academicJournals

Vol. 8(11), pp. 447-455, 18 March, 2013
DOI 10.5897/SRE12.764
ISSN 1992-2248 © 2013 Academic Journals
http://www.academicjournals.org/SRE

Scientific Research and Essays

Full Length Research Paper

Image authentication using perceptual hashing

Kelsey Ramirez-Gutierrez, Mariko Nakano-Miyatake and Hector Perez-Meana*

ESIME Culhuacan, National Polytechnic Institute, Av. Santa Ana 1000, Col. San Francisco Culhuacan, 04430 México D.F. México.

Accepted 12 March, 2013

This paper presents a review of image authentication methods, based on the perceptual image hashing approach. Firstly we analyze two algorithms, which have the capability of determining if an image is authentic or not, even if it has suffered content preserving distortions such as compression, filtering and other signal processing operations; as well as some malicious modification such as geometric distortions. Next two modifications of these algorithms are analyzed which improve their performance by increasing their robustness against geometric distortions providing them also tamper detection capability. Finally two recently proposed algorithms with not only the tamper detection capability, but also with the capability of localizing tampered regions are described. Evaluation results are given to show the performance of these methods under analysis.

Key words: Image hashing, tamper detection and localization, image normalization.

INTRODUCTION

Currently the amount of information transmitted and shared through the internet is exponentially growing with the use of social networks, which have became an important way to transmit messages, opinions and share information about our life with many known people. However, this information sharing is not always secure because the transmitted images can be modified and may cause damage to any person or his family. This is because personal information can be tampered using software such as Photoshop®, CorelDraw®, or any other photo editor available in internet. Thus it is fundamental to develop mechanisms that allow an efficient image authentication.

The image authentication methods can be divided in active and passive methods, where the passive methods, also called image forensic methods, carried out the authentication without requiring previous information about the image to be authenticated, while the active methods extract some information of the image to be authenticated; or embed useful information on the image under analysis. In both cases the extracted or embedded information is used during the authentication (Lian et al., 2009). These active authentication methods can be classified in: watermarking-based and image hashing-based schemes. The first one inserts an imperceptible signal into the image to be authenticated to create a watermarked image, which may be a random signal or a signal related to the image to be authenticated. During the authentication process, the watermark is extracted from the watermarked image and used for authentication purposes (Ahmed and Siyal, 2006), or even to restore the tampered image. Some of these schemes have been proposed in the last few years (Ismali et al., 2010; Jin, 2010; Moskowitz et al., 2010). The hashing-based techniques, also called multimedia fingerprinting, take out a set of robust features from the image to be authenticated to create a hash code, which is stored or transmitted separately, to be used during the

*Corresponding author. E-mail: hmperezm@ipn, hperez.meana@gmail.com. Tel./Fax: +52-55-5656-2058.

authentication process. During the authentication process, this code is extracted from the suspicious image using the same method used to estimate the stored or transmitted authentication code. It is then compared with the code extracted from the suspicious image and if the difference between both codes is smaller than a given threshold, the image under analysis is considered as authentic; otherwise, it is determined as a tampered one. Among these schemes Zhen-kun et al. (2010) proposes a scheme which estimates a perceptual hash using a block-DCT and principal component analysis (PCA). Zhang et al. (2010) propose an image hashing approach with tampered region localization capability based on the estimation of a global and local perceptual image hashing. Swaminathan et al. (2006) developed a novel hashing algorithm where the Fourier transform of the image under analysis are modulated as random variables and its uncertainty quantified in terms of differential entropy to generate the perceptual image hashing. Evaluation results show that this algorithm is robust to content preserving operations such as compression, filtering and common geometric operations up to 10° rotation and 20% cropping; while keeping the capability of detecting malicious modifications that do not preserve the image content, such as cut and paste type editing. An image hashing technique based on virtual multiplicative watermark detection is proposed by Khelifi et al. (2010). Evaluation results using content preserving manipulations such as cropping, rotation and JPEG compression are provided to show the performances of proposed approach. Monga et al. (2007) propose a robust image hashing algorithm based on a non-negative matrix factorization method (NNF), in which the image is consider as a matrix and the image hashing as a dimensionally reduced code that retains the original image information keeping at the same time the capability of detecting malicious attacks. The NNF has several important properties that simultaneously allow the development of simple detection methods that are able to minimize the hashing detection probability error (Monga et al., 2007). Other important approach was proposed by Ahmed et al. (2010) using a secret key to modulate the image pixels, creating in such way a transformed feature space. Next a wavelet transform is applied to the resulting feature space to estimate the perceptual hashing code. This scheme accurately discriminates between content preserving distortions, such as JPEG compressing and filtering etc. and malicious attacks providing also tampered region location capability.

