http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (1): 207-212, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.207.212

Multipurpose Perceptual Image Hashing Based on Block Truncation Coding

[1]Mei-Lei Lv and [2]Zhe-Ming Lu
[1]Department of Information and Electrical Engineering, Quzhou College, Quzhou 324000, China
[2]School of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China

Abstract: This study presents a new multipurpose image hashing scheme based on Block Truncation Coding (BTC). Vector Quantization (VQ) and BTC are both block-based lossy image compression techniques for gray-level images, but BTC can maintain the mean and standard deviation after compression. In our scheme, the original gray-level image is first partitioned into non-overlapping small blocks. BTC is then performed on each block to yield two mean values, i.e., a lower mean and a higher mean, as well as a bit plane. The relationship between two mean values are utilized to generate the intermediate binary image for copyright protection, while the number of '1's in the bit plane is compared with a threshold to generate the intermediate binary image for content authentication. Finally, the authentication mark and permuted copyright logo are respectively XOR-ed with the two intermediate binary images to obtain final authentication and protection fingerprints. Because BTC is a fast encoding scheme, our proposed method is therefore with lower complexity compared to VQ-based multipurpose image hashing schemes. Experimental results demonstrate the effectiveness and efficiency of the proposed scheme.

Key words: Perceptual image hashing, hash values, copyright protection, content authentication, block truncation coding

INTRODUCTION

The rapid growth of multimedia and Internet technologies has produced huge amount of audiovisual information in the digital format, resulting in information explosion and several serious issues. The first issue is how to protect intellectual property rights since digital multimedia can be losslessly copied and distributed over Internet. Copyright protection of digital images is defined as the process of proving the intellectual property rights to a court of law against the unauthorized reproduction, processing, transformation or broadcasting of a digital image (Herrigel *et al*., 1998). The second issue is how to authenticate the content of digital multimedia as it is easy to modify and forge multimedia data by widely available editing tools. The ability to detect changes in digital multimedia has been very important for many applications, content authentication has therefore been one of the most important issues in the digital world (Lv *et al*., 2007). The third issue is how to efficiently search desired multimedia content from the huge multimedia database and therefore content-based retrieval has been an interesting and rapid developing research area since the 1990's. In general, techniques for content authentication and copyright protection can be classified into three categories: digital signature based, watermark based (Fiaidhi and Mohammed, 2003; Khan *et al*., 2008; Lu and Li, 2006; Lu *et al*., 2000, 2003, 2005; Lu and Sun, 2000; Qureshi and Tao, 2006) and perceptual hash based (Dittmann *et al*., 1999; Lei *et al*., 2010; Lu and Liao, 2003; Lv and Lu, 2011; Monga *et al*., 2006; Monga and Evans, 2006; Monga and Mhack, 2007; Venkatesan *et al*., 2000; Yu *et al*., 2010; Yu and Lu, 2009). A digital signature is a mathematical scheme used to demonstrate the authenticity of a digital message or document. Similar to handwritten signatures, digital signatures must fulfill the following characteristics: (1) they should be unforgeable; (2) recipients must be able to verify them; (3) signers must be unable to repudiate them later. In addition, digital signatures cannot be constant and must be a function of the entire document it signs. Digital watermarking is the process of embedding watermark into digital multimedia such that the watermark can be extracted or detected later for many purposes such as copy protection and content authentication. Digital watermarking has been an active and important research subject and development and commercialization of watermarking techniques is being deemed necessary to help address many challenges faced by the rapid proliferation of digital content. Perceptual image hashing is an effective technique for image indexing, watermarking and content authentication. A perceptual hash is a hash function designed for multimedia contents. Perceptual

Corresponding Author: Zhe-Ming Lu, School of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China
Tel/Fax: +86-571-87951589

hash functions use fingerprinting techniques with cryptosystem-like constraints. The properties of a perceptual hash function are: easiness of computation, weak collision resistance and a fixed output bit length called perceptual digest. A small content change yields a small change of the perceptual digest. A large content change leads to a large change of the perceptual digest. An image hash function can be used as the robust feature of an image for image retrieval or copyright protection. An image hash function can be split into two stages. In the first step, a feature vector (or intermediate binary string) is extracted from the image to capture the important perceptual aspects of the image. In the second step, the feature vector (or the intermediate string) is securely transformed, compressed or quantized to obtain the final hash.

