# Image Content Authentication based on Wavelet Edge Features

L. Sumalatha
Associate Professor
Dept.of CSE
University College of Engg.,JNTUK,Kakinada

V. Venkata Krishna
Phd,Professor & Principal
Dept.of CSE
CIET,Rajahmundry

A. Vinay Babu
Phd,Professor & Principal
Dept.of CSE
JNTU College of Engg.,JNTUH,HYdrabed

## ABSTRACT

Reversible image authentication has drawn a great attention for its ability to recover the original image from the watermarked image. The primary concern of authentication is to prevent from unauthorized manipulation of the image and hence has attained good importance. This paper proposes a block based reversible watermarking scheme for image authentication based on histogram modification of the differences between adjacent coefficients using DWT. A content watermark is computed from the image wavelet edge features (WEF) and is inserted into the vertical (LH) subband in a reversible manner. The proposed scheme restores the original image without any distortion from the marked image after the hidden data have been extracted. Also can detect and localize tampered areas of the watermarked image. Experimental results demonstrate the performance of the proposed scheme.

## Keywords

Image authentication, Reversible data hiding, Simple hash, Tamper detection.

## 1. INTRODUCTION

Image authentication has gained a considerable attention due to the increasing requirement of transmitting the images over unsecured channels such as the internet. For multimedia applications like military, medical and quality control, authenticity and integrity of the image is the prime concern. This is because of the importance of the content that resides in the image. Any tamper to such an image could change the decisions based on that image. 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 researchers 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. Schneider and Chang [1] computed a content signature from the image histogram. However, this approach resulted in a long signature and a required a long computational time. The histogram approach is robust against compression of small rates only and the image content may be altered unnoticeably without changing the image histogram. Image edges give relatively good information about the image content because they allow the identification of the object structures. Queluz [2] method obtains a binary image describing the pixels with or without edges. The gradient is computed in each pixel using Sobel operator. Unfortunately, the algorithm is not able to reconstruct the damaged data. Similarly, Dittman J. & Steimatez A. [3] has proposed a method based on determining the image edges and transforming them into a characteristic code to generate the image content signature. Techniques that compute separate hashes for each line and each column of an image lines and columns are known as line column functions [4]. These hashes are stored and compared afterwards find changes. If any change in the hashes is found, the image is declared manipulated otherwise it is declared authentic. Storck [5] proposed characteristic extraction in DCT domain. The selected coefficients were encoded with MD5 hash function. Alternatively the DWT has been successfully used in various image processing applications including filtering, multi resolution analysis and image compression. Yu and Hu [6] applied Sobel operator to the coefficients of three level Haar DWT of the original image to obtain binary Sobel edge map. Later MD5 hash function is applied to get the signature. Lou and Liu [7] proposed a method for generating a signature on image statistics. Tzeng and Tsai [8] proposed a method to generate an image digital signature using both edges and statistical characteristics.

In fact the signatures computed in the above methods needs to be attached or dissimulated in the image in order to verify its authenticity later. Watermarking techniques are used to dissimulate the signature in the image. Some of the watermarking techniques which used edges as image content for computing image hash and embedded into the transform domain are discussed in this paper. Ellinas et al. [9] proposed an approach for still image digital watermarking in which the watermark embedding process employs the wavelet transform and incorporates Human Visual System (HVS) characteristics as hash. Bedi et al. [10] has done block level embedding in Discrete Hartley Transform (DHT) and the Discrete Cosine Transform (DCT) using the edges of the image block as the threshold. Lu et al. [11] presented a feature based watermarking scheme which embeds in the selected subband coefficients of the image transformed by DFT. Thurgood et al. [12] presented a hybrid watermarking algorithm by combining fragile and robust watermarking. The watermark is a content hash generated from the host image. The watermark is embedded into the DWT Transform of the image. Roy et al. [13] exploited the tradeoff between the length of the hash and tamper localization and presented a robust image hashing method in which the hash is calculated from the features of the image. Recently, several reversible data hiding techniques have also been designed which used the image characteristics as medium for embedding authentication data into the image reversibly. Reversible data hiding is one of the fragile watermarking techniques that allow embedding (hide) data inside an image and later the hidden data can be retrieved as required and the exact copy of the original image is found. There are different ways to embed reversibly in literature. Ni et al. [14] used a pair of peak/zero points to embed the data for which image histogram is shifted to create extra space. De

