A Fragile Video Watermarking Algorithm for Content Authentication based on Block Mean and Modulation Factor

A.F.EIGamal Department of CS Mansoura University Egypt N.A.Mosa Department of CS Mansoura University Egypt W.K.EISaid
Department of CS
Mansoura University
Egypt

ABSTRACT

Most watermarking algorithms are either robust watermarking for copyright protection or fragile watermarking for tamper detection. This paper proposes a fragile video watermarking algorithm that has the ability to detect tamper in spatial domains. The original video frame is converted from RGB color space into YCbCr color space, then the chrominance component Cb is partitioned into non-overlapping blocks of pixels according to the number of bits of the original watermark. The watermark bits are embedded using a mathematical rule for each block separately. A detailed study for the applicability of this algorithm to content authentication is conducted. Experimental results reveal that the proposed algorithm achieves a low computation cost and high detection rate against a wide range of tampering attacks such as Filtering, Non-Geometric Transformation and Geometric Transformation.

Keywords

Content Authentication, Fragile Video Watermarking, Tampering Attacks, Modulation Factor.

1. INTRODUCTION

With the rapid development of multimedia network technology, the digital media, particularly video information has reached an extraordinary level. However, during transmission, video information is usually vulnerable to malicious attacks of different kinds, which result in casting doubts on the integrity and authenticity of a video content. Therefore, in recent years, implementing effective protection of the authenticity and integrity of a video content in a network environment has become the top research issue in the field of multimedia information security. The most popular method suggested for achieving the authenticity of digital video is the digital watermarking technology [1, 2]. Digital watermarking is an authentication means, which embeds visible or invisible information called watermark into the digital media (image, audio and video) without affecting its perceptual quality, and the embedded watermark can be extracted and used for verification purposes [3].

The underlying techniques used to implement digital watermarking in video sequences can be roughly classified into spatial and frequency domains, based on the method of hiding the watermark bits in the host video [4, 5]. Spatial domain watermarking is performed by modifying the pixel values of the host video frame directly [6, 7]. Transform domain techniques, on the other hand, alter the spatial pixel values of the host video frame according to a pre-determined transform and are more robust than spatial domain echniques, since they disperse the watermark in the spatial domain of the video frame, making it difficult to remove the

watermark through malicious attacks like cropping, scaling and rotation [8, 9, 10].

To solve the problem of illegal copying and proving ownership of a video content, robust video watermarking methods have been proposed, and to solve the problem of identifying manipulations of video sequences, fragile video watermarking methods have been suggested [11].

Most studies in the field of multimedia security consider video watermarking an extension of image watermarking on video frames. Thus, fragile video watermarking schemes can be classified into two classes. The first is called block-wise fragile watermarking schemes [12, 13], which divide a host data into small blocks and embed the mark into each block, which makes its effect confined to identifying tampered blocks. The second is known as pixel-wise fragile watermarking schemes [14, 15], in which the watermark information derived from gray values of host pixels is embedded into the host pixels themselves, whereby, tampered pixels can be identified due to the absence of the watermark information they carry.

However, robustness is not an important factor for fragile watermarking. The most important factors include [16]:

Perceptual Quality: It means, all kinds of processes do not degrade the quality of the original multimedia signals.

Location Capability: It is the capability of the algorithm to locate the modified region in multimedia signals. From this viewpoint, there are three kinds of locating accuracy, namely locating single pixel tampered, locating single block tampered and locating the whole signal.

Security: It is the ability of the algorithm to guarantee the authenticity and integrity of received multimedia signals. If an unauthorized user forges an arbitrary signal, or accesses the authenticator freely, the fragile watermark system is useless. Hence, the security issue should be taken into consideration by the designer when constructing the fragile watermark system.

Generally, an effective authentication system based on fragile watermarking should have the following three desirable features [17]:

- To be able to insert invisible authentication data under normal viewing conditions;
- To be able to determine whether or not the multimedia content has been altered;
- To be able to locate the alteration, if any;

The purpose of this paper is to present a fragile watermarking method for color video authentication. The proposed algorithm does not set any requirements to detect the presence of a watermark. Therefore, this algorithm is completely blind.