This paper presents a review of six recently proposed image authentication methods, based on perceptual hashing approach. Firstly two algorithms that are able to accurately authenticate an image even if it has suffered some content preserving distortion are analyzed. Next two recently proposed modifications of such algorithms are presented, that add to the original ones the tamper detection capability. Finally two recently proposed algorithms with not only the tamper detection capability, but also with the capacity of localizing the tampered regions are analyzed.

PERCEPTUAL IMAGE HASHING ALGORITHMS

Here four important perceptual hashing algorithms, are analyzed based on the discrete Radon transform, whose purpose is to authenticate a given image by comparing the stored perceptual hash code with that extracted from the image under analysis; even if it has suffered some kind of content preserving distortions such as compression, filtered and other signal processing operations, as well as some geometric distortions. Two recently proposed algorithms with the capacity of detecting, not only if the image under analysis has been tampered, but also to determine the tampered region are also analyzed.

Image hashing algorithms based on the discrete Radon transform

A very efficient image hashing algorithm, whose block diagram is shown in Figure 1, was proposed by Wu et al. (2009). In this scheme, firstly the two dimensional Radon transform (2D-RT) is applied to the image under analysis, to obtain $R(\gamma,\alpha)$, where γ and α are the radial and angle coordinates respectively. Next the RT, $R(\gamma,\alpha)$, is divided into 40X20 blocks to estimate a 40X20 matrix whose *(k,j).th* element corresponds to the mean value of the (j,k)-th block. Next the first level decomposition of 1D-Haar Wavelet Transform of each column of this matrix is calculated, keeping only the high frequency coefficients, to obtain a 20X20 matrix. Finally the 2D-FFT of this matrix is calculated keeping only the real components which, in the authentication stage, are compared with the stored or transmitted original perceptual hash. This comparison is done taking in account a threshold value which is defined in terms of BER (Bit Error Rate); which is given by the number of erroneous bits divided by the total number of bits.

Another efficient image hashing algorithm based on the Radon transform, whose block diagram is shown in Figure 2, was proposed by the Seo' et al. (2004). In it, firstly the 2D-RT of the image to be authenticated is obtained and then the normalized auto-correlation of each radial projection is calculated. Next the Log-mapping and interpolation operations are applied. Later the 2D FFT of the resulting matrix is estimated keeping only the 21X21 lowest frequency elements. The magnitude and phase of these elements become the entry of a first order 2D Filter whose coefficients are F(0,0)=F(1,1)=-1 and F(0,1)=F(1,0)=1. Finally the XOR operation of the resulting 20X20 elements from the phase and magnitude is computed, whose result is the hash

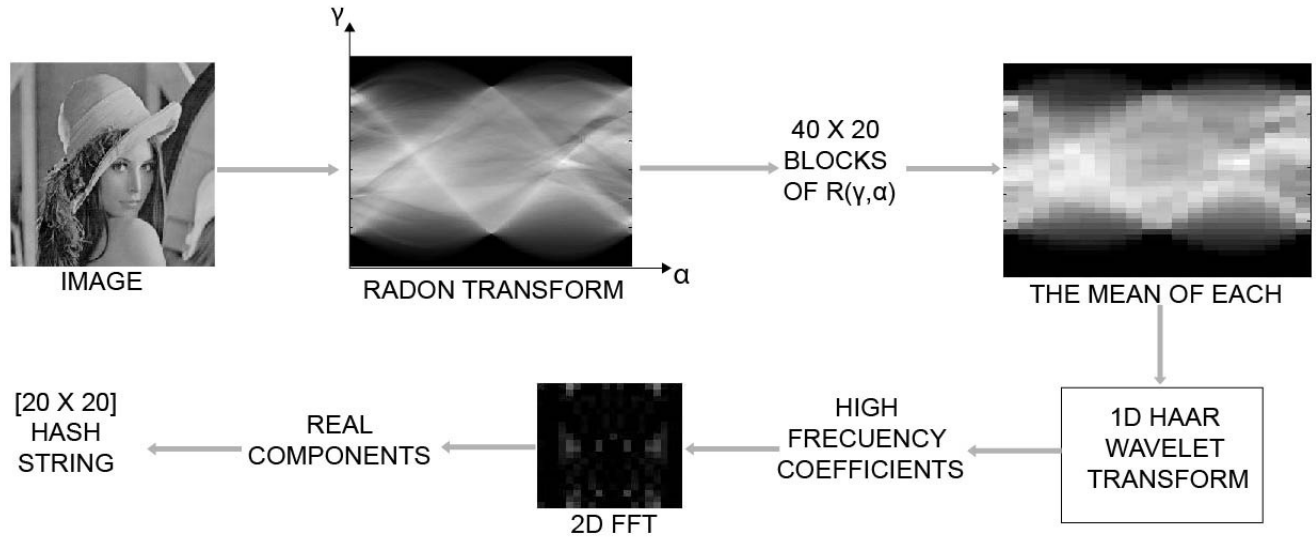


Figure 1. Block diagram of Wu et al. (2009) algorithm.