Vleeschouwer et al. [15] proposed a circular histogram scheme and used a relative position of the center of mass of the zone-based histogram to convey the information bits. Lee et al [16] proposed a reversible image authentication method that embeds the hash of the image in the histogram of the difference image. However the histogram shifting technique does not work well when the image has an equal histogram. To overcome this drawback the present paper proposed block based fuzzy approach for embedding the signature that is computed from edges of the approximation (LL) subband of the transformed image in to the vertical (LH) subband. In the vertical subband, the differences between the adjacent coefficients generate a difference histogram and multiple peak points of the histogram are selected based on threshold can be used for embedding. The threshold value has to be transmitted to the recipient via a side channel to ensure successful restoration. The embedding method used in the present paper is adopted from Tai et al. [21] method. The present paper consists of 4 sections. Section 2 describes the proposed method. In Section 3, the experimental results are shown. Section 4 concludes the present study.

# 2. PROPOSED WAVELET EDGE FEATURE CONTENT WATERMARK (WEF-CW) METHOD

## 2.1 Watermark Embedding

The embedding method involves the computation of 7 steps. The process of embedding is shown Fig 2.

**Step 1:** Discrete Wavelet Transform

Apply the 1- level Haar wavelet transform with lifting scheme on the input image of resolution M × N.

**Step 2:** Content Watermark Generation

Image edges give good information about the image content because they allow the identification of the object structures. This is the reason the present paper evaluated edge information as the image content in the second step. Edge detection is a fundamental tool used in most of the image processing applications to obtain information from the images as a precursor step to feature extraction. The present study found that edges are relatively a good choice for image content authentication. Based on this assumption the present paper evaluates the edge information on the LL subband of the transformed image of step one for the following reasons. i) Edge detects and outlines boundaries between objects and the background in the image. ii) Edges form boundaries between the different textures. iii) Edge reveals the discontinuities in image intensity from one pixel to another.

The step 2 evaluates the edges by using canny edge operator on the LL subband because it provides better edge information with an advantage of being less sensitive to noise.

**Step 3:** Simple Hash Function

To be more resistant to attacks a hash value is evaluated in the third step, on the edge information of LL subband of the second step in the following way.

- The edge image is divided into non-overlapping blocks of size 4×4 pixels.
- From each block, a simple hash of 4-bits is calculated as shown in Figure 1.

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

$h_1 = b_{11} \oplus b_{21} \oplus b_{31} \oplus b_{41}$

$h_2 = b_{12} \oplus b_{22} \oplus b_{32} \oplus b_{42}$

$h_3 = b_{13} \oplus b_{23} \oplus b_{33} \oplus b_{43}$

$h_4 = b_{14} \oplus b_{24} \oplus b_{34} \oplus b_{44}$

**Fig 1: Simple hash function**

Hash code, H = $h_1h_2h_3h_4$. Likewise the hash code of all the blocks is computed and concatenated to form a binary sequence which is called the content watermark.

**Step 4:** Adjacent Coefficient Difference (ACD)

In step 4, ACD is evaluated. For this the LH sub band of step 1 is divided into non overlapping blocks of size 4x4. A series of transformed coefficients $P_1$, $P_2$, $P_3$,…, $P_k$ are be obtained, by traversing the entire sub-band in inverse S-order block by block. The ACD on the entire sub band is evaluated by considering the sequence of adjacent coefficient differences in the same inverse S-order, by travelling block by block. The Inverse S order is considered to compute k-1 ACD's. The ACD's are denoted as $d_1$, $d_2$, $d_3$,…,$d_{k-1}$ and evaluated based on Equation 1.

$$d_i = \begin{cases} P_i & \text{if } i = 0 \\ |\, P_{i-1} - P_i|, & \text{otherwise} \end{cases} \quad \text{where } 1 \le i < k. \qquad (1)$$