The rest of the paper is organized as follows: Section 2 discusses the content authentication background. Section 3 describes the proposed algorithm in complete detail. Section 4 includes the experimental results. Section 5 is the conclusion of this paper, which is followed by a list of the relevant references.

2. BACKGROUND FOR CONTENT AUTHENTICATION

Content Authentication has become one of the most important research topics. Many real applications need a methodology that assures that when delivering something to somewhere; it is delivered as it is. The appropriate methodology should be simple and should secure to assure the authenticity of the work and the source of the transmitted work [18].

The watermarking-based Content Authentication can be classified into two types: The first type is Exact Authentication, in which the security requirement is to reject any message that has been alerted to the slightest degree; while the second type is Selective Authentication. Unlike the first type, it only needs to verify some selective places in the work in order to be authenticated [1, 19].

Exact Authentication can be fulfilled by using fragile watermarks, which are designed to detect any unauthorized modifications. On the other hand, Selective Authentication can be accomplished by using semi-fragile watermarks, which can discriminate between common signal processing operations and small noise and malicious content modification; in the other words, it is robust to light changes and fragile to significant changes [20].

Generally, the uses of Content Authentication system depend on the application validity level. For applications where no modifications in the multimedia content are allowed such as medical diagnosis and crime detection, Exact Authentication is considered an effective tool. Whereas, Selective Authentication is used in many applications that accept some benign processing operations into the multimedia content for the purposes of transmission, enhancement and restoration[20, 21, 22].

3. PROPOSED ALGORITHM

In a color-video frame, high correlation exists among R, G, and B planes, so major changes can be achieved without significant degradation, by exploiting the psychovisual redundancy and spatial correlations. In the proposed algorithm, the psychovisual redundancy is reduced by converting RGB to a less correlated color space such as YCbCr. On the other hand, the spatial redundancy is reduced by block modulation. This section introduces a novel fragile watermarking algorithm in the spatial domain for color video authentication using block mean and modulation factor. The detailed algorithm is as follows:

3.1 Embedding Phase

Let the binary watermark of the size M1xM2 pixels, to be embedded, be denoted as W=(0 for black and 1 for white) and the original video frame of the size N1xN2 pixels be denoted as F=(24-bit color). An illustration of the watermark embedding process is shown in Figure 1. First, the video frame is transformed from RGB color space into another less correlation color space such as YCbCr. Next, the

chrominance component Cb is selected for watermarking, since the human vision system is less sensitive to chrominance changes than luminance, major changes can be made on Cb without significant degradation [23]. After that, the Cb component is tilled into B*B non-overlapping blocks of pixels, then each block is watermarked separately. Finally, the watermark bits are embedded by using new mathematical formula. The concrete embedding procedure can be summarized as follows:

Inputs: Color video and binary watermark image.

Outputs: Watermarked color video.

Steps:

- (1) Read the color video V & the binary watermark image W.
- (2) Divide V into distinct frames F.
- (3) Convert F from RGB color space into YCbCr format for better watermarking efficiency. Since the pixel values are highly correlated in RGB color space, the watermark embedding in YCbCr color space is preferred. Transforming RGB to YCbCr is done by [23]:

$$Y = (77/256)*R + (150/256)*G + (29/256)*B,$$

$$Cb = -(44/256)*R - (87/256)*G + (131/256)*B + 128, (1)$$

$$Cr = (131/256)*R - (110/256)*G - (21/256)*B + 128$$

- (4) Select the chrominance component Cb of each frame to embed the watermark bits, where the chrominance part can lose much data, without affecting the frame quality.
- (5) Divide Cb into non-overlapping blocks B_i (with the size b^*b) according to the number of bits of the original watermark image, where each bit in the watermark image corresponds to one block in the Cb component.
- (6) Perform the following steps for each B*B block to embed the watermark information bits:
 - 6.1 Calculate the block mean M as follows:

$$\mathbf{M} = \sum_{\mathbf{i}}^{\mathbf{r}} \sum_{\mathbf{j}}^{\mathbf{c}} \mathbf{B}(\mathbf{i}, \mathbf{j}) / \mathbf{n}$$
 (2)

Where n is the total number of block pixels.

