to certify the integrity and authenticity of the digital images. It is a complete solution for claiming legitimate usage, authentication of authorized users, and it is also possible to provide extra information along with the digital contents. The transfer of watermarked images can discourage unauthorized copying. This is because the owner can prove his ownership by extracting the watermark using some methods and security keys. Several approaches have been proposed for the image content authentication. These approaches can be classified into strict and selective authentication. Strict Authentication consists of conventional cryptography and fragile watermarking techniques; whereas semi fragile and digital signature based algorithms are classified as selective authentication. Several researches have used these image characteristics for image authentication. Typically the image characteristics include edges, colors or grey levels, histograms, DWT or DCT coefficients, textures , Statistical measurements form the image content. In signature based schemes [1-4], the signature is the hash of image contents or image characteristics computed and encoded via public key cryptosystem or signed value. These mechanisms can detect if an image has been changed; however, they cannot locate where the image was changed. Fragile watermarking schemes [5-10] for tamper proofing/authentication computes a key-dependent function on the local areas of the image and embedded into the corresponding areas. Watermarking techniques are used to dissimulate the signature in the image. Some of the watermarking techniques which used image characteristics for computing image hash and embedded into the transform domain are discussed in this paper. In [11], an approach for still image digital watermarking is proposed in which the watermark embedding process employs the wavelet transform and incorporates Human Visual System (HVS) characteristics. In [12], a block level embedding in Discrete Hartley Transform (DHT) and the Discrete Cosine Transform (DCT) using the edges of the image block as the threshold is proposed. In [13], a feature based watermarking scheme which embeds in the selected subband coefficients of the image transformed by DFT is presented. In [14], a hybrid watermarking algorithm by combining fragile and robust watermarking is proposed. The watermark is a content hash generated from the host image. The watermark is embedded into the DWT Transform of the image. A tradeoff between the length of the hash and tamper localization was exploited and a robust image hashing method in which the hash is calculated from the features of the image is presented in [15]. In authenticating an image using the fragile watermark scheme, the watermark is extracted from the given image to verify its integrity. The local content-based watermark considered usually extracts robust feature point, and then partitions the image into multi-area using the feature point as the centre; finally the watermark is repeatedly embedding into each area. The present paper is organized as follows, Section II discuss the related works. Section III illustrates the watermark embedding and an extraction method, Section IV describes the experimental results and gives a comparison between the proposed method and other existing methods. Conclusions are given in Section V.

II. RELATED WORK

In [5], Walton proposed an authentication scheme using watermarking. A checksum is constructed out of the seven most significant bits of each pixel. The pixels for embedding are chosen pseudo randomly and the checksum bits are embedded in the LSB of the chosen pixel. In [16], Wong proposed a block based watermarking technique. The detailed process is described as follows: The original image is divided into non-overlapping blocks. The LSB's of all the pixels in the block are modified to zero. Then a hash value is computed using the modified block and the image dimensions as given in below:

$$H_i = H(M, N, B_i') \quad (1)$$

Where H is the cryptographic hash function such as MD5, M and N are the image dimensions. The signature of the each block is obtained by XORing the computed hash with the watermark pattern. The signature is encrypted by a public key cryptosystem as given below:

$$C_i = E_K(H_i \oplus W_i) \quad (2)$$

Where C_i is the signature, '⊕' is the XOR operation and E_K is the encryption function. The signature C_i is embedded into the LSBs of the pixels in block Bi.

In the verification process, the watermarked image is divided into non-overlapping blocks and the signature is calculated from the LSB of each pixel of the block. The hash H_i' is computed using (1). The watermark is obtained by decrypting the signature C_i' by

$$W_i' = D_K(H_i' \oplus C_i') \quad (3)$$

where D_K is the decryption function.

In [17], Chang et al. proposed an authentication method based on fragile watermarking. At first the image is divided into 3×3 overlapping blocks. The center pixel of each block is embedded with the cryptographic hash of the features of the corresponding block. The feature of a block consists of the eight neighboring pixels, the index of the block, the height and width of the image and the user's secret key. A cryptographic hash of the feature of the block is calculated using MD5 as given in (4). In figure 1, X represents the center pixel in which the data is embedded. The 8-neighbors of the center pixel are P_1, P_2,.., P_8.