**Step 5:** Histogram Shifting

In the fifth step a difference histogram is generated based on ACD computed in Step 3. The peak point in the histogram indicates the frequency of occurrence of the corresponding ACD value. Here in this paper multiple peaks are used for embedding. Hence the histogram bins are adjusted by a fuzzy logical expression as given in equation (2) to create free space for data embedding. For this purpose a threshold τ value is used which is a non negative number and the threshold is raised to the power of 2 subjected to a maximum value of 5. If the number of coefficients selected for embedding increase by powers of 2 then more number of coefficients introduce distortion in the image. The coefficients are shifted by $2^{\tau}$ which *is* given by

$$P'_i = \begin{cases} P_i & \text{if } i = 0 \\ P_i + 2^{\tau} & \text{if } d_i > 2^{\tau} \text{ and } P_i \ge P_{i-1} \\ P_i - 2^{\tau} & \text{if } d_i > 2^{\tau} \text{ and } P_i < P_{i-1} \end{cases} \qquad (2)$$

**Step 6:** Embedding

The coefficients with the maximum occurrences are considered for embedding the content watermark in step six. The number of coefficients used for embedding is based on the threshold τ discussed in the previous step. From the difference calculated form step 4, the message is embedded into the selected LH coefficient as,

$$P'_i = \begin{cases} P_i + (d_i + b), \text{ if } P_i \ge P_{i-1} \text{ and } di < 2^{\tau} \\ P_i - (d_i + b), \text{ if } P_i < P_{i-1} \text{ and } di < 2^{\tau} \end{cases} \qquad (3)$$

Where b is one bit of the content watermark, b is {0, 1}.

The binary logo is embedded into HH component by,

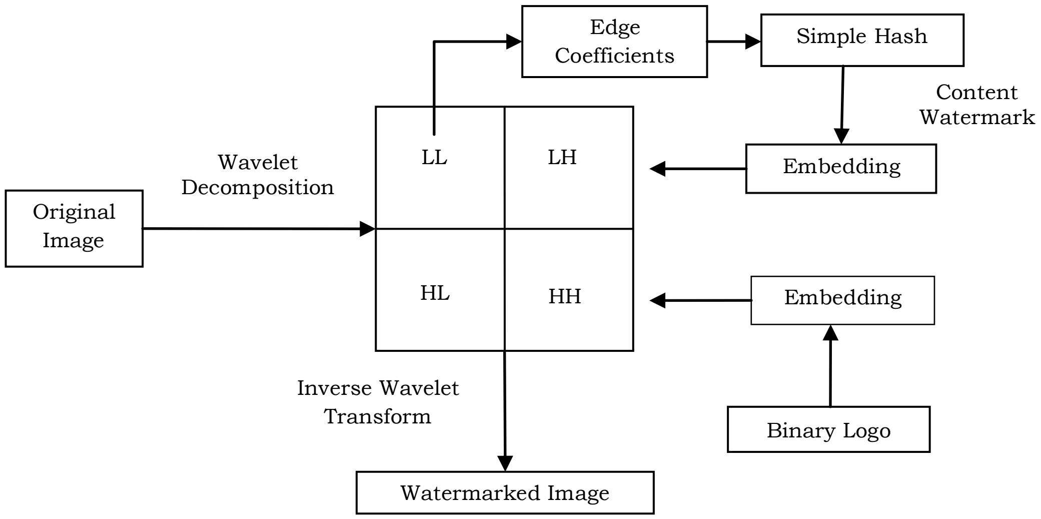


**Fig 2: Block diagram of embedding watermark**

- Finding the sum (S) of the LL, LH, HL and HH components.
- Modify the coefficient of HH by the watermark bit by,

$$P_i = \begin{cases} P_i + 1 & \text{if } b = 1 \text{ and mod } (S,2) = 1 \\ P_i & \text{Otherwise} \end{cases} \qquad (4)$$

**Step 7:** Watermarked Image

In step 7, the inverse wavelet transform is performed to reconstruct the watermarked image.

## 2.2 Watermark Extraction

Let τ be the threshold. For an M-pixel 8-bit watermarked image W with a pixel value $P'_i$, where $P'_i$ denotes the grayscale value of the *i*th pixel, $0 \leq i \leq M - 1$, $P'_i \epsilon$ 0, 255.

**Step 1:** Perform 1-level Haar wavelet transform using lifting scheme on the original image and acquire the LL, LH, HL and HH components.

**Step 2:** Divide the LH in to 4×4 non overlapping blocks. Scan each block in inverse S order, Find the adjacent coefficient difference.