- 6.2 Find the block size and store it in S.
- 6.3. Create PRN matrix of size S containing pseudorandom integer values drawn from the discrete uniform distribution on 1:3, with the same random number generator.
- 6.4 Divide the block into two equal parts: Upper part H and Lower part L as equations below:

$$H = B(1:(r/2),1:c)$$
 (3)

$$L = B((r/2) + 1 : r, 1 : c)$$
 (4)

Where r, and c are the number of block rows and columns respectively.

6.5 Modify the Upper part and Lower part of the block by adding the binary watermark bits W_i in the following manner:

$$\begin{split} & \text{If W}_i = 0 \ , \\ & \quad H = M + \alpha \left(mean \left(PRN \right) \right) \\ & \quad L = M - \alpha \left(mean \left(PRN \right) \right) \\ & \quad OtherWise \\ & \quad H = M - \alpha \left(mean \left(PRN \right) \right) \\ & \quad L = M + \alpha \left(mean \left(PRN \right) \right) \end{split} \tag{5}$$

Where α is the modulation factor, which can be used for completely controlling the quality of watermarked frame and the watermark detection rate.

- 6.6 Create a watermarked block W_b by adding modified H, L in the Upper and Lower parts respectively.
- (7) Collect the watermarked blocks obtained from the previous steps to get the watermarked frame $W_{\rm f}$.
- (8) Convert back the watermarked frame from YCbCr color space to RGB. Transforming YCbCr to RGB is done by [23]:

$$R = Y + 1.371*(Cr - 128),$$

$$G = Y - 0.698*(Cr - 128) - 0.336*(Cb - 128),$$

$$B = Y + 1.732*(Cb - 128)$$
(6)

(9) Calculate the PSNR (peak-signal-to-noise ratio) value between original video frame F and watermarked frame W_f .

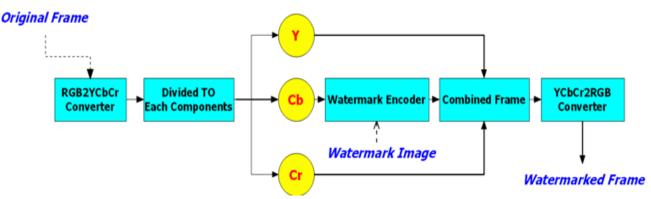


Fig 1: Watermark Embedding Procedure

3.2 Extraction Phase

The procedures of the extraction phase are performed in a reverse order to the embedding, as shown in Figure.2. The extraction algorithm does not need the original frame to recover the embedded watermark, because it belongs to a blind family. The details of the extraction algorithm are listed as follows:

Input: Watermarked color video. **Output:** Binary watermark image.

Steps:

- (1) Read the watermarked video W_v.
- (2) Divide W_v into distinct watermarked frames W_f.
- (3) Convert W_f from RGB color space into YCbCr format.
- (4) Select the chrominance component Cb of each frame to extract the watermark.
- (5) Divide Cb into non-overlapping blocks WB_i (with the size b*b) according to the number of bits of the original watermark image.
- (6) Perform the following steps for each watermarked block to extract the original watermark bits:
 - 6.1 Divide the block into two equal parts: Upper part H and Lower part L as mentioned previously.
 - 6.2 Calculate the mean value $M_{\rm H}$ of the Upper part of the block as follows:

$$\mathbf{M_H} = \sum_{\mathbf{i}}^{\mathbf{r}} \sum_{\mathbf{j}}^{\mathbf{c}} \mathbf{H}(\mathbf{i}, \mathbf{j}) / \mathbf{n}$$
 (7)

Where n is the total number of block pixels into upper part.

6.3 Calculate the mean value M_L of the Lower part of the block as follows:

$$\mathbf{M_L} = \sum_{i}^{r} \sum_{j}^{c} \mathbf{L(i,j)} / \mathbf{n}$$
 (8)

Where n is the total number of block pixels into lower part.