Most traditional image hashing methods are designed only for one purpose, e.g., content authentication or image retrieval. Technically, they can be roughly classified into following categories: statistics based (Venkatesan *et al*., 2000), relations based (Lu and Liao, 2003), low-level features based (Dittmann *et al*., 1999), feature points based (Monga and Evans, 2006), clustering based (Monga *et al*., 2006), non-negative matrix factorizations based (Monga and Mhack, 2007) and DCT-domain statistics based (Lei *et al*., 2010; Yu *et al*., 2010). Venkatesan *et al*. (2000). utilized randomized signal processing techniques to irreversibly transform an image into random binary strings that are robust against compression or geometric distortions. Lu and Liao (2003) proposed a structural digital signature for image authentication based on the fact that, in a subband wavelet decomposition, a parent node and its child nodes are uncorrelated, but they are statistically dependent. Dittman *et al*. (1999) proposed the application of feature points to perceptual hashing since they are sensitive to several perceptually insignificant modifications as well as content changing operations. Monga *et al*. (2006) proposed a wavelet based feature detector to extract significant image features based on the characteristics of the visual system. Monga *et al*. (2006) proposed the idea to divide image hashing into two steps, i.e., feature extraction (intermediate hash) followed by data clustering (final hash). For any perceptually significant feature extractor, they provided a polynomial-time heuristic clustering algorithm to automatically determine the final hash length needed with a specified distortion. Monga and Mhack (2007) proposed the non-negative matrix factorization (NMF) for image hashing, where they viewed an image as a matrix and the goal of hashing as a randomized dimensionality reduction operation that maintains the nature of the original image matrix against intentional attacks of guessing and forgery. Lei *et al*. (2010) proposed a new robust image hashing scheme based on the Discrete Cosine Transform (DCT) and Least-Squares Line (LSL) fitting of Discrete Wavelet Transform (DWT) coefficients. Recently, Yu *et al*. (2010) proposed a novel image hashing scheme based on the statistical invariance of DCT coefficients, where they extracted the invariant parameters with the modified ML principle.

To achieve multiple purposes of copyright protection and content authentication simultaneously, several multipurpose image hashing schemes (Yu and Lu, 2009; Lv and Lu, 2011) have been proposed recently. They proposed a multipurpose image hashing scheme based on DCT-VQ, where two index tables are used to generate two fingerprints for authentication and copyright protection respectively. Similarly, Lv and Lu (2011) proposed a multipurpose image hashing scheme based on Mean-Removed VQ. In this study, we propose a new multipurpose image hashing scheme based on Block Truncation Coding (BTC). The advantages lie in three aspects. First, it is multipurpose. Second, the copyright protection and authentication can be performed visually other than conventional image hashing schemes. Last, the proposed method is fast. The experimental results demonstrate the effectiveness and efficiency of the proposed scheme.

BTC-BASED MULTIPURPOSE IMAGE HASHING SCHEME

Block truncation coding: Block Truncation Coding (BTC) (Delp and Mitchell, 1979) is a simple and fast lossy image coding technique, which has the advantage of being easy to implement compared to transform coding and Vector Quantization (VQ) (Linde *et al*., 1980; Gray, 1984). Its simplicity, performance and channel error resisting capability make it attractive in the real-time image transmission. BTC is a one-bit adaptive moment-preserving quantizer that preserves certain statistical moments of small blocks of the input image in the quantized output. The original BTC method preserves the block mean and the block standard deviation. Lema and Mitchell present a simple and fast variant of BTC named Absolute Moment BTC (AMBTC) (Lema and Mitchell, 1984) that preserves the higher mean and the lower mean of a block, which can be expressed as follows:

In the original AMBTC method, the image is divided into blocks of size $k = 4\times4$. The mean value m of the pixels in each block x is taken as the one-bit quantizer threshold, i.e.,

$$m = \frac{1}{k}\sum_{i=1}^{k} x_i \quad (1)$$

The two output quantization level values are defined as:

$$L = \frac{1}{k-q}\sum_{x_i \le m} x_i \quad (2)$$

$$H = \frac{1}{q}\sum_{x_i > m} x_i \quad (3)$$

where, L and H denote the lower mean and the higher mean respectively and q stands for the number of pixels whose values are larger than the mean value. If q = 0, then each pixel in the block has the same value, so we can define H = L = m for this case. Then a two-level quantization is performed for the pixels in the block to form a bit plane so that '0' is stored for the pixels with values not larger than the mean and the rest of the pixels are presented by '1'. The image is re-constructed at the decoding phase from the bit plane by assigning the value L to '0' and H to '1'. Thus a compressed block appears as a triple (L, H, P), where L, H and P denote the lower mean, the higher mean and the bit plane, respectively. Figure 1 gives an example of encoding and decoding an image block based on AMBTC. The advantages of AMBTC lie in four aspects, i.e., it is very fast, it is easy to implement, it has low computational demands and it preserves the quality of the reconstructed image and retains the edges. Obviously, in the AMBTC, the lower mean and the higher mean are coded separately with 8 bits each and the bit plane needs 16 bits, so the bit rate of AMBTC is (8+8+16)/16 = 2bits/pixel.

Proposed image hashing scheme: Our BTC-based multipurpose image hashing scheme is depicted in Fig. 2. The main idea is to obtain two intermediate binary images according to the number of '1's in the bitplane and the relationship between the lower mean and high mean of each block and then perform the first XOR operation between one intermediate binary image and the permuted copyright logo and the second XOR operation between the other intermediate binary image and the authentication mark, respectively. The resulting two binary images can be finally served as the authentication and copyright fingerprints of the original gray-level image. Given the N×N sized input original image I_O, the N/4×N/4 sized input binary copyright logo I_L, the N/4×N/4 sized input binary authentication mark I_M, assume the output binary copyright fingerprint is denoted as F_C of size N/4×N/4 and the output binary authentication fingerprint is denoted as F_A of size N/4×N/4, then the whole multipurpose image hashing process can be illustrated as follows:

Step 1: Segment I_O into non-overlapping blocks B_{ij} of size 4×4, where i, j = 1, 2,..., N/4 and permute I_L with the key, Key0, to obtain the permuted logo I_L'.

Step 2: Calculate the lower mean L_{ij}, the higher mean H_{ij} and the bitplane P_{ij} for each block B_{ij} as shown in Eq.1-3 and Fig. 1.

Step 3: Map the mean matrices $L = \{L_{ij}\}$ and $H = \{H_{ij}\}$ to the binary image I_C based on the mapping function MF1, which can be described as follows:

$$I_{ij}^{C} = \begin{cases} 1 & H_{ij} - L_{ij} \ge T_0 \\ 0 & H_{ij} - L_{ij} < T_0 \end{cases} \quad (4)$$

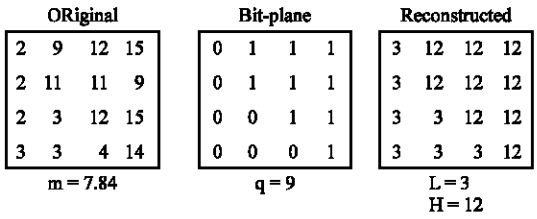

Fig. 1: AMBTC by the triple (L, H, P)

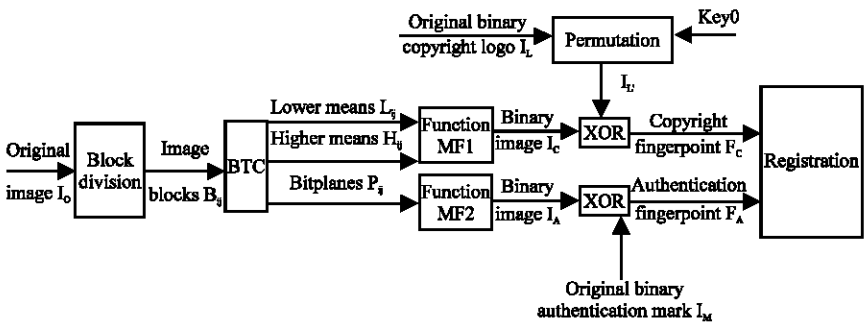

Fig. 2: BTC-based image hashing process

where, T_0 is a threshold and we set $T_0 = 20$ in this study.

Step 4: Map the bitplane sequence $\{P_{ij}\}$ to the binary image I_A based on the mapping function MF2, which can described as follows:

$$I_{ij}^{A} = \begin{cases} 1 & n_{ij} \geq T_1 \\ 0 & n_{ij} < T_1 \end{cases} \quad (5)$$

where, n_{ij} denotes the number of '1's in P_{ij} and T_1 is a threshold. This paper sets $T_1 = 8$.

