Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 233 – 240

Procedia Computer Science

Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Adaptive Digital Watermarking for Copyright Protection of Digital Images in Wavelet Domain

Prasanth Vaidya S.[a], Chandra Mouli P.V.S.S.R.[a,*]

[a]School of Computing Science and Engineering, VIT University, Vellore - 632014, India

Abstract

Digital image watermarking is the process of embedding watermark into a digital image for authentication and thereby protecting the digital image from copyright violation. In this paper, an adaptive invisible watermarking scheme is proposed in wavelet domain. The proposed method is adaptive in the sense that the scaling and embedding factors are calculated using Bhattacharyya distance and the fourth cumulant moment - kurtosis. The proposed method can be easily employed to preserve the ownership rights and in addition for piracy of digital data prevention. The proposed method is robust to all image and signal processing attacks and highly secured for the protection of copyright information as the process is executed in wavelet domain. Experimental results and statistical evaluation of the results shows the efficacy of the proposed method.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Keywords: Adaptive watermarking; Invisible watermarking; Bhattacharyya distance; Kurtosis; Wavelet based watermarking;

1. Introduction

Due to information explosion, growth of digital content is ever increasing in the order of peta bytes. At present Internet has become a powerful source of information to the end users, at the same time unauthorized and copyright Violated information is also easily available, making them unsure about the originality of information. On the other Hand establishing the legal ownership of digital content is important for the content providers. In such scenario, Availability of authentic information from authorized sources is what the end users and content providers will be looking for. To ensure authenticity and legal ownership of digital content, various methods such as steganography, cryptography, and watermarking have been proposed in the literature. Digital watermarking is one such powerful information hiding technique extensively used to overcome illegal copying, modifying and redistributing the digital content.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.063

Watermarking is used for copyright identification (mark impressed on piece of paper). Digital watermarking is the process of hiding of information in carrier signal when applied in digital domain where it embeds a mark (text/logo) into an image, text or video. Watermarking is defined, in simple, as a practice of imperceptibly altering a work to embed a message about that work[1,2,3,4,5,6]. Digital watermarking is used as a tool for identifying the authorized consumer of the data. It can also be used to detect the data that has been illegally distributed. A typical watermarking system is shown in Fig. 1.

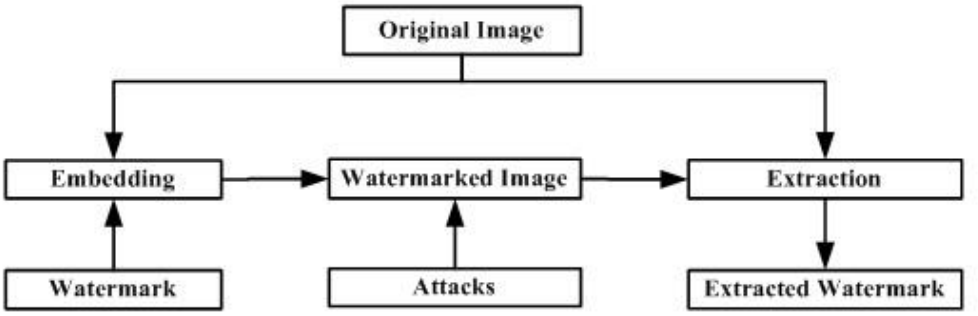

Fig. 1. General watermarking system

Image processing operations and image transforms are commonly used to create and apply watermarks. In general, watermarking system is divided into two distinct steps: watermark embedding and watermark extraction. Watermark embedding watermark can be done either in spatial domain or in frequency domain. In the spatial domain, pixels in the host image are manipulated with the pixels of the watermarked image[7,8]. In frequency domain, watermark is embedded into the coefficients of Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT) or Discrete Fourier Transform (DFT). This is referred to as spread spectrum and provide more robustness in the watermarking process[9,10]. Attacks are made during the transmission of watermarked image along a communication channel. Attacks may not necessarily remove the watermark, but disables its readability[11,12].

While designing watermark, main features to be considered are imperceptibility, robustness, fidelity and security. Imperceptibility feature desires the watermarked image to look almost identical with original image. Robustness ensures insusceptibility of watermark to the transformations and Fidelity ensures non degradability of the watermark. Security is the ability to resist malicious attacks which specifically prevent watermark purpose.