6.4 Calculate the difference value Diff between the mean of Upper part M_H and the mean of Lower part M_L of the block as follows:

$$Diff = M_{H} - M_{L}$$
 (9)

6.5 Extract the watermark bit using the following formula:

If
$$Diff \Rightarrow 0$$
,

$$\mathbf{W}^{*}(\mathbf{i},\mathbf{j})=\mathbf{0}$$

$$\mathbf{W}^{*}(\mathbf{i},\mathbf{j}) = \mathbf{1}$$

- (7) Collect the resultant bits from the previous steps for all blocks to obtain the binary watermark $\boldsymbol{W}^{*}.$
- (8) Measure the CER (correctly extracted ratio) value between original and extracted watermark.
- (9) Output the extracted watermark W*.

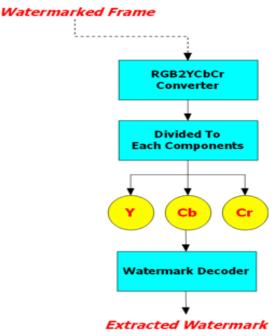


Fig 2: Watermark Extracting Procedure

Theoretically, the proposed algorithm has the capability to recover the embedded watermark completely, if the watermarked frame has not been tampered with in any significant manner. However, in practice it seems difficult, because the conversion process between color spaces produces minor variations in a limited number of blocks. Therefore, it was necessary to take this aspect into account in the experiment to be conducted in the next part.

4. EXPERIMENTAL RESULTS

The experiments were carried out on well-known color video sequences (i.e. Akiyo) with a frame size of 352*264 as shown in Figure.3. These sequences are 30 fps (frame per second) within a period of 10 seconds. In addition, a binary image with half the size of the video frames is considered as the watermark shown in Figure.4. The perceptual quality of watermarked frames is studied with PSNR, which is given by Eq.11 [24]. While the capability of tamper detection is investigated by CER, which is used as a general measure of the similarity between the original and extracted watermarks, and is defined by Eq.13 [25].

$$PSNR = 10 log_{10} \frac{(R*R)}{MSE} [dB]$$
 (11)

Where R=256, MSE is the mean square error, which is defined as:

MSE =
$$\sum_{j=1}^{r} \sum_{k=1}^{c} \frac{[F(j,k) - WF(j,k)]^2}{r * c}$$
 (12)

Where F is the original video frame and WF is the watermarked video frame.

$$CER = \frac{B_c}{m*n} * 100 [\%]$$
 (13)

Where m*n means the size of the watermark image, and Bc is the number of correctly extracted watermark bits.



4.1 Selection of Modulation Factor

Generally, the accurate measurement of the invisibility as perceived by a human observer is a great challenge in our fragile watermarking system. This is because the amount and visibility of distortions introduced by the watermarking algorithm strongly depend on the value of the modulation factor. However, as it has been previously suggested, the modulation factor value does not only affect the watermarked frame quality, but also affects the correctly extracted ratio of the watermark. So, the modulation factor value should be selected to make a balance between these two requirements. Since the efficiency of the new method depends on the way through which the modulation factor has been selected, several experiments have been performed on a set of video frames from every video sequence using variant modulation factors to get the optimal value. In those experiments, a set of integer values in the range 1 to 5 has been generated for the modulation factor, then for each value, the PSNR and CER values are calculated for all watermarked frames without tampering. The ideal value of the modulation factor is the value that achieves full recovery of the watermark from all test frames and makes the perceptual degradation in the watermarked frames unnoticeable. The relationship between the modulation factor α and average PSNR, average CER for all watermarked frames is shown in Figure.5 and Figure.6 respectively.