**Step 3:** If $| P'_i – P'_{i-1} | < 2^{\tau} +1$, extract message bit $b_1$ by

$$b_1 = \begin{cases} 0, & \text{if } | P'_i - P'_{i-1}| \text{ is even} \\ 1, & \text{if } |P'_i - P'_{i-1}| \text{ is odd} \end{cases} \qquad (5)$$

where $P'_{i-1}$ denotes the restored value of $P_{i-1}$. The extracted message bits from the content watermark.

3) The first pixel is not modified and can be used as reference pixel. The remaining pixels can be restored by

$$P_i = \begin{cases} P_i + \delta & \text{if } |P_i - P'_{i-1}| < 2^{T+1} \text{ and } P_i < P'_{i-1} \\ P_i - \delta & \text{if } |P_i - P'_{i-1}| < 2^{T+1} \text{ and } P_i > P'_{i-1} \end{cases} \qquad (6)$$

$$\text{Where } \delta = \left\lceil \frac{| P'_i - P'_{i-1} |}{2} \right\rceil$$

The pixel $P_i$ is shifted by $2^{\tau}$ units if $|P_i\text{-}P'_{i-1}| > 2^{\tau+1}$. Thus, an exact copy of the original coefficient can be obtained.

**Step 4:** From the HH component extract the binary logo by

- Find the sum(S) of the LL, LH, HL and HH components.
- Message $b_2 = \begin{cases} 0 & \text{if mod}(S,2) = 1 \\ 1 & \text{otherwise} \end{cases}$ (7)

## 3. EXPERIMENTAL RESULTS

The present paper displayed eight original images of resolution 512×512 as shown in Figure 3, to evaluate and compare the performance. Figure 4 shows the resultant watermarked images. To test the efficacy of the proposed WEF-CW 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 the Equation (8) and (9)

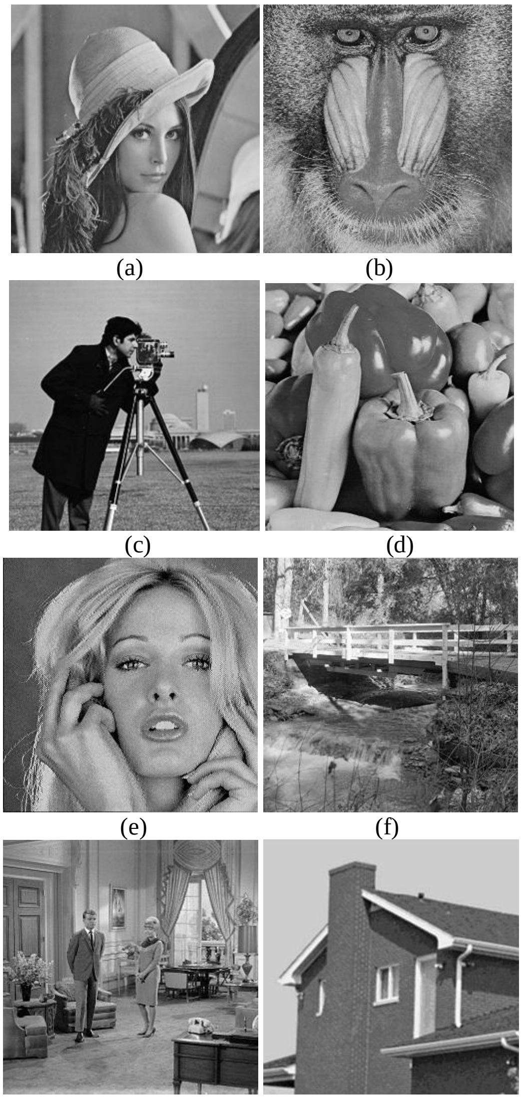
$$\text{PSNR (I, W)} = 10 * \text{Log}_{10} [(255^2/ \text{MSE} ] \qquad (8)$$

$$\text{MSE} = \frac{1}{\text{M x N}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(I(i,j) - W(i,j)\right)^2 \qquad (9)$$

Where I(i,j) is the original image and W(i,j) is the watermarked image. To verify the robustness of any digital watermarking method, Normalized Cross Correlation (NCC) is used, which is defined by the Equation (10).