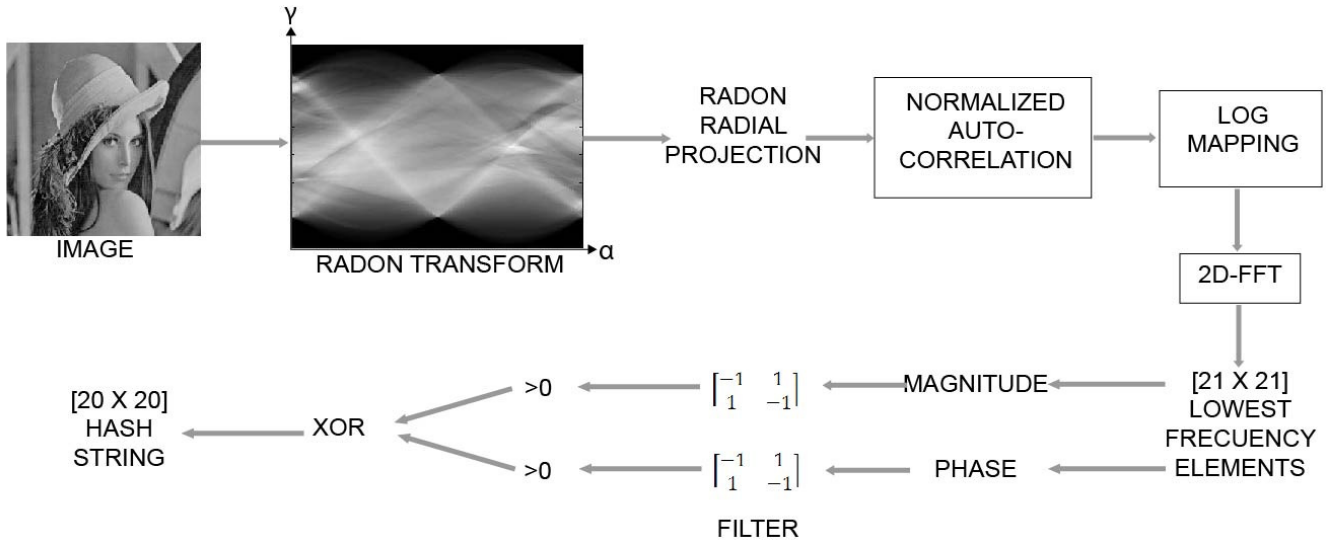


Figure 2. Block diagram of Seo et al. (2004) algorithm.

string of 400 elements.

These algorithms performs fairly well when the image be authenticated suffer some distortion due to standard signal processing operations such as filtering, compression and noise addition, etc. However their performance degrades when the image is geometrically distorted. To improve the performance of Wu et al. (2009) and Seo et al. (2004) algorithms under geometric distortions, Ramirez et al. (2012) improved the above mentioned algorithms inserting an image normalization preprocessing stage. As a result the modified algorithms provides better performance than Seo et al. (2004) and Wu et al. (2009) schemes under geometric distortions providing them also a tamper detection capability.

Perceptual image hashing algorithms for image tamper detection and localization

The image hashing algorithms described in the previous "image hashing algorithms based on the discrete Radon transform" performs fairly well when they are required to determine if the image is that supposed to be, however their performance considerable degrades when they are

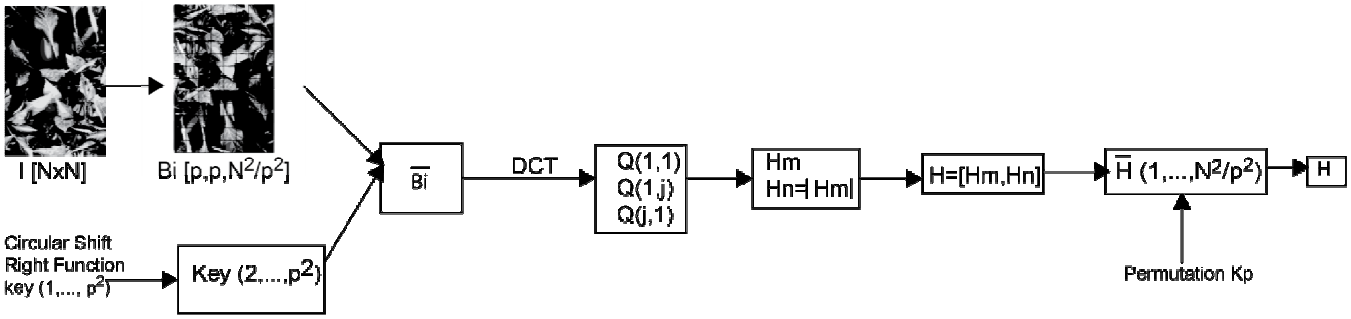


Figure 3. Block diagram of image hashing scheme proposed by Ahmed et al. (2009) based on the DCT.