Watermark can be categorized into three types: robust, semi-fragile, and fragile. Robustness caters for copyright protection in order to declare rightful ownership. Semi-fragile watermarks are used for detecting unauthorized modifications. Fragile watermarks are used for image authentication[13,14].

Digital watermarking applications include broadcast monitoring, owner identification, proof of ownership, transaction tracking, authentication, copy control, device control, and legacy enhancements [1].

DWT has more advantages than other transforms for many applications such as copyright protection and ownership identification[15]. Lili. et al.[16] implemented Wavelet based image watermarking technique by training ANN to memorize the relationship between a set of original DWT coefficients and its watermarked version. Qi, Xiaojun, and Xing Xin[17] applied quantization method for approximating sub band of the Haar wavelet transform of each block, Lin, Tzu-Chao, and Chao-Ming Lin[18] proposed wavelet based cryptography and watermarking scheme that verifies the copyright owner of the image. Nasir, I., et al. [19] proposed robust image watermarking scheme where feature points are used to eliminate synchronous errors between watermark embedding and detection. Interpolation techniques are used to achieve highly efficient watermarking scheme with greater payload capacity and higher image fidelity, compared to other schemes which can guarantee high image quality without sacrificing embedding capacity[20,21,22]. Su, Qingtang, et al. showed that DWT schemes are used to embed a large watermark in the cover data which provides high robustness against common attacks, while embedding such watermarks QR decomposition is used to attain higher invisibility of watermark[23]. Dawei et al.[24] proposed wavelet watermarking scheme where watermark is embedded into sub band coefficients as low frequency components have more effect on image quality than others, further high frequency can be easily removed after filtering.

In view of the above literature survey, this paper proposes a robust watermarking scheme in wavelet domain by calculating the embedding factor and scaling factor adaptively. In the proposed scheme, watermark is present invisibly within the content and can able to confirm the ownership, if necessary.

The rest of the paper is organized as follows. Section 2 gives the brief description of the concepts used in the proposed scheme. The proposed method is discussed in Section 3. In Section 4, experimental results are presented along with analysis of attacks for robustness testing. Section 5 concludes the work.

2. Preliminaries

2.1. Discrete Wavelet Transform

The 2-D discrete wavelet transform is computed by performing low-pass filtering and high-pass filtering of an image. The wavelet transform technique decomposes the given input image into approximation sub-band (LL) which is considered to be the low frequency band, middle frequency sub-bands (LH, HL) consists of both horizontal and vertical details and high frequency sub-band (HH) consists of diagonal details. The simplest wavelet which is used in the proposed scheme is Haar wavelet. The approximate band corresponds to low frequency components and detail bands correspond to high frequency components [25].
Wavelets can be best used as base functions for signal and image representation. Discrete wavelet transform (DWT) is one of the significant transform that translates an image from spatial domain to frequency domain. Using DWT, simultaneous interpretations can be made for both spatial and frequency domain and is widely used in watermarking as it is found to augment imperceptibility in the watermarked image.

2.2. Bhattacharyya Distance

Bhattacharyya distance measures the similarity of two discrete or continuous probability distributions. Bhattacharyya distance for multivariate normal distributions $P_i = N(\mu_i, \sum_i)$ is defined in equation (1).

$$D_B = \frac{1}{8}(\mu_1 - \mu_2)^T \Sigma^{-1}(\mu_1 - \mu_2) + \frac{1}{2}\ln\left(\frac{\det\Sigma}{\sqrt{\det\Sigma_1 \det\Sigma_2}}\right) \quad (1)$$

Where μ_i and $\sum_i$ are the mean and covariance's of the distributions and $\Sigma = \frac{\Sigma_1 + \Sigma_2}{2}$.
In general, the probability density functions of the images are normal distributed or near normal distributed. Same is the case with the watermark image. The similarity between the two images determines the strength of watermark to embed into the cover image such that the perceptibility of the cover image does not change and at the same time embed the watermark into the cover image[26,27,28].