P_3	P_2	P_1
P_4	X	P_8
P_5	P_6	P_7

Figure 1. The embedded pixel X and its eight neighbors

The cryptographic hash of the block is given by,

$$H(B_i) = (P_1 \| P_2 \| \ldots\ldots \| P_8 \| i \| ID \| K_u) \quad (4)$$

where $\|\cdot\|$ is the concatenation operator, B_i is the i^{th} block of the image, 'i' is the block number, ID is the image identity and K_u is the user secret key. The hash of each is obtained, and is embedded into r least significant bits (LSBs) of the pixel X, where $2 \le r \le 4$.

III. PROPOSED METHOD

A. *Embedding*

Step 1: Signature Generation

The proposed LECH authentication scheme generates the signature in the first step. Various low-level visual features (e.g. color, texture, shape, edges) can be extracted from the images. Edge aims at identifying points in a digital image at which the image brightness changes sharply or more formally and has discontinuities. Edge detection process detects and outlines the boundaries between objects and the background in the image. Edge features are useful to overcome the attacks generated by noise, edge strips and acuity. That's why the proposed method evaluates edge features on the entire image. For this the canny edge operator is used. The canny edge detector finds the edges by looking for local maximum of the gradient of unprocessed input image. A simple hash is computed from the edge features of the original image (Let it be called Edge Image). The process of finding hash involves dividing the edge image into 4×4 non overlapping blocks. The present method is a localized method because the hash is basically derived on a local block size 4×4. By dividing the image in to non overlapping blocks, the proposed method achieves high security. This hash is embedded into the corresponding block of the original image. The steps for computing the simple hash of each block are:

Step i: Compute the edge coefficients of the original image by using Canny edge operator.

Step ii: Divide the image with the edge coefficients into non overlapping blocks of size 4×4 pixels.

Step iii: Calculate the simple hash for each block of size m×n as shown below.

b_{11}	b_{12}	b_{13}	b_{14}
b_{21}	b_{22}	b_{23}	b_{24}
b_{31}	b_{32}	b_{33}	b_{34}
b_{41}	b_{42}	b_{43}	b_{44}
h_1	**h_2**	**h_3**	**h_4**

$$h_1 = b_{11} \oplus b_{21} \oplus b_{31} \oplus b_{41}$$
$$h_2 = b_{12} \oplus b_{22} \oplus b_{32} \oplus b_{42}$$
$$h_3 = b_{13} \oplus b_{23} \oplus b_{33} \oplus b_{43}$$
$$h_4 = b_{14} \oplus b_{24} \oplus b_{34} \oplus b_{44}$$

Hash code $H = h_1 h_2 h_3 h_4$.

The Hash code H is called as the content watermark.

Step 2: Secret Data

A 128 bit secret key which is shared with the receiver is used to compute the secret data. The key is replicated to L bits. Here, L is the total length of hash code of all blocks. The proposed LECH method considers a test image of size 256×256, which gives 4096 non overlapping blocks of size 4x4. Each block results in a 4-bit hash code by which length of L is16384 bits (4×4096) can be obtained. By this mechanism the LECH method replicates 128 times to form 16384 bits. The proposed LECH uses a simple XOR operation to combine four bits of the key with four bit hash code of each block in the following way. Let H be the simple hash of all blocks. Let the sequence of watermark bits (B) is $\{b_1 b_2 \ldots b_n\}$, where n =L. The secret data to be embedded into each block is calculated by the proposed LECH by (5).

$$S = b_1 \oplus h_1 \; b_2 \oplus h_2 \; b_3 \oplus h_3 \; b_3 \oplus h_3 \tag{5}$$

Step 3: Pixel Prediction Technique

In the third step the pixel locations are identified for inserting the data. The entire mechanism is explained below:

Using the JPEG-LS prediction technique [18] the local texture among three pixels can be analyzed. As shown in figure 2 the predictive pattern predicts pixel X from its three adjacent pixels P_c, P_a and P_b. The pixel X is tested whether it belongs to a horizontal edge or vertical edge or neither is performed. A vertical edge exists if $P_c \geq \max(P_a, P_b)$ and $\max(P_a, P_b) = P_a$; namely, the predictive value X' equals P_b. Otherwise, there is a horizontal edge, and the predictive value X' is equal to P_a such that $P_c \geq \max(P_a, P_b)$ and $\max(P_a, P_b) = P_b$. Similarly, in case that the predictive value X'equals to either P_a or P_b when $P_c \leq \min(P_a, P_b)$, there is a vertical or horizontal edge. However, when the pixel value P_c falls in neither the maximum nor the minimum value interval, then it indicates a non formation of an edge.