required to detect a tampered image, besides that they have not the capability of locating the tampered regions. Because it is important that the algorithm, besides that it can detect if an image has been tampered, be also able to determine where it has been altered, we now analyze two algorithms that satisfies this requirement in a very accurate way.

Image hashing with tamper detection and localization capability based on DCT

Ahmed and Siyal (2006), propose an efficient perceptual hashing scheme with tamper detection capability, shown in Figure 3, which can be summarized as follows: Firstly the input image I of *NXN* pixels is divided into (N^2/P^2) non-overlapping blocks of *PXP* pixels. Assume that $B_i(x,y)$ denotes the gray value of a pixel at the spatial location (x,y) of the *i-th* block and select a random key with unique integer entries, $k_i(w)$,$w=1,2,3,\ldots P^2$. Next, using $k_i(w)$ obtain P^2-1 keys as follows

$$K_i(w) = C\left(K_{i-1}(w)\right), \quad i = 2,..., P^2 \tag{1}$$

Where $C(\bullet)$ denotes the circular shift right function.

Using the estimated $K_i(w)$ given by (1), a random intensity transformation is applied to each block $B_i(x,y)$ which is given by

$$\overline{B}_i(x,y) = \sqrt{\left(B_i(x,y) + L\right)^2 \alpha K_i(w)} \tag{2}$$

where $1 \le x \le P, \quad 1 \le y \le P, \quad 1 \le w \le P^2$ and L, S and α are constants. Subsequently an intermediate hash is estimates with the vectors H_{Mi}, H_{Ni} as follows

$$\overline{H}(I) = \{(H_{M1}, H_{N1}), (H_{M1}, H_{N1}), \ldots, (H_{MZ}, H_{NZ})\} \tag{3}$$

$$H_{Mi} = Q_i(1,1) + \sum_{j=1}^{8} Q_i(1,j) + \sum_{k=2}^{8} Q_i(k,1), \tag{4}$$

$$H_{Ni} = \left| Q_i(1,1) + \sum_{j=1}^{8} Q_i(1,j) + \sum_{k=2}^{8} Q_i(k,1) \right|, \tag{5}$$

where $z = (N/P)^2$ and $Q_i(j,k)$ is the (j,k)-th DCT coefficient of *i-th* block, $\overline{B}_i$. Next using the intermediate Hash function, $\overline{H}(I)$ the perceptual hash is estimated by permuting the entries $\overline{H}(I)$ using another secret key k_p, as follows

$$H(I) = permute^{K_p}\left(\overline{H}(I)\right) \tag{6}$$

Image authentication

During the authentication process, the received image $\hat{I}$ is processed in the same way described above to obtain the estimated perceptual hash

$$\hat{H}(I) = \{(\hat{H}_{M1}, \hat{H}_{N1}), (\hat{H}_{M1}, \hat{H}_{N1}), \ldots, (\hat{H}_{MZ}, \hat{H}_{NZ})\} \tag{7}$$

The inverse permutation is then applied to the stored of transmitted perceptual hash $H(I)$, using the same users key, used for obtaining the intermediate hash $\overline{H}(I)$ as follows