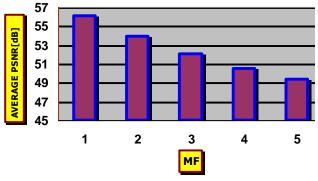


Fig 5: Average PSNR for different modulation factor

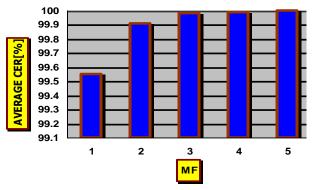


Fig 6: Average CER for different modulation factor

It can be concluded from the above results, that the maximum PSNR rates of frame quality are achieved by using small values of modulation factor. However, the embedded watermark cannot be fully recovered from all watermarked frames. This is mainly because of the impact of color space conversion into some watermarked blocks. Therefore, the modulation factor of 5 is considered the optimal value, because it achieves the correctly extracted ratio for all test frames. Moreover, according to [26], it maintains the quality of watermarked frames either at the level of human eyes perception or at a typical PSNR rate.

4.2 Tamper Detection Test

An important property of the fragile watermarking algorithms is that they are not only able to determine whether the original video has been altered or not, but are also able to locate any alteration made on the video frames. This section presents some of the experiments conducted to show the capability of the proposed algorithm to locate the modified region in a watermarked video. Before proceeding, at the very outset, let us mention that the modulation factor α =5, which is decided by preliminary investigations and the accepted correctly extracted ratio is 100%. In addition, it should be noted that all the experiments in this part have been performed using Matlap 7.11 and Photoshop 9.0.

4.2.1 Detection Test Against Non-Geometric Transformation

To test the response of the watermarking algorithm against Non-Geometric attacks like the different types of noise addition, watermarked frames are modified by adding Salt & Pepper Noise with the Density of 0.005 and Gaussian Noise with the Variance of 0.05. The edited frames with Salt & Pepper Noise and the extracted binary watermarks are shown in Figure. 7. On the other hand, the corrupted frames with Gaussian Noise and the extracted binary watermarks are shown in Figure. 8. The results indicate that the algorithm is sensitive to Non-Geometric Transformation because CER is smaller than 100% for both test frames. Therefore, we can detect that the watermarked frame has been altered.

Tampered Frame	Extracted Watermark	CER [%]
		97.80
		97.87

Fig 7:Detector Response To Salt & Pepper Noise(D=0.005)

Tampered Frame	Extracted Watermark	CER [%]
	15 m	70.91
		70.53

Fig 8: Detector Response To Gaussian Noise (V=0.05)

4.2.2 Detection Test Against Geometric Transformation

To test the response of the watermarking algorithm against Geometric attacks like rotation, cropping and flipping, watermarked frames are rotated with angle of 180°. In addition, watermarked frames are alerted by cropping a 64*64 block from various regions including: left top, right top, left bottom and right bottom. Furthermore the watermarked frames are flipped in both directions (horizontally and vertically). Figure.9 shows the extracted binary watermarks from rotated frames. Figure.10 shows the extracted binary watermarks from watermarked frames under cropping process. Figure.11 shows the extracted binary watermarks from watermarked frames after the flipping process. From the results in Figure.9, it can be observed that the recovered watermarks differ from the original whether at the level of human vision or at the level of CER. On the other side, as shown in Figure.10 the altered blocks by cropping process are clearly identifiable. Moreover as shown in Figure.11, the extracted watermarks are flipped according to the direction of flipping process. Therefore, the algorithm is more effective to Geometric Transformation.

Tampered Frame	Extracted Watermark	CER [%]
		21.35
		21.35

Fig 9: Detector Response To Rotation (Angle=180)

Tampered	Extracted	CER [%]
Frame	Watermark	
		95.59
No.		95.59
		95.59
		95.59

Fig 10: Detector Response To Cropping (Area=64*64)

Tampered Frame	Extracted Watermark	CER [%]
		89.91
		89.91
	管察	20.54
	管	20.54

Fig 11:Detector Response To Flipping

4.2.3 Detection Test Against Filtering

One of the most common manipulations in digital signal processing is filtering. To evaluate the response of the watermarking algorithm to filtering attacks, watermarked frames were tested on various types of filtering such as average filter, median filter, sharpen filter and motion filter. Figures.12, 13, 14, and 15 show all scenarios of watermarked frames and extracted watermarks after filtering process. As can be seen, the rates of correctly detected manipulations differ from one filter to another. Although the different impacts of various filters into watermarked video, the original watermark cannot be recovered completely from any filtered frame. This proves that the algorithm has the ability to detect tampering under the lowest and the highest levels of filter attacks.