P_c	P_b	
P_a	X	

Figure 2. JPEG-LS prediction

By applying JPEG-LS prediction for X, its predictive value X' is computed by (6),

$$X' = \begin{cases} \min(P_a, P_b) & \text{if } P_c \geq \max(P_a, P_b) \\ \max(P_a, P_b) & \text{if } P_c \leq \min(P_a, P_b) \\ P_a + P_b - P_c & \text{otherwise} \end{cases} \tag{6}$$

The present paper considers the embedding pixel based on the JPEG-LS prediction technique. The pixels in a block are scanned in rastar scan order. The decision to find a pixel for embedding is based on the variance of its three neighboring pixels. The three neighboring pixels can be any one of the eight occurrences of figure 3. This occurrence is based on the variance of the three neighboring pixels. If the variance falls within a predefined threshold, then the corresponding pixel is selected for embedding. This process is continued in the entire block for finding the embedding pixel.

(a)

P_c	P_b	
P_a	X	

(b)

	P_b	P_c
	X	P_a

(c)

P_b	X	
P_c	P_a	

(d)

	X	P_b
	P_a	P_c

(e)

	P_c	
P_a	X	P_b

(f)

P_b	X	P_a
	P_c	

(g)

	P_b	
Pc	X	
	P_a	

(h)

	P_b	
	X	P_c
	P_a	

Figure 3. (a),(b),(c),(d),(e),(f),(g) and (h) are the patterns of finding embedding pixels in a 3x3 block.

Step 4: Embedding

The embedding mechanism of secret data is derived in the fourth step. For this the proposed LECH computes the difference value d_i between the selected pixel and the predicted pixel by (7) and (8)

$$d_i = P_S - P_s' . \tag{7}$$

Embed a bit b into the difference d_i as,

$$d_i' = 2 * d_i + b . \tag{8}$$

Using (9), the watermarked pixel is obtained,

$$P_s'' = P_s' + d_i' \tag{9}$$

B. Extraction

The steps needed to perform for extracting the secret data from the watermarked image and to recover the original pixel from the cover image is described as follows.

Step 1:The watermarked image is divided into 4x4 non overlapping blocks. In each block, the stego pixel P_s'' is found from the variance of the three neighboring pixels.

Step 2:compute the difference by $d_i' = P_s' - P_s''$. The watermark bit is computed by $b = d_i' \bmod 2$. To get the content watermark the extracted bits are XORed with the secret key. The original difference value $d_i = \left\lfloor \frac{d_i'}{2} \right\rfloor$.

Step 3: Extract the original pixel by

$$P_S = P_S'' + d_i \qquad (10)$$

Thus, an exact copy of the original pixel is obtained.

C. Tamper Detection and Localization

The proposed LECH method can be used to detect the tampered locations. The tampered locations are found by the following algorithm.

Algorithm: Tamper detection and localization by the proposed LECH method.

Begin

Step 1. From the recovered image, find the edge coefficients (edge image).

Step 2. Divide the edge image into 4×4 blocks.

Step 3. Find the simple hash of each block. Compute the secret data as per (5). Fold the secret data into one bit (w).

Step 4. Compare w with the extracted watermark bit b.

$$\text{The block} = \begin{cases} \text{Authentic} & \text{if } w = b \\ \text{Tampered} & \text{otherwise} \end{cases}$$

End

IV. EXPERIMENTAL RESULTS

The present paper displayed eight original images of resolution 512x512 as shown in figure.4, to evaluate and compare the performance. Figure 5 shows the resultant watermarked images. To test the efficacy of the proposed LECH method, PSNR and NCC values are evaluated. The larger the PSNR value, the higher the image quality. This is due the fact that stego image is inverted to its original image after the data extraction, and the embedding capacity is increased to a significant factor when the visual quality of the stego image does not decline to an unacceptable degree, e.g., PSNR>30 dB. The Peak Signal to Noise Ratio (PSNR) in decibel (dB) between the original image (I) and its watermarked version image (W) is expressed by (11) and (12)

$$\text{PSNR (I, W)} = 10 * \text{Log10} [(2552/ \text{MSE}] \qquad (11)$$

$$\text{Mean Square Error (MSE)} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(I(i,j) - W(i,j)\right)^2 \qquad (12)$$

Where I (i, j) is the original image and W (i, j) is the watermarked image.