$$\overline{H}(I) = Inverse - permutation^{K_p}\left(H(I)\right) \tag{8}$$

Next the difference between the stored and extracted perceptual hash is computed

$$D_{Mi} = \left| H_{Mi} - \hat{H}_{Mi} \right| \tag{9}$$

$$D_{Ni} = \left| H_{Ni} - \hat{H}_{N_i} \right| \tag{10}$$

Finally if $D_{Mi} > \tau$ or $D_{Ni} > \tau$, where τ is a given

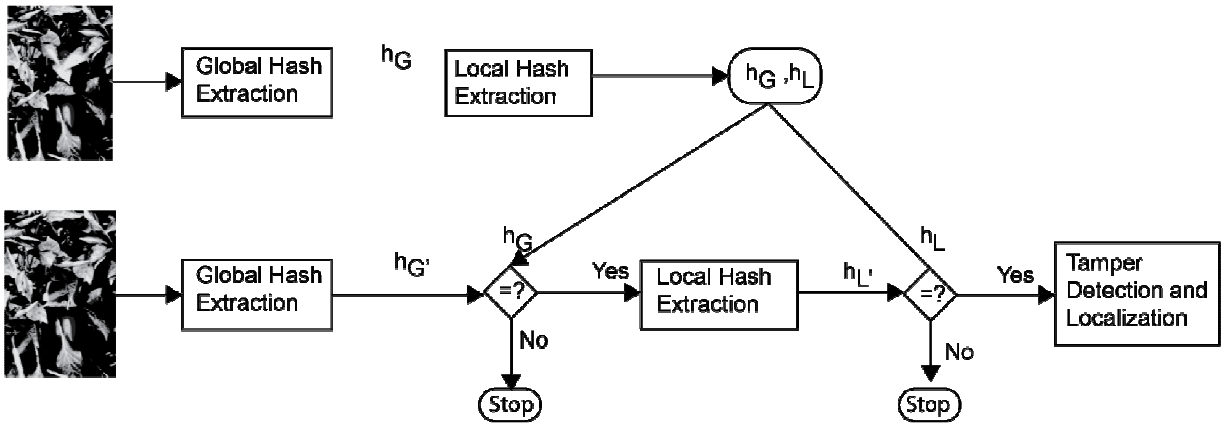


Figure 4. Block diagram of Liu et al. (2010) algorithm.

threshold, the block is considered a tampered.

Perceptual hashing based on image structure information

An efficient perceptual image hashing algorithm, with tamper detection capability, was proposed by Liu et al. (2010). This scheme, shown in Figure 4, firstly determines if the image under analysis was tampered by using a global perceptual hash; and then, if it is considered as tampered, the modified region is located by estimating a local Hash.

Global Hash estimation

For estimating the global Hash, firstly the image under analysis is segmented into *NG* rectangular regions, $B_0, B_1, \ldots, B_{N_G-1}$ whose size can be from 1/32 to 1/8 of the original image size. Next a feature vector $\lfloor d_0, d_1, d_2, \ldots, d_{N_G-1} \rfloor$ is estimated, where *di* is the i-th component is given by

$$d_i = L\left((B_{(i+1) \bmod N_G}\right) - L(b_i) \quad 1 < I < N_G, \tag{11}$$

Where

$$L(B_i) = \frac{1}{l_i + w_i} \sum_{c=x_i}^{x_i+l_i} \sum_{r=y_i}^{y_i+w_i} I(c,r) \tag{12}$$

Finally the feature vector $\lfloor d_0, d_1, d_2, \ldots, d_{N_G-1} \rfloor$ is quantized into a binary hash vector

$$h_G = \left[h_{G_0}, h_{G_1}, h_{G_2}, \ldots, h_{G_{N_G-1}} \right], \tag{13}$$

where

$$h_{G_i} = \begin{cases} 1, & d_i < 0 \\ 0 & d_i \geq 0 \end{cases}, \quad 0 \leq i < N_G \tag{14}$$

Local hash extraction

After determining that the image under analysis was tampered, it is very important to find the tampered region. To this end, each block B_i is divided into 4 sub-blocks D_{io}, D_{i1}, D_{i2}, D_{i3} and a hash vector of 6 bits is estimated as follows: Firstly estimate the mean value of the luminance of each sub-block

$$L(D_{ki}) = \frac{1}{l_k + w_k} \sum_{c=x_k}^{x_k+l_k} \sum_{r=y_k}^{y_k+w_k} B_i(c,r), \quad 0 \leq k \leq 3 \tag{15}$$

Then using such sub-blocks a features vector is estimated as follows

$$F_i = \left[(L_{i0} - L_{i1}), (L_{i0} - L_{i2}), (L_{k0} - L_{i3}), (L_{i1} - L_{i2}), (L_{i1} - L_{i3}), (L_{i2} - L_{i3}) \right] \tag{16}$$

whose components are then codified to form the 6 bits hash vector of block B_i as follows

$$h_{L_{5m+i}} = \begin{cases} 1, & f_{mi} < 0 \\ 0 & f_{mi} \geq 0 \end{cases}, \quad 0 \leq m < 5 \tag{17}$$