Tampered Frame	Extracted Watermark	CER [%]
		90.09
		90.09

Fig 12:Detector Response To Average Filter(W= [5x5])

Tampered Frame	Extracted Watermark	CER [%]
		87.49
	经	87.60

Fig 13:Detector Response To Median Filter (W= [5x5])

Tampered Frame	Extracted Watermark	CER [%]
Topical state of the state of t		99.25
Total Control of the		99.23

Fig 14:Detector Response To Sharpen Filter(Alpha=0.3)

Tampered Frame	Extracted Watermark	CER [%]
		97.90
		97.91

Fig 15: Detector Response To Motion Filter (Len=10,Theta=0)

4.2.5 Detection Test Against Other Effects

This part of the evaluation test studies the effect of significant modifications, which assume that no mark exists into watermarked video such as Text Adding, and Localized replacement attacks, which means substituting a part of watermarked frame by another one. Figure.16 reveals a scenario of changing critical information of watermarked frames by inserting the word "Egypt" into different areas. Figure.17 reveals a scenario of replacing the face of weather forecasting presenter in the first watermarked frame with the face of the first author and replacing the face of weather forecasting presenter in the second watermarked frame with the face of the third author daughter. As shown in Figure.16, the extracted watermarks after text adding indicate the capability of the algorithm to detect the embedded text and locate the edited regions within the watermarked frames. On the other hand, the results in Figure.17 indicate the negative impact of localized replacement attacks into the extracted watermarks in the corresponding tampered area of the watermarked frames, so the proposed algorithm is desirable to provide an indication of how much alteration has occurred and where it is located.

Tampered	Extracted	
Frame	Watermark	CER [%]
EGYPT	EGYPT	98.34
EGYPT	EGYPT	98.51

Fig 16: Detector Response To Text Adding

Tampered Frame	Extracted Watermark	CER [%]
		88.67
		86.55

Fig 17: Detector Response To Localized Replacement Attacks

5. CONCLUSION

This paper proposes a fragile watermarking algorithm for tamper detection of color videos in YCbCr color space utilizing both the block feature and modulation factor. The authentication code generated by the proposed algorithm belongs to a blind family. Therefore, it does not require an original video to extract embedded data, and can detect unlawful attacks without the original watermark by detecting the invalid micro blocks caused by the attacks. The simulation results show that the capability of the proposed algorithm to detect and locate video tampering without effect on the visual quality of the watermarked video. In our future work, the video frames can be subject to scene change analysis to embed an independent watermark in the sequence of frames forming a scene, and repeating this procedure for all the scenes within an original video.