2.3. Kurtosis

Kurtosis is a descriptor of the shape of the probability distribution. It is the ratio of the fourth cumulant and second cumulant [29,30]. The kurtosis of a normal distribution is defined in equation (2).

$$k = \frac{\mu^4}{\sigma^4} \quad (2)$$

Kurtosis and Bhattacharyya distance are combined for the calculation of scaling and embedding factors. These two measures are related for the reason that they deal with the shape of the probability distribution. Random guess of scaling and embedding factors is a tedious task and hence adaptive calculation is required. It is felt that Bhattacharyya distance and kurtosis can be employed for calculation of same and the results proved that the scaling and embedding factors calculated provides the robustness of the proposed approach. The scaling and embedding factors are calculated from the equations (3) and (4) respectively.

$$\alpha = k - d \tag{3}$$

$$\beta = 1 - (k - d) \tag{4}$$

Where *k*, *d* represent the kurtosis and Bhattacharya distance.

3. Proposed Method

The embedding and extraction algorithms are discussed in detail in this section. The block diagram of the watermark embedding is shown in Fig.2

3.1. Watermark Embedding

The pseudo code for embedding a watermark is described in this section. Scaling and embedding factors are calculated using equations (3) and (4) respectively. Watermark is embedded into the LL band of the cover image using equation (5). The modified LL band is combined with the LH, HL and HH bands of cover image to form the final watermarked image.

$$\begin{aligned} LL' &= \alpha \times LL + \beta \times W \\ &= (k - d) \times LL + (1 - k - d) \times W \end{aligned} \tag{5}$$

Algorithm: Watermark Embedding
Input: Cover image (I), Watermark (W).
Output: Watermarked image (I')
Step-1: Calculate the scaling and embedding factors (α, β)
Step-2: Apply 2 level DWT using Haar wavelet on the cover image
Step-3: Extract LL band.
Step-4: Insert watermark using equation (5)
Step-5: Combine the modified LL sub band (*LL'*) with other LH, HL and HH bands of cover image.
Step-6: Apply inverse DWT to get watermarked image

3.2. Watermark Extraction

The block diagram of the watermark extraction is shown in Fig.3. The pseudo code for extracting a watermark is described in this section.

In extraction process, reverse process of embedding is done where earlier calculated embedding factors are used for extraction. The original image and watermarked images has to be transformed into two level DWT to extract watermark from low frequency sub band of watermarked image. Watermark is extracted as defined in equation.

$$wm = \frac{LL' - \alpha \times LL_1}{\beta} \tag{6}$$

Where wm is the extracted watermark, LL_I' is the LL band of the watermarked image and LL_I is the LL band of the cover image.

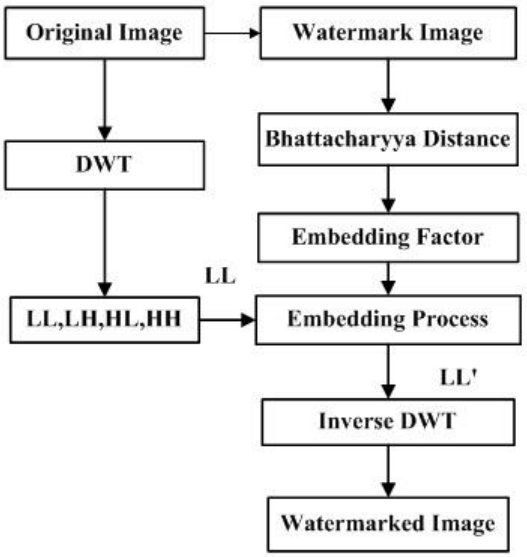

Fig. 2. Block diagram of proposed embedding method

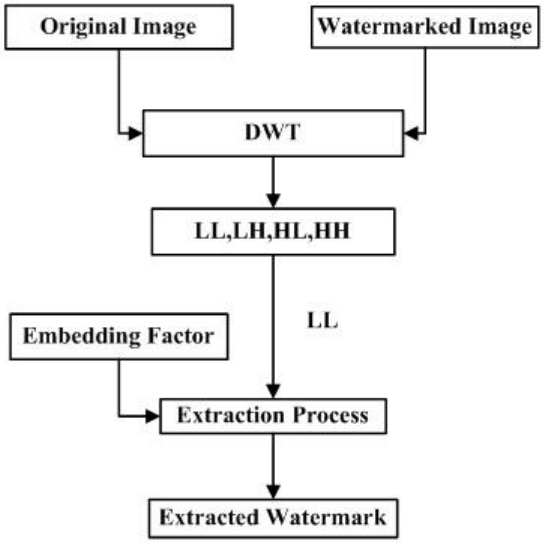

Fig. 3. Block diagram of proposed extraction method

Algorithm: Watermark Extraction
Input: Cover image (I), Watermarked image (I').
Output: Watermark Extracted (wm)
Step-1: Apply 2-level Haar wavelet on the cover image and watermarked image.
Step-2: Extract low frequency bands of both images.
Step-3: Obtain the scaling and embedding factors calculated during embedding process.
Step-4: Extract watermark using equation (6).