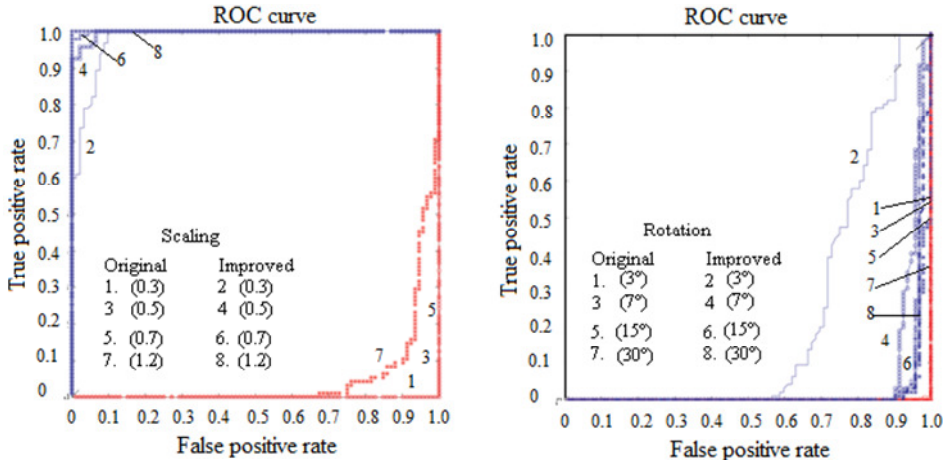
Finally, assuming that N_L blocks are selected to extract the local hash vector a $6N_L$ *bits,* the hash vector is generated as $h_L = \left[h_{L_0}, h_{L_1}, h_{L_2}, \ldots, h_{L_{6N_L-1}} \right]$

RESULTS

Table 1 presents the evaluation results obtained using the Wu et al. (2009) and Seo et al. (2004) Algorithms,

Table 1. Performance comparison using the normalized Hamming distance.

Parameter	Wu's Algorithm	Wu's Improved Algorithm	Seo's Algorithm	Seo's Improved Algorithm
NO ATTACK	0.0000	0.0000	0.0000	0.0000
JPEG 60%	0.0011	0.0228	0.0128	0.0594
JPEG 40%	0.0044	0.0403	0.0153	0.0872
GAUSSIAN FILTER	0.0044	0.0428	0.0389	0.0925
SHARPENING FILTER	0.0153	0.1047	0.1178	0.1944
MEDIAN FILTER	0.0061	0.0556	0.0461	0.0889
GAMMA 0.8	0.0156	0.1769	0.1217	0.2781
GAMMA 1.2	0.0153	0.1339	0.1047	0.2428
ROTATION 3º	0.3306	0.0367	0.4656	0.1119
ROTATION 7º	0.4308	0.0836	0.4914	0.1044
ROTATION 15º	0.4625	0.0231	0.4972	0.0883
ROTATION 30º	0.4842	0.0478	0.5017	0.1433
ROTATION 60º	0.4694	0.0836	0.5078	0.2283
ROTATION 90º	0.4331	0.1514	0.1622	0.1389
SCALING 0.3	0.2831	0.1556	0.4669	0.2600
SCALING 0.5	0.2725	0.0353	0.4578	0.1292
SCALING 0.7	0.1731	0.1117	0.3681	0.1622
SCALING 1.2º	0.3836	0.0450	0.2539	0.1047
SCALING 1.5	0.2758	0.0794	0.3781	0.0525
SHEARING X	0.4347	0.0300	0.4450	0.0769
SHEARING Y	0.4639	0.0347	0.5097	0.0992



(a) (b)

Figure 5. Tamper detection using the original and improved Seo et al. (2004) algorithm for tamper detection when the image under analysis, besides the tamper distortion, is modified by (a) different scaling factors, (b) several rotation angles.

together with two rescently proposed modification of such algorithms (Ramirez et al., 2012), when they are required to verify the autheticity of several content preserving and non-preserving distorted images. From these results it follows that, although Wu et al. (2009) and Seo et al. (2009) algorithms performs fairly good in many situations, their improved version performs better, specially when the image under analsys suffer content preserving distorsions such as common signal processing tasks such as filtering, compression geometric modifications and even non-preserving content attacks. This fact is also confirmed by the ROC curves shown in Figures 5 and 6.