Step 5: Perform the XOR operation between I_C and I_L' to obtain the final copyright fingerprint F_C. Similarly, perform the XOR operation between I_A and I_M to obtain the final authentication fingerprint F_A.

The authentication process: The authentication process is shown in Fig. 3, which can be briefly expressed as follows:

Inputs: The suspect image I_O', the registered copyright fingerprint F_C and the registered authentication fingerprint F_A, the original copyright logo I_L and the original authentication mark I_M.

Outputs: The binary decision result of the copyright existence and the binary decision result of the authenticity.

Step 1: Using the same steps 1-4 in the hashing process to obtain the binary images I_C' and I_A' from the suspect image I_O'.

Step 2: Perform the XOR operation between I_C' and F_C to obtain the suspect permuted logo I_{PL} and perform the XOR operation between I_A' and F_A to obtain the suspect mark I_M'. Then, the suspect permuted logo I_{PL} is further inversely permuted with the key, Key0, to obtain the suspect logo I_L'.

Step 3: Calculate the Hamming Similarity (i.e., the percentage of identical bits when comparing two binary strings) between the suspect logo I_L' and the original logo I_L. If the similarity is larger than the threshold TH_1, then the copyright exists; otherwise, the copyright doesn't exist. Similarly, compare the suspect mark I_M' with the original mark I_M. If the similarity is larger than the threshold TH_2, then the suspect image I_O' is authentic; otherwise, it is not authentic.

EXPERIMENTAL RESULTS

To demonstrate the effectiveness of our scheme, the 256 gray-level 512×512 Woman image is used as the test image, as shown in Fig. 4a. The Woman image is segmented into 16384 blocks of size 4×4 for BTC encoding. The original copyright logo, the permuted copyright logo and the original authentication mark are given in Fig. 5a-c, respectively. The two binary images of size 128×128 obtained with the mapping functions MF1 and MF2 are shown in Fig. 5d, e and the final obtained two fingerprints are shown in Fig. 5f, g. The copyright logo and authentication mark extracted from the image without any attack are shown in Fig. 5h, i. To check the robustness and authentication ability of our algorithm, we perform several attacks on the original image, including