4. Experimental Results and Robustness Testing

To demonstrate the performance of proposed watermarking scheme several experiments are presented. The eleven different gray-level images "airplane, Barbara, girl1, girl2, house1, house2, lena, mandrill, original frame, peppers and tree" of size 256×256 and "cameraman" of size 64×64 are used as cover images and the watermark respectively. The cover images and watermark are shown in Fig. 4 and Fig. 5 respectively. Fig. 6 represents sample watermarked images. The performance of the proposed watermarking scheme is evaluated based on values of Peak signal to noise ratio (PSNR) and Normalized correlation coefficient (NCC). PSNR between the watermarked image and cover image has been used to evaluate imperceptibility, and easily defined via the mean square error (MSE)[31]. PSNR between the cover image *I* and the watermarked image *I'*, MSE is defined in equation (7), PSNR (in db) is defined in equation (8).

$$MSE = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I_{i,j} - I'_{i,j})^2}{mn} \tag{7}$$

$$PSNR = 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \tag{8}$$

Here, MAX_I is the maximum possible pixel value of the image. The PSNR values obtained are shown in Table 1. NCC is the metric used to find the correlation coefficient between the original watermark and the extracted watermark. The closer the value of NCC to 1, the similar the extracted watermark to the original watermark. The NCC is defined in equation (9). The NCC values obtained are shown in Table 2.

$$NCC = \frac{\sum_{a=1}^{m}\sum_{b=1}^{n} w(a,b) \times w'(a,b)}{\left(\sqrt{\sum_{a=1}^{m} w(a,b)^2}\right)\left(\sqrt{\sum_{a=1}^{m} w'(a,b)^2}\right)} \tag{9}$$

To test robustness, fidelity and other features of proposed methodology various types of attacks are applied to the watermarked image during communication. Most common attacks are noise attack, cropping, rotation, scaling and translate attacks are applied. Retrieved water marks are shown in figure 7 [(a)-(g)].

Fig. 4. Sample cover images

Fig. 5. sample watermark

Fig. 6. Sample watermarked images

Fig. 7. Retrieved watermarks with (a) No attack (b) salt and pepper noise (c) Gaussian noise (d) cropping (e) rotation (f) scaling and (g) translate Attacks

Noise attack: Salt and pepper noise and Gaussian noise attacks are applied for different mean and variance values. The results shown are for $\mu = 0$; $\sigma^2 = 1$.

Cropping attack: Cropping attack is tested by cropping the watermarked image randomly. PSNR values are good for all the images expect for house1 image which is not having similar characteristics of the cover image. Rotation attack: Rotation attack is a type of geometric attack which rotates the image by a specified angle. The results shown are for 30^{o} anti-clockwise direction. PSNR values are good for all the images expect for house1 image, which is having PSNR value around 20. NCC value range from 0.5-0.6.

Table 1. Comparison of PSNR values between cover image and watermarked image on various attacks

Cover images	No attack	Salt & Pepper noise attack	Gaussian noise attack	Cropping attack	Rotation attack	Scaling attack	Translation attack
Airplane	31.13	28.20	25.17	31.88	33.90	37.20	31.36
Barbara	52.07	31.41	26.08	52.43	50.68	54.73	52.22
Girl1	38.93	31.08	25.97	39.89	41.67	34.86	39.16
Girl2	22.86	22.24	21.57	23.86	25.66	41.22	23.08
House1	16.17	16.06	15.99	16.79	18.98	14.76	16.72
House2	35.11	29.83	25.21	35.85	37.87	41.36	35.41
Lena	47.49	32.15	26.01	35.85	37.87	41.36	35.41
Mandrill	33.67	29.96	25.21	34.61	36.45	34.46	33.83
Original frame	35.81	29.90	25.82	36.42	38.48	37.22	36.09
Peppers	22.73	21.22	20.62	23.48	25.55	26.82	29.80
Tree	32.88	28.81	24.97	33.81	35.68	37.66	33.38