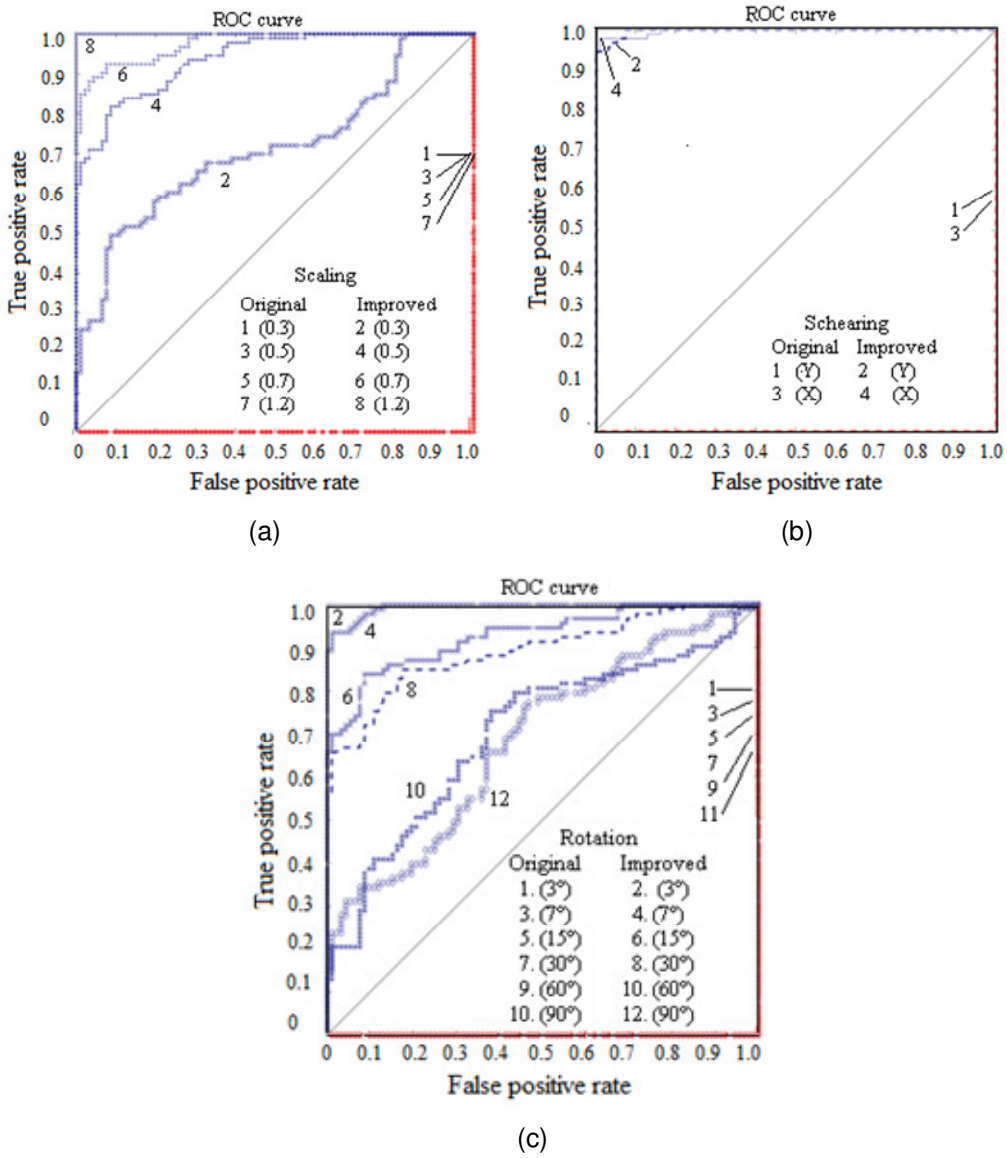


Figure 6. Tamper detection using the original and improved Wu at al. (2009) algorithm for tamper detection when the image under analysis, besides the tamper distortion, is modified by (a) different scaling factors, (b) shearing in x and y and several rotation angles.

Figure 7 shows the Ahmed and Siyal, (2006) algorithm tamper detection capability, where it is possible to observe that the tampered areas are correctly detected.

Figure 8 shows the performance of Liu et al. (2010) algorithm. This results show that the Liu et al. (2010) algorithm, is able of correctly identifying a forged image as well as detecting the tampered regions.

DISCUSSION

This paper presented a review of some recently proposed successful image hashing–based authentication algorithms. Firstly two perceptual hashing algorithms for image authentication, when the images under analysis are distorted by image content preserving operations are analyzed (Seo et al., 2004; Wu et al., 2010). These algorithms are robust in this situation, although their performance decreases when the images under analysis suffer geometric distortions. These algorithms were modified to improve their performance when the image under analysis suffer geometric distortion, as well as to provide them tamper detection capability (Ramirez et al., 2012). Because the tamper detection and localization tasks are also very important, two recently proposed algorihms were analyzed (Ahmed et al., 2010; Liu et al.,

Figure 7. Tamper detection and localization performance of Ahmed et al. (2009) algorithm.