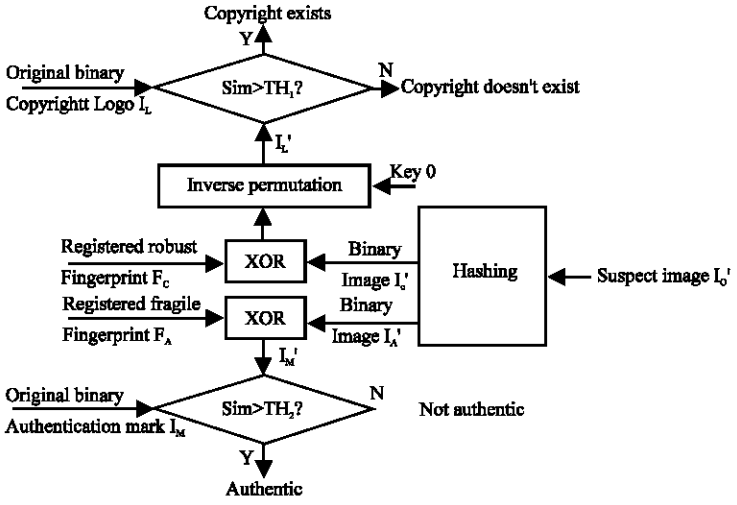

Fig. 3: The authentication process

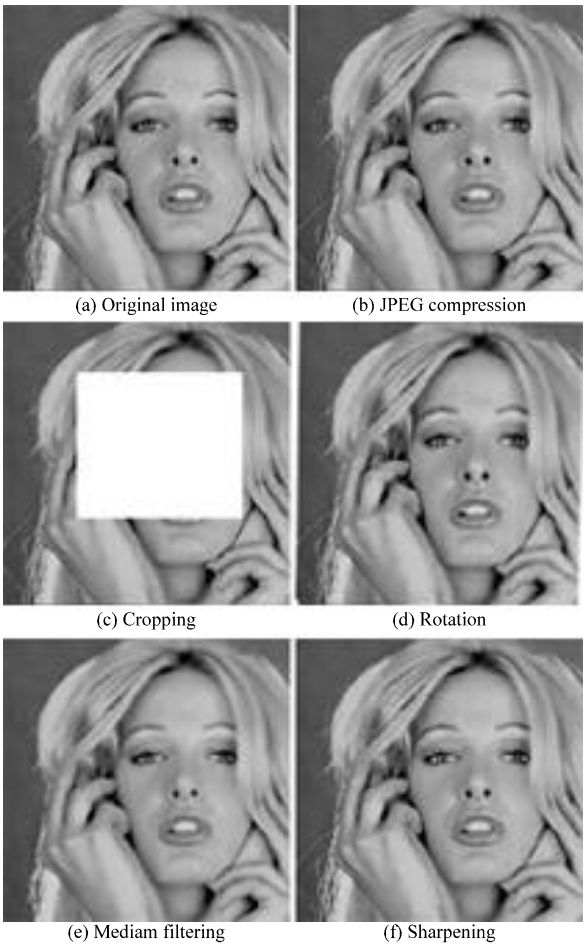

Fig. 4: The original and attacked Woman images

JPEG compression with QF = 50, cropping in the middle part of the image, rotation by angle 1°, median filtering with the radius of 3 pixels and sharpening. The attacked images are shown in Fig. 4b-f. The extracted logos and marks against these attacks are shown in Fig. 5 j-s. Here, the similarity between the extracted mark $M' = \{M'_{ij}\}$ and the original mark $M = \{M_{ij}\}$ is defined as follows:

$$Sim = \frac{1}{128\times128}\sum_{i=1}^{128}\sum_{j=1}^{128}|M'_{ij} - M_{ij}| \quad (6)$$

We also test the complexity of our scheme and the VQ based multipurpose image hashing scheme presented (Lv and Lu, 2011), we find that the complexity of our algorithm is only one tenth that of the algorithm by Lv and Lu (2011). The reason is that VQ should perform the time-consuming codeword search algorithm during

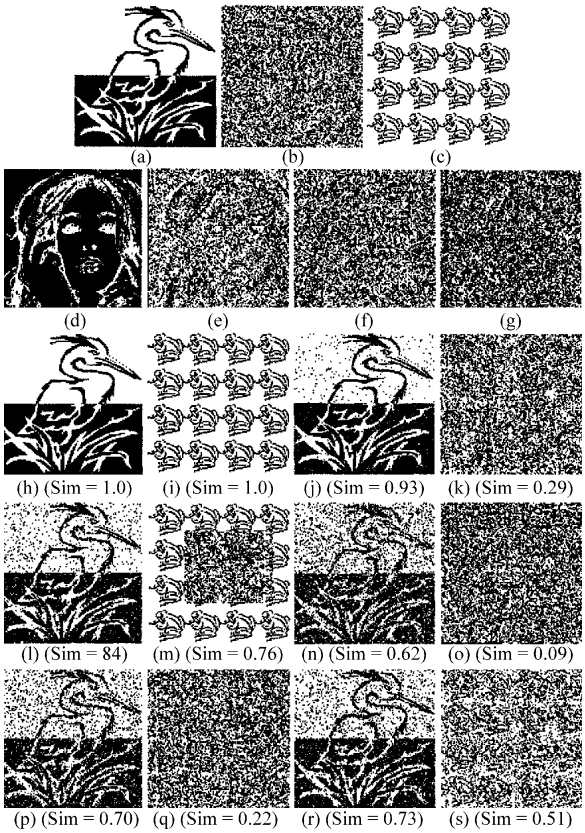

Fig. 5: Performance testing results; (a-c) Original copyright logo, permuted logo and original authentication mark; (d-g) Obtained binary image I_C, binary image I_A, copyright fingerprint and authentication fingerprint; (h-i) Extracted copyright logo and authentication mark without any attack; (j-s) Extracted 5 copyright logos and 5 authentication marks under 5 attacks, i.e., JPEG compression with QF = 50, cropping in the middle part of the image, rotation by angle 1°, median filtering with the radius of 3 pixels and sharpening, respectively

image encoding. From these results, we can easily see that the proposed method is both effective and efficient.

CONCLUSIONS

In this study, we propose a novel multipurpose perceptual image hashing scheme based on block truncation coding by performing different mapping functions on the number of '1's in the bitplane and the relationship between the lower mean and higher mean, respectively. In contrast with the traditional perceptual image hashing schemes, our scheme can be used to

protect copyright and authenticate image content simultaneously and the authentication process can be visually recognized. Compared with the multipurpose image hashing based on VQ, the proposed method is much faster. Experimental results show that the hashing process for copyright protection is robust against most common image processes and the hashing process for content authentication is fragile.