$$\text{NCC} = \sum_{i=0}^{N-1} W(i) \text{ x } W'(i) / \sum_{i=0}^{N-1} W(i) \times W(i) \qquad (10)$$

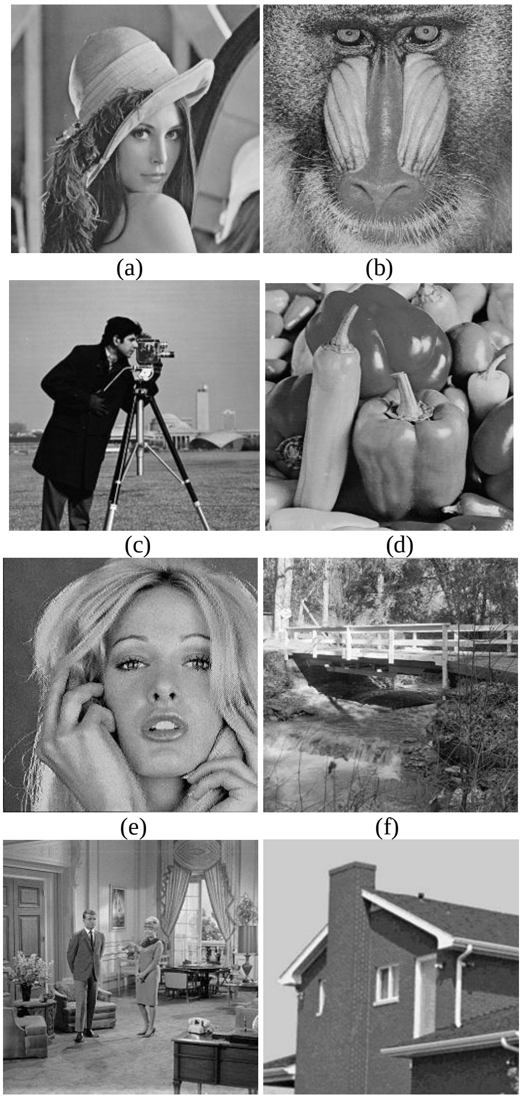
where W(i) is the original watermark and W′(i) is the extracted watermark.



(a) (b) (c) (d) (e) (f) (g) (h)

**Fig 3: Original images (a) Lena (b) Baboon (c) Cameraman (d) Peppers (e) Tiffany (f) Walkbridge (g) Livingroom (h) House**

Table 1 shows the PSNR and NCC values of the proposed WEF-CW method on eight test images. The results of table 1 indicate good embedding quality and imperceptibility. The content watermark is of 4096 bits. The difference values obtained in step 4 and their frequency of occurrence is obtained from the difference histogram. To embed the content watermark the number of difference values that have to be used is based on threshold τ, which is raised to the power of 2 i,e. $\tau=2$, $2^{\tau}=2^{2}=4$. That means, a maximum of 4 difference values which are the peak points in the difference histogram are used for embedding the content watermark. From Figure 4 it is clearly seen that there is no visual difference between the original and watermarked images and hence the imperceptibility condition is satisfied.



(a) (b) (c) (d) (e) (f) (g) (h)

**Fig 4: Original images (a) Lena (b) Baboon (c) Cameraman (d) Peppers (e) Tiffany (f) Walk bridge (g) Living room (h) House**

**Table 1: Performance of the WEF-CW method on Eight Original Images**

| Original images | WEF-CW Method | |
|---|---|---|
| | PSNR(dB) | NCC |
| Lena | 46.042 | 0.99 |
| Baboon | 45.526 | 1 |
| Camera man | 45.526 | 0.98 |
| Peppers | 45.667 | 0.99 |
| Tiffany | 45.463 | 1 |
| Walk Bridge | 45.239 | 0.98 |
| Plane | 45.802 | 0.98 |
| House | 46.331 | 0.99 |

The Proposed WEF-CW method is compared with Ellinas et al. [9], Kung et al.[20], Al Qershi et al.[18] and Hameed et al. [19] methods for image authentication. Graph I shows the comparison of the proposed method with other methods. It is clearly seen that the proposed scheme outperforms than the other methods.