6. REFERENCES

- [1] Cox, I.J., Miller, M.L., and Bloom, J. A., "Digital watermarking and fundamentals", Morgan Kaufmann, San Francisco, 2002.
- [2] Wu, M., and Liu, B. D., "Data hiding in image and video: Part I-fundamental issues and solutions", IEEE Trans. Image Processing, Vol. 12, No. 6, PP: 685-695, 2003.
- [3] Yassin, N.I., Salem, N.M., and El Adawy, M.I.," Block based video watermarking scheme using wavelet transform and principle component analysis", IJCSI International Journal of Computer Science Issues, Vol.9, Issue. 1, No. 3, PP: 296-301, 2012.
- [4] Sinha, S., Bardhan, P., Pramanick, S., Jagatramka, A., Kole, D.K., and Chakraborty, A., "Digital video watermarking using discrete wavelet transform and principal component analysis", International Journal of Wisdom Based Computing, Vol. 1, No. 2, PP: 7-12, 2011.
- [5] Jayamalar, T., and Radha, V., "Survey on digital video watermarking techniques and attacks on watermarks", International Journal of Engineering Science and Technology, Vol. 2, No. 12, PP: 6963-6967, 2010.
- [6] Kalker, T., Depovere, G., Haitsma, J., and Maes, M., "A video watermarking system for broadcast monitoring", Proceedings of The SPIE, Vol. 3657, PP: 103-112, 1999.
- [7] Paul, R.T., "Review of robust video watermarking techniques", IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE, No. 3, PP: 90-95, 2011.
- [8] Cox, I. J., Kilian, J., Leighton, F.T., and Shamoon, T., "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Processing, Vol. 6, No. 12, PP: 1673-1687, 1997.
- [9] Li, C.H., and Wang, S.S., "Transform based watermarking for digital images and video", IEEE International Conference, 1999.
- [10] Sinha, S., Pramanick, S., Jagatramka, A., Bardhan, P., Kole, D.K., and Chakraborty, A., "Digital video watermarking using singular value decomposition", Proceedings on IEEE EDS Student Paper Conference, PP: 53-56, 2011.
- [11] Do.err, G., and Dugelay, J.L., "A guide tour of video watermarking", Signal Processing Image Communication", Vol. 18, No. 4, PP: 263-282, 2003.
- [12] Wong, P.W., and Memon, N., "Secret and public key image watermarking schemes for image authentication and ownership verification", IEEE Trans. Image Process., Vol. 10, No. 10, PP: 1593-1601, 2001.

- [13] Yang, H., and Kot, A.C., "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier", IEEE Signal Process. Lett., Vol. 13, PP: 741-744, 2006.
- [14] Lu, H., Shen, R., and Chung, F.L., "Fragile watermarking scheme for image authentication", Electron. Lett, Vol. 39, No. 12, PP: 898-900, 2003.
- [15] Wu, J., Zhu, B.B., Li, S., and Lin, F., "A secure image authentication algorithm with pixel-level tamper localization", in Proc. Int. Conf. Image Processing, PP: 1573-1576, 2004.
- [16] Liu, S.H., Yao, H.X., Gao, W., and Liu, Y.L.,"An image fragile watermark scheme based on chaotic image pattern and pixel-pairs", Applied Mathematics and Computation, Vol. 185, PP: 869-882, 2007.
- [17] Wu, M., and Liu, B., "Watermarking for image authentication", IEEE Trans.Image Processing, Vol 2, PP: 437-441, 1998.
- [18] Alomari, R.S., and Al-Jaber, A., "A fragile watermarking algorithm for content authentication", International Journal of Computing and Information Sciences, Vol. 2, No. 1, PP: 27-37, 2004.
- [19] Zhao, Y., "Dual domain semi fragile watermarking for image authentication", Master Thesis, University of Toronto (Canada), 2003.
- [20] Haouzia, A., Noumeir, R., "Methods for image authentication: a survey", Multimedia Tools and Applications, Vol. 39, Issue. 1, PP: 1-46, 2008.
- [21] Cox, I.J., and Miller, M.L., "The first 50 years of electronic watermarking", EURASIP Journal on Advances in Signal Processing, Vol. 2, PP: 126-132, 2002.
- [22] Mintzer, F., Braudaway, G.W., and Yeung, M.M., "Effective and ineffective digital watermarks", in Proc. ICIP'97, IEEE Int. Conf. on Image Processing, Santa Barbara, CA, Vol. III, PP: 223-226, 1997.
- [23] Salomon, D., "Data compression the complete reference", 3rd ED, Morgan Kaufmann Publishers, 2004.
- [24] Ramamurthy, N., and Varadarajan, S., "The robust digital image watermarking scheme with back propagation neural network in DWT domain", Procedia Engineering, Vol. 38, PP: 3769-3778, 2012.
- [25] Watanabe, J., Hasegawa, M., and Kato, S., "A robust and fragile watermarking method", International Workshop on Spectral Methods and Multirate Signal Processing, Vienna, Austria, PP: 211-216, 2004.
- [26] Zayer, W.H., and Mnati, M.N., "Secure and non blind watermarking scheme for RGB images using arnold scrambling based on DWT", Advances in Environmental Biology, Vol. 5, No. 9, PP: 2697-2707, 2011.