Table 2. Comparison of PSNR values between watermark image and extracted watermark image on various attacks

Cover images	No attack	Salt & Pepper noise attack	Gaussian noise attack	Cropping attack	Rotation attack	Scaling attack	Translation attack
Airplane	1.00	0.6181	0.8747	0.8946	0.5537	0.9991	0.6410
Barbara	1.00	0.1146	0.8170	0.8943	0.1131	0.6141	0.6312
Girl1	1.00	0.7592	0.8805	0.8946	0.6171	0.9995	0.6412
Girl2	1.00	0.8692	0.8975	0.8944	0.6044	0.9998	0.6446
House1	1.00	0.9906	0.9535	0.8943	0.6252	0.9999	0.6415
House2	1.00	0.5599	0.8179	0.8938	0.6454	0.9982	0.6452
Lena	1.00	0.1458	0.8489	0.8944	0.2919	0.9827	0.6336
Mandrill	1.00	0.7156	0.8053	0.8946	0.6474	0.9991	0.6451
Original Frame	1.00	0.5356	0.8619	0.8943	0.5443	0.9956	0.6399
Peppers	1.00	0.9665	0.9279	0.8942	0.6222	0.9998	0.6403
Tree	1.00	0.6298	0.7880	0.8940	0.6444	0.9991	0.6414

Table 3. Comparison of PSNR(in dB) Values.

Images	Proposed Method	Wu et al. [20]	Peng et al. [32]
Barbara	52.07	46.89	29.30
Lena	47.79	45.33	32.96

Similarly scaling and translation attacks are also checked and the corresponding PSNR values and NCC values are given in Table 1 and Table 2. PSNR values of the proposed method is Compared with Wu et al.[20] & Peng et al.[32]. The obtained numerical results and comparisons are given in Table 3. From the results, it is inferred that higher PSNR values for the proposed method over the other two methods.

5. Conclusion

In this paper, a novel and robust method for calculation of scaling and embedding factors is proposed using Bhattacharya distance and Kurtosis. The calculated scaling and embedding factors are utilized in wavelet domain for invisible watermarking. The process is robust and efficient which is evident from the experimental results. From the results, it is evident that the watermarked image resembles the cover image without any loss of detail between cover

image and watermarked image. The PSNR values are in the acceptable range indicating the similarity of the watermarked image with the cover image. Watermark is extracted from the watermarked image on various attacks. NCC values resemble the similarity matching of the extracted watermark with the original watermark. The proposed method withstands all the image and signal processing attacks.