The proposed WEF-CW method is also tested for its robustness against various attacks on Lena image of size 256×256 as given below:

- Additive noise like Gaussian, Salt and Pepper and Additive Uniform noise were added randomly
- Filtering like median filtering, Gaussian filtering and low pass filtering with sizes 3×3, 7×7
- Rotation with angle $10^0$
- Image Sharpening
- JPEG Compression with quality factors 40 and 80

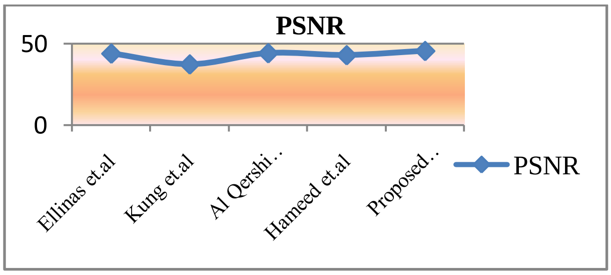


**Fig 5: Comparison of PSNR values of Proposed WEF-CW method with other Methods**

**Table 2: Comparison of PSNR values of attacks performed on Lena image using WEF-CW method with Lu et al. [11] and Tang et al. [17] methods**

| Type of Attacks | Lu et al. Method | Tang et al. Method | WEF-CW Method |
|---|---|---|---|
| | NCC | | |
| Gaussian noise | 0.76 | NA | 0.85 |
| Salt and pepper noise | 0.85 | NA | 0.89 |
| Additive Uniform Noise | NA | 0.88 | 0.88 |
| Median filter (3×3) | NA | 0.13 | 0.45 |
| Gaussian filter(3x3) | NA | 0.63 | 0.72 |
| Median filter (7×7) | 0.85 | NA | 0.86 |
| Low pass filtering (7×7) | 0.85 | NA | 0.89 |
| Rotation 10 degrees | 0.85 | NA | 0.84 |
| JPEG 80 | 0.92 | 0.75 | 0.97 |
| JPEG 40 | 0.92 | 0.38 | 0.81 |
| Image Sharpening 3×3 | NA | 0.5 | 0.74 |

The PSNR values with the above attacks for the WEF-CW method and others like Lu et al. [11] and Tang et a.l [17] methods are given in Table 2. The results clearly show the efficacy of the proposed scheme even with attacks when compared to other methods.

## 3.1 Tamper Detection and Localization

A region of pixel intensities in the watermarked image is tampered and replaced with the pixel intensities same as in the original image. The attacked image does not show any visual difference when compared with the original image. However, the extracted watermark clearly shows the tampered region. Fig. 6a) is the tampered image and Fig 6d) shows the extracted logo with localized tamper.

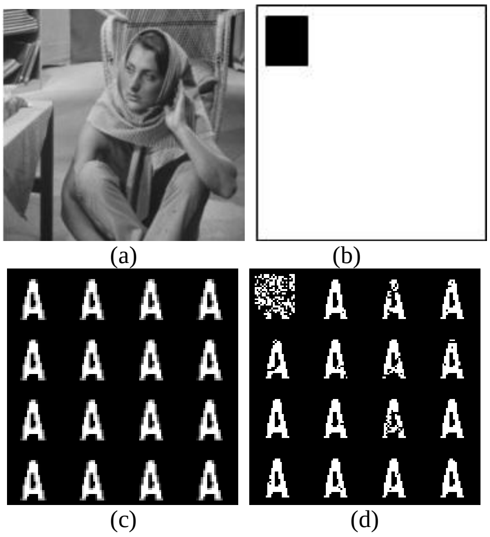

(a) (b)
(c) (d)

**Fig 6: a) Watermarked Image b) Difference image showing tampered region c) Original Binary Logo d) Extracted logo indicating the tampered region.**

## 4. CONCLUSIONS

This paper has proposed an efficient WEF-CW method for reversible data hiding using adjacent coefficient differences. The content of the image is embedded into image itself. The proposed WEF-CW scheme restores the original image without any distortions from the watermarked image after the hidden data is extracted. The experimental results demonstrate the good embedding quality and imperceptibility of the proposed WEF-CW method. The advantage of the WEF-CW method is that it can easily identify tamper locations and is capable of accurate tamper localization when the image has been attacked by malicious tamper while tolerating JPEG lossy compression to a large extent and it is sensitive to the change of parameter. Further the experiments also indicate the efficacy of the proposed WEF-CW method over other existing methods. Thus, it can be concluded that this scheme is robust and more fragile to malicious distortions.