To verify the robustness of the digital watermarking method, Normalized Cross Correlation (NCC) is used, which is defined by (13).

$$\text{NCC}= \sum_{i=0}^{N-1} W(i) \times W'(i) \,/\, \sum_{i=0}^{N-1} W(i) \times W(i) \qquad (13)$$

where W(i) is the original watermark and W′(i) is the extracted watermark.

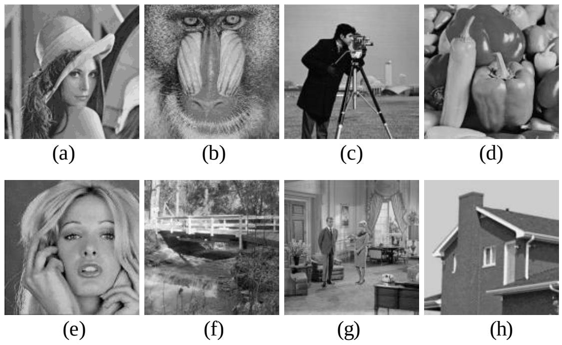


Figure 4. Test Images- a) Lena, b)Baboon, c)Cameraman, d)Peppers, e)Tiffany, f)Walk bridge, g)Living room, h)House.

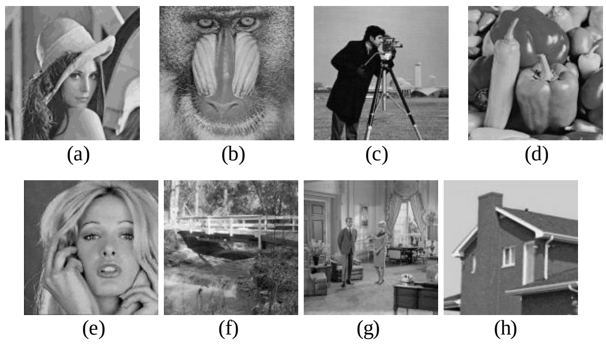


Figure 5. Watermarked Images- a)Lena, b)Baboon, c)Cameraman, d)Peppers, e)Tiffany, f)Walk bridge, g)Living room, h)House.

Table I shows the performance results of the proposed LECH scheme on eight test images. The results show that the PSNR values are high for the proposed LECH method. Higher value of PSNR and NCC indicates good embedding quality and imperceptibility. Based on the simulation results, the quality of every embedded image is observed to be greater than 47 dB for all original images. As a result, the difference between the original and embedded images is unnoticeable in vision.

TABLE I. THE PERFORMANCE OF THE PROPOSED LECH SCHEME ON EIGHT TEST IMAGES.

Quality Factors	Lena	Baboon	Camera man	Peppers
PSNR(dB)	48.30	48.57	48.36	48.33
NCC	1.0	1.0	1.0	1.0

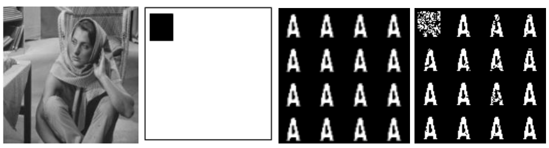
Quality Factors	Tiffany	Walk Bridge	Living room	House
PSNR(dB)	48.37	48.57	48.42	48.35
NCC	1.0	1.0	1.0	1.0

The proposed LECH method is compared with some of the existing fragile watermarking schemes for image authentication. Table II. Shows a comparison of the proposed LECH method with other methods presented in [19]-[22]. Table II gives the average of the PSNR values of these methods applied on several test images. It can be seen that the proposed LECH method yields better performance than the other competing schemes in terms of PSNR and the tamper detection rate is close 100%. The reason is that the LECH scheme embeds the block hash in to the same block. Further the hash is computed with the edges of the corresponding to that block. Hence if any pixel is changed it results in a wrong hash and hence the block can be identified as tampered.

TABLE II. A COMPARISON BETWEEN THE PROPOSED LECH SCHEME AND OTHER METHODS.