References

1. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.. *Digital watermarking and steganography*. Morgan Kaufmann; 2007.
2. You, X., Du, L., Cheung, Y.m., Chen, Q.. A blind watermarking scheme using new nontensor product wavelet filter banks. *Image Processing, IEEE Transactions on* 2010;**19**(12):3271–3284.
3. Deng, C., Gao, X.B., Tao, D.C., Li, X.L.. Digital watermarking in image affine co-variant regions. In: *Machine Learning and Cybernetics, 2007 International Conference on*; vol. 4. IEEE; 2007, p. 2125–2130.
4. Deng, C., Gao, X., Li, X., Tao, D.. Invariant image watermarking based on local feature regions. In: *Cyberworlds, 2008 International Conference on*. IEEE; 2008, p. 6–10.
5. Deng, C., Gao, X., Tao, D., Li, X.. Geometrically invariant watermarking using affine covariant regions. In: *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*. IEEE; 2008, p. 413–416.
6. Li, X.. Watermarking in secure image retrieval. *Pattern Recognition Letters* 2003;**24**(14):2431–2434.
7. Nikolaidis, N., Pitas, I.. Robust image watermarking in the spatial domain. *Signal processing* 1998;**66**(3):385–403.
8. Bruyndonckx, O., Quisquater, J.J., Macq, B.. Spatial method for copyright labeling of digital images. *Proc IEEE Nonlinear Signal and Image Processing* 1995;:456–459.
9. Huang, J., Shi, Y.Q., Shi, Y.. Embedding image watermarks in dc components. *Circuits and Systems for Video Technology, IEEE Transactions on* 2000;**10**(6):974–979.
10. Lin, S.D., Chen, C.F.. A robust dct-based watermarking for copyright protection. *Consumer Electronics, IEEE Transactions on* 2000; **46**(3):415–421.
11. Mishra, A., Agarwal, C., Sharma, A., Bedi, P.. Optimized gray-scale image watermarking using dwt–svd and firefly algorithm. *Expert Systems with Applications* 2014;**41**(17):7858–7867.
12. Petitcolas, F.A., Anderson, R.J., Kuhn, M.G.. Attacks on copyright marking systems. In: *Information Hiding*. Springer; 1998, p. 218–238.
13. Abdallah, H.A., Ghazy, R.A., Kasban, H., Faragallah, O.S., Shaalan, A.A., Hadhoud, M.M., et al. Homomorphic image watermarking with a singular value decomposition algorithm. *Information Processing &Management* 2014;**50**(6):909–923.
14. Shih, F.Y.. *Digital watermarking and steganography: fundamentals and techniques*. CRC Press; 2007.
15. Huang, X., Zhao, S.. An adaptive digital image watermarking algorithm based on morphological haar wavelet transform. *Physics Procedia* 2012;**25**:568–575.
16. LIU, L., CAO, T., LU, Y., ZHANG, H.. Analysis on the weighting factor of wavelet-based watermarking scheme? *Journal of Computational Information Systems* 2012;**8**(10):4285–4292.
17. Qi, X., Xin, X.. A quantization-based semi-fragile watermarking scheme for image content authentication. *Journal of visual communication and image representation* 2011;**22**(2):187–200.
18. Lin, T.C., Lin, C.M.. Wavelet-based copyright-protection scheme for digital images based on local features. *Information Sciences* 2009; **179**(19):3349–3358.
19. Nasir, I., Khelifi, F., Jiang, J., Ipson, S.. Robust image watermarking via geometrically invariant feature points and image normalisation. *Image Processing, IET* 2012;**6**(4):354–363.
20. Wu, H.T., Huang, J.. Reversible image watermarking on prediction errors by efficient histogram modification. *Signal Processing* 2012; **92**(12):3000–3009.
21. Lagzian, S., Soryani, M., Fathy, M.. A new robust watermarking scheme based on rdwt-svd. *International Journal of Intelligent Information Processing* 2011;**2**(1):22–29.
22. Li, Q., Yuan, C., Zhong, Y.Z.. Adaptive dwt-svd domain image watermarking using human visual model. In: *Advanced Communication Technology, The 9th International Conference on*; vol. 3. IEEE; 2007, p. 1947–1951.
23. Su, Q., Niu, Y., Wang, G., Jia, S., Yue, J.. Color image blind watermarking scheme based on qr decomposition. *Signal Processing* 2014; **94**:219–235.
24. Dawei, Z., Guanrong, C., Wenbo, L.. A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons & Fractals* 2004; **22**(1):47–54.
25. Falkowski, B.. Forward and inverse transformations between haar wavelet and arithmetic functions. *Electronics Letters* 1998;**34**(11):1084–1085.
26. Bhattacharyya, A.. On a measure of divergence between two multinomial populations. *Sankhy¯a: The Indian Journal of Statistics* 1946; :401–406.
27. Khotanzad, A., Bouarfa, A.. Image segmentation by a parallel, non-parametric histogram based clustering algorithm. *Pattern Recognition* 1990;**23**(9):961–973.
28. Choi, E., Lee, C.. Feature extraction based on the bhattacharyya distance. *Pattern Recognition* 2003;**36**(8):1703–1709.
29. Dodge, Y., Cox, D., Commenges, D., Solomon, P.J., Wilson, S., et al. *The Oxford dictionary of statistical terms*. Oxford University Press; 2003.
30. Li, D., Mersereau, R.M., Simske, S.. Blur identification based on kurtosis minimization. In: *Image Processing, 2005. ICIP 2005. IEEE International Conference on*; vol. 1. IEEE; 2005, p. I–905.
31. Huynh-Thu, Q., Ghanbari, M.. Scope of validity of psnr in image/video quality assessment. *Electronics letters* 2008;**44**(13):800–801.
32. Peng, F., Li, X., Yang, B.. Adaptive reversible data hiding scheme based on integer transform. *Signal Processing* 2012;**92**(1):54–62.