## 5. ACKNOWLEDGMENTS

The authors express deep sense of gratitude to Dr. G.Tulasi Ram Das, Honorable Vice Chancellor, JNTUK for his valuable support. 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. Authors would like to thank the anonymous reviewers for their valuable comments.

## 6. REFERENCES

[1] Schneider M, Chang S-F, 1996. A Robust content based digital signature for image authentication. In Proceedings of the IEEE international conference on image processing, vol 2, pp 231-235.

[2] Queluz MP, 1998. Towards robust content based techniques for image authentication. In: Proceedings of IEEE Signal processing society, workshop on multimedia signal processing.

[3] Dittman J. Steimatez A, 1999. Content based digital signature for motion pictures authentication and content fragile watermarking. In: Proceedings of the IEEE international conference on multimedia computing and systems, vol II, Florence, Italy, pp 209-213.

[4] Dugelay J-L, rey C, 2002. Un panorama des Methods de Tatouage Permettant d'Asseurer un Service d'Intégrité. Revue Traitement du Signal, 18(4), France.

[5] Storck D, 1996. A new approach to integrity of digital images. In proceedings of the IFIP conference on mobile communications, pp 309-316.

[6] Yu S, Hu Y. Zhou J, 2004. Content based watermarking scheme for image authentication. In: Proceedings of the control, automation, robotics and vision conference, vol 2, pp 1083-1087.

[7] Lou DC, Liu JL, 2000. Fault resilient and compression tolerant digital signature for image authentication, IEEE Trans Consum Electron, 46:31-39

[8] Tzeng CH, Tsai WH, 2001. A new technique for authentication of image/vedio for multimedia applications. In: proceedings of ACM multimedia workshops –multimedia and security: new challenges, Ottawa, Ontario, Canada.

[9] Ellinas, J. N., Dimitios E. Manolakis, 2007. A Robust Wavelet-based Watermarking Algorithm Using Edge Detection, Proceedings of World Academy of Science, Engineering and Technology, vol. 25, 438-443.

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

[11] Lu W, Lu H, Chung F.L, 2010. Feature based robust watermarking using image normalization, Computers and Electrical Engineering 36, pp 2–18.

[12] Thurgood J, Peplow R, A, 2005. Digital Watermarking Algorithm for Authentication and Tamper Detection, Proceedings, Prasa, pp 05-09.

[13] Roy S and Sun Q, Sep 2007. Robust hash for detecting and localizing image tampering, in Proc. IEEE International Conference on Image Processing.

[14] Ni Z, Shi Y, Ansari N, and Su W, 2003. Reversible data hiding, Proc. ISCAS ,vol. 2, pp. 912–915.

[15] De Vleeschouwer C, Delaigle J.F, Macq B, 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management, IEEE Trans. On Multimeida, vol. 5, no. 1.

[16] Lee S. K., Suh Y. H, and Ho Y.S, 2006. Reversible image authentication based on watermarking, in Proc. IEEE Int. Conf. Multimedia Expo, Toronto, ON, Canada, pp. 1321–1324.

[17] Tang C.H and Hang H.M, 2003. A Feature-Based Robust Digital Image Watermarking Scheme, IEEE Transactions on Signal Processing, Vol. 51(4).

[18] Al-Qershi O.M, Bee Ee K, 2009. Authentication and Data Hiding Using a Reversible ROI-based Watermarking Scheme for DICOM Images, World Academy of Science, Engineering and Technology 50, pp 801-806.

[19] Hameed K,.Mumtaz A, Gilani S.A.M, 2006. Digital image watermarking in the wavelet transform domain, World Academy of Science and Technology, 13 pp 86-89.

[20] Kung C.M, Chao S.T, Tu Y.C, Yan Y.H, Kung C.H, 2009. A Robust Watermarking and Image Authentication Scheme used for Digital Content Application J. Multimedia, 4 (3) 112.

[21] Tai W.L, Yeh C.M, and Chang C.C, 2009. Reversible Data Hiding Based on Histogram Modification of Pixel Differences, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 19(6), pp 906-910.