REFERENCES

Delp, E. and O. Mitchell, 1979. Image compression using block truncation coding. IEEE Trans. Commun., 27: 1335-1342.

Dittmann, J., A. Steinmetz and R. Steinmetz, 1999. Content based digital signature for motion picture authentication and content-fragile watermarking. Proc. IEEE Int. Conf. Multimedia Comput. Syst., 2: 209-213.

Fiaidhi, J.A.W. and S.M.A. Mohammed, 2003. Towards developing watermarking standards for collaborative e-learning systems. Inform. Technol. J., 2: 30-34.

Gray, R.M., 1984. Vector quantization. IEEE ASSP Magazine, 1: 4-29.

Herrigel, A., J.O. Ruanaidh, H. Petersen, S. Pereira and T. Pun, 1998. Secure copyright protection techniques for digital images. Lecture Notes Comput. Sci., 1525: 169-190.

Khan, A., X. Niu and Z. Yong, 2008. A robust framework for protecting computation results of mobile agents. Inform. Technol. J., 7: 24-31.

Lei, Y.Q., K.Y. Chau, Z.M. Lu and W.H. Ip, 2010. DCT-domain global feature and DWT-domain least-squares line fitting based local feature for robust image hashing. Int. J. Innovative Comput. Inform. Control, 6: 2513-2521.

Lema, M.D. and O.R. Mitchell, 1984. Absolute moment block truncation coding and its application to color images. IEEE Trans. Commun., 32: 1148-1157.

Linde, Y., A. Buzo and R.M. Gray, 1980. An algorithm for vector quantizer design. IEEE Trans. Commun., 28: 84-95.

Lu, C.S. and H.Y.M. Liao, 2003. Structural digital signature for image authentication: An incidental distortion resistant scheme. IEEE Trans. Multimedia, 5: 161-173.

Lu, Z.M. and S.H. Sun, 2000. Digital image watermarking technique based on vector quantisation. Electronics Lett., 36: 303-305.

Lu, Z.M., J.S. Pan and S.H. Sun, 2000. VQ-based digital image watermarking method. Electron. Lett., 36: 1201-1202.

Lu, Z.M., C.H. Liu, D.G. Xu and S.H. Sun, 2003. Semi-fragile image watermarking method based on index constrained vector quantisation. IEE Electron. Lett., 39: 35-36.

Lu, Z.M., D.G. Xu and S.H. Sun, 2005. Multipurpose image watermarking algorithm based on multistage vector quantization. IEEE Trans. Image Process., 14: 822-831.

Lu, Z.M. and S.Z. Li, 2006. Multipurpose watermarking algorithm for secret communication. Chinese J. Electronics, 15: 79-84.

Lv, W.L., Y. Guo and B. Luo, 2007. A novel image content authentication algorithm based on laplace spectra feature. Proceeding of the Chines Control Conference, July 26-31, Hunan, China, pp: 265-269.

Lv, M.L. and Z.M. Lu, 2011. An image hashing scheme based on mean-removed vector quantization for multiple purposes. Inform. Technol. J.

Monga, V. and B.L. Evans, 2006. Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs. Proc. IEEE Trans. Image, 15: 3452-3465.

Monga, V., A. Banerjee and B.L. Evans, 2006. A clustering based approach to perceptual image hashing. IEEE Trans. Inform. Forensics Sec., 1: 68-79.

Monga, V. and M.K. Mhcak, 2007. Robust and secure image hashing via non-negative matrix factorizations. IEEE Trans. Inform. Forensics Sec., 2: 376-390.

Qureshi, M.A. and R. Tao, 2006. A comprehensive analysis of digital watermarking. Inform. Technol. J., 5: 471-475.

Venkatesan, R., S.M. Koon, M.H. Jakubowski and P. Moulin, 2000. Robust image hashing. Proc. IEEE Conf. Image Process., 3: 664-666.

Yu, F.X. and Z.M. Lu, 2009. A DCT-VQ based multipurpose image hashing scheme for copyright protection and content authentication. Int. J. Innov. Comp. Inform. Control, 5: 2703-2710.

Yu, F.X., Y.Q. Lei, Y.G. Wang and Z.M. Lu, 2010. Robust image hashing based on statistical invariance of DCT coefficients. J. Inform. Hiding Multimedia Signal Process., 1: 294-300.