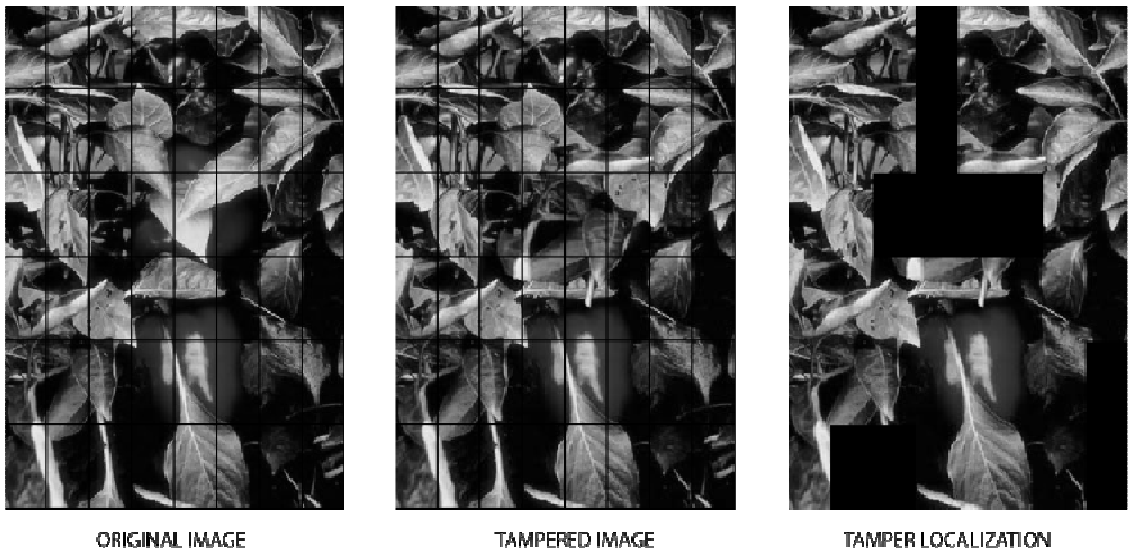


Figure 8. Tamper detection and localization with Liu et al. (2010) algorithm.

2010). Evaluation results show that both algorithms provide fairly good performance when they are required to perform tamper detection and localization tasks.

ACKNOWLEDGEMENTS

The authors thank the National Science and Technology Council of Mexico (CONACyT) and to The National Polytechnic Institute of Mexico for the financial support provided during the realization of this research.

REFERENCES

Ahmed F, Siyal MY (2006). A novel hashing scheme for image authentication. International Conference of Innovations in Information Technology, Dubai, pp. 1-5.

Ahmed F, Siyal MY, Abbas VU (2010). A secure and robust hash-based scheme for image authentication. Sig. Process. 90:1456-1470.

Lian SG, Kanellopoulos D, Ruffo G (2009). Recent advances in multimedia information system security. Informatica 33:3-24.

Liu Z, Li Q, Zhang H, Peng X (2010). An Image Structure Information based Robust Hash for Tamper Detection and Localization. Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Darmstadt, Germany, pp. 430-433.

Khelifi F (2010). Perceptual image hashing based on virtual

watermark detection. IEEE Trans. Image Process. 19(4):981-994.
Ismali I, El-Zoghdy S, Abdo A (2010). A novel technique for data hiding. Int. J. Comput. Appl. 32(1):1191-124.
Jin C (2010). Adaptive digital watermark system using soft computation. Int. J. Comput. Appl. 32(3):341-346.
Monga V, Kivac-Mihcak M (2007). Robust and secure image hashing via non-negative matrix factorization. IEEE Trans. Info. Forens. Secur. 2(3):376-390.
Moskowitz I, Ahmed F, Lafferty P (2010). Information theoretic effects of JPEG compression on image steganography. Int. J. Comput. Appl. 32(2):129-140.
Ramirez-Gutierrez K, Nakano-Miyatake M, Perez-Meana H (2012). Improvement of Radon Transform-based Perceptual Hashing using Image Normalization. Int. J. Comput. Appl. 34(4):249-259.
Seo J, Haitsma J, Kalker T, Yoo C (2004). A robust image fingerprinting system using the radon transform. Elsevier, Sig. Process.: Image Commun. 19:325-339.
SWaminathan W, Mao Y, Wu M (2006). Robust and secure image hashing. IEEE Trans. Info. Forens. Secur. 1(2):215-230.
Wu D, Zhou X, Niu X (2009). A novel image hash algorithm resistant to print-scan. Sig. Process. 89:2415–2424.
Zhang Z, Yu Z, BaiNa S (2010). Detection of Composite Forged Image. International Conference on Computer Application and System Modeling (ICCASM), Taiyuan, China. pp. 572-576.
Zhen-kun W, Wei-zong Z, Ouyang J, Peng-fei L, Yi-hua D, Meng Z (2010). A Robust and discriminative image perceptual hash algorithm. Fourth International Conference on Genetic and Evolutionary Computing, Shenzhen, China, pp. 709-712.