Method	Block Size	Payload (bits)	PSNR (dB)	Missing rate of Tampering
X. T. Zeng et al.[19]	8×8	4096	38.60	0.37%
Z.C. Ni et al. [20]	8×8	729	40.10	NA
X. Zhang et al. [21]	8×8	131012	37.9	0.13%
P. L. Lin et al.[22]	4×4	131072	44.37	0.39%
Proposed LECH Scheme	4×4	4096	48.93	0.10%

For tamper detection a region of pixel intensities in the watermarked image is tampered and replaced with the pixel intensities same as in the original image. The Algorithm Tamper detection and localization by the proposed LECH method is used to find the tampered locations. The extracted watermark clearly shows the tampered region. This attack, called copy attack is shown in figure 6. According to the simulation results, the positions of the tampered areas are marked correctly. For more applications, our proposed image authentication scheme also can be extended to dealing with color images and compressed images using similar methods in different domains, even though it is for grayscale and uncompressed images in the spatial domain. The proposed method can detect any tampering of size 4×4 pixels with a missing rate less than 0.10%.



(a) (b) (c) (d)

Figure 6. Watermarked Image b) Tampered Region c) Binary Logo d) Extracted Logo with tampered region.

V. CONCLUSIONS

This paper proposed an efficient image authentication method LECH by embedding the content of the image into itself. The present study found that edges are relatively a good choice for image content authentication and hence the hash of the edge image block is computed and embedded into the corresponding block itself. With this the tampered blocks can be identified and localized. Further the proposed LECH method uses reversible data hiding scheme that makes use of the JPEG-LS predictive technique to predict the pixels for embedding. Unlike the LSB embedding technique which can be removed easily, LECH method used the Difference expansion method to embed bit of information into the predicted pixel. This improves the stego-image quality. Hence the experimental results show that the performance of the proposed scheme is better than those of some well-accepted schemes in terms of payload and stego-image quality and successfully identifies the tampering of the image content. It also accurately localizes maliciously tampered regions. Thus it can be concluded that this scheme is more fragile to malicious distortions.

ACKNOWLEDGMENT

The authors wish to thank anonymous referees for their constructive comments. The authors express their deep sense of gratitude to Honorable Vice Chancellor, Dr. G. Tulasi Ram Das for encouraging research and development. Also the authors would like to express their sincere thanks to Dr. E.V. Prasad, Registrar, JNTUK and Dr. J.V.R. Murthy, Professor of CSE and Chairman Board of Studies for their precious suggestions in refining the present study. Also the authors would like to express their gratitude to Sri K.V.V. Satyanarayana Raju, Founder & Chairman, and Sri K. Sasi Kiran Varma, Managing Director, Chaitanya group of Institutions for providing necessary Infrastructure.

REFERENCES

[1] D.C. Lou, J.L. Liu.Fault resilient and compression tolerant digital signature for image authentication. IEEE Transactions on Consumer Electronics 2000, 46 (1): 31–39.

[2] L. Xie, G.R. Arce, R.F. Graveman. Approximate image message authentication codes, IEEE Transactions on Multimedia, 2001, 3 (2) : 242–252.

[3] P.Y. Tsai, Y.C. Hu, C.C. Chang, A novel image authentication scheme based on quadtree segmentation, Imaging Science Journal 2005, 53 (3):149–162.

[4] C.S. Chan, C.C. Chang, An efficient image authentication method based on Hamming code, Pattern Recognition 2007,40: 681–691.

[5] S.Walton. Information Authentication for a slippery new age. Dr.Dobbs J. 1995. 20(4):18-26.

[6] P.W. Wong, N. Memon. Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Transactions on Image Processing 2001, 10 (10): 1593–1601.

[7] W.N. Lie, G.S. Lin, S.L. Chen.Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques. IEEE Transactions on Information Forensics and Security 2006, 1 (3): 330–341.

[8] T.Y. Lee, S.D. Lin. Dual watermark for image tamper detection and recovery. Pattern Recognition 2008, 41 (11) : 3497–3506.

[9] J.C. Patra, J.E. Phua, C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digital Signal Processing ,2010, 20 (6): 1597–1611.

[10] F. Ahmed, NM.Y. Siyal. A secure and robust hash-based scheme for image authentication. Signal Processing , 2010, 90 (5): 1456–1470.

[11] John N. Ellinas, Dimitrios E. Manolakis. A Robust Wavelet-based Watermarking Algorithm Using Edge Detection. Proceedings of World Academy of Science, Engineering and Technology. 2007, 25: 438-443.

[12] S.S. Bedi, G. S. Tomar, Shekhar Verma. Robust Watermarking of Image in the Transform Domain using Edge Detection, IEEE UKSim 2009: 11th International Conference on Computer Modelling and Simulation,2009

[13] Wei Lu, Hongtao Lu, Fu-Lai Chung. Feature based robust watermarking using image normalization. Computers and Electrical Engineering 2010, 36: 2–18

[14] Jeremy Thurgood, Roger Peplow. A Digital Watermarking Algorithm for Authentication and Tamper Detection. Proceedings, Prasa 2005, 05-09

[15] Sujoy Roy, Qibin Sun. Robust hash for detecting and localizing image tampering. Proc. IEEE International Conference on Image Processing, Sep 2007.

[16] P.W. Wong. A public key watermark for image verification and authentication, Proceedings of ICIP, Chicago. 1998: 425-429.

[17] Chin-Chen Chang , Yih-Shin Hu, Tzu-Chuen Lu. A watermarking-based image ownership and tampering authentication scheme. Pattern Recognition Letters , 2006, 27: 439–446

[18] ISOiIEC JTC 29/WG1 FCD 14495 public draft, 1997. JPEG-LS: Lossless and Nearlossless Coding of Continuous-Tone Still Images.

[19] Xian-TingZeng ,Ling-DiPing , Xue-ZengPan. A lossless robust data hiding scheme, Pattern Recognition 43 (2010) 1656–1667

[20] Z.C. Ni, Y.Q. Shi, N. Ansari, W. Su, Q.B. Sun, X. Lin. Robust lossless image data hiding designed for semi-fragile image authentication, IEEE Transactions on Circuits and Systems for Video Technology 18 (4) (2008) 497–509.

[21] Xinpeng Zhang, Shuozhong Wang. Fragile watermarking scheme using a hierarchical mechanism. Signal Processing, Apr. 2009, 89(4):675–679.

[22] Phen Lan Lin, Chung-Kai Hsieh, Po-Whei Huang. A hierarchical digital watermarking method for image tamper detection and recovery, Pattern Recognition 38 (2005) 2519 – 2529.

AUTHOR'S PROFILE

L.Sumalatha recieved her B.Tech from Acharya Nagarjuna University, Guntur in the year 2000 and M.Tech(CSE) from JNT University, Hyderabad in the year 2004. At present she is working as Associate Professor in Dept of Computer Science and Engineering, University College of Engineering, JNTUK, Kakinada. She is having teaching experience of about 12years and taught many courses to UG and PG Students. She is pursuing her Ph. D from JNT University Kakinada. Her research areas includes Information Security and Digital image Processing.

Dr.V.Venkata Krishna received B.Tech. (ECE) degree from Sri Venkateswara University. He completed his M. Tech. (Computer Science) from JNT University. He received his Ph.D in Computer Science from JNT University in 2004. He worked as Professor and Head for ten years in Mahatma Gandhi Institute of Technology, Hyderabad. Later he worked as a principal at VVCE, Hyderabad and CIST Kakinada. Presently he is working as Principal for Chaitanya Institute of Engineering and Technology, Rajahmundry. He is an advisory member for many Engineering colleges. He has published 30 research articles. Presently he is guiding 10 research scholars. He is a life member of ISTE and CSI.

Dr. V.Vijaya Kumar received integrated M.S.Engg, degree from Tashkent Polytechnic Institute (USSR) in 1989. He received his Ph.D. degree in Computer Science from Jawaharlal Nehru Technological University (JNTU) in 1998. He has served the JNT University for 13 years as Assistant Professor and Associate Professor and taught courses for M.Tech students. He has been Dean for Dept of CSE and IT at Godavari Institute of Engineering and Technology since April, 2007.His research interests include Image Processing, Pattern Recognition, Network Security and Steganography, Digital Watermarking, and Image retrieval. He is a life member for CSI, ISTE, IE, IRS, ACS and CS. He has published more than 120 research publications in various National, Inter National conferences, proceedings and Journals.

