Computer and Information Science; Vol. 14, No. 3; 2021
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Novel Approach for Robust Perceptual Image Hashing

Azhar Hadmi[1,2] & Awatif Rouijel[1,2]

[1] Higher Institute of Audiovisual and Film, Rabat, Morocco

[2] Institut National des Postes et Telecommunications, Lab. STRS, Rabat, Morocco

Correspondence: Azhar Hadmi, Higher Institute of Audiovisual and Film, Rabat, BP 10000, Avenue Allal Al Fassi, Morocco.

Received: April 28, 2021 Accepted: June 10, 2021 Online Published: July 5, 2021

doi:10.5539/cis.v14n3p38 URL: https://doi.org/10.5539/cis.v14n3p38

Abstract

Perceptual image hashing system generates a short signature called perceptual hash attached to an image before transmission and acts as side information for analyzing the trustworthiness of the received image. In this paper, we propose a novel approach to improve robustness for perceptual image hashing scheme for generating a perceptual hash that should be resistant to content-preserving manipulations, such as JPEG compression and Additive white Gaussian noise (AWGN) also should differentiate the maliciously tampered image and its original version. Our algorithm first constructs a robust image, derived from the original input by analyzing the stability of the extracted features and improving their robustness. From the robust image, which does perceptually resemble the original input, we further extract the final robust features. Next, robust features are suitably quantized allowing the generation of the final perceptual hash using the cryptographic hash function SHA1. The main idea of this paper is to transform the original image into a more robust one that allows the extraction of robust features. Generation of the robust image turns out be quite important since it introduces further robustness to the perceptual image hashing system. The paper can be seen as an attempt to propose a general methodology for more robust perceptual image hashing. The experimental results presented in this paper reveal that the proposed scheme offers good robustness against JPEG compression and Additive white Gaussian noise.

Keywords: perceptual image hashing, security, robustness, image malicious tempering detection, content authentication

1. Introduction

The widespread use of multimedia technology has made it relatively easy to manipulate and tamper visual data. In particular, digital image processing and image manipulations tools offer facilities to intentionally alter image content without leaving perceptual traces (Qureshi & Deriche, 2015). Therefore, there should be some mechanism to prove the authenticity of the image in question other than human vision. A simple way to authenticate digital data is to calculate the data hash using standard cryptographic hash functions like MD5 (Rivest, 1992) or SHA1 (National Institute of Standards and Technology [NIST], 1995) and form a digital signature. However, the direct use of cryptographic hash functions is designed to be strongly dependent on every single bit of the input data (Menezes, Oorschot, Vanstone & Rivest, 1997). This property of cryptographic hash functions is not suitable for multimedia data, since the carried information is mostly retained even when the multimedia data have undergone various content-preserving operations like for example compression or filtering. All the content-preserving manipulations change the bits of the multimedia data while leaving the image perception unaltered. Multimedia image authentication, therefore, requires techniques which not authenticate the digital representation of the visual data but its visual appearance. Perceptual image hashing schemes have been proposed as solutions to get over the above problems by establishing the "perceptual equality" of image content. Such schemes extract features from image and generate a hash value (usually just few bytes) based on those features. Perceptual hashes are expected to be able to survive on acceptable content-preserving manipulations and reject malicious manipulations. As an ideal image hashing scheme, visually similar images should have the same perceptual hashes (i.e., perceptual robustness) and visually distinct images should have totally different hashes (i.e., discrimination). Hence, perceptual image hashing should be resistant to content-preserving manipulations, such as JPEG compression and Additive white Gaussian noise, and also should differentiate the maliciously tampered image and its original version. A perceptual image hashing system is also expected to be secure. This means that is impossible to keep the same perceptual hash value for a given image when its perceptual/visually content is modified.

The performance of a perceptual image hashing system primarily consists of robustness, discrimination and security. Robustness means that the perceptual image hashing system always generates the same perceptual hash values for perceptually similar images. Discrimination means that different visually image inputs must result in totally different hash values. A perceptual image hashing system is secure when it is impossible for an adversary to keep the same perceptual hash value in case the image content is perceptually modified. To authenticate the received image, the receiver needs only to compare its hash value with the one of the original image since the reference image does not exist.

Based on the statistical analysis of the extracted features behavior (Hadmi, Puech, Ait Essaid, & Ait ouahman, 2011), we propose in this paper a novel approach for perceptual image hashing system for image authentication that simultaneously attempts to address these core issues. Unlike most existing schemes that only focus on extracting robust visual features to generate the final perceptual hash, we propose a new approach by enhancing the robustness of the extracted features. We propose to transform the original image into a robust one that allows the extraction of robust features to the quantization stage. Thus, after using the cryptographic hash function SHA1, the final robust and secure perceptual hashes are then generated.

Rest of the paper is organized as follows: in Section 2, we introduce an overview of perceptual image hashing schemes published in the literature. In Section 3, we present our proposed method to generate a robust perceptual hash. Section 4 presents experimental results and Section 5 concludes this paper with future directions.

2. Previous Work

In recent years, accompanying with the rapid development of the technique for digital signal processing, digital images have been indispensable in our daily life. Also, through many image editing software, it has become easy to create or modify images conveniently. This poses a serious problem in case a digital content is to be used as an evidence. To address this issue, perceptual hashing schemes have been proposed. Most of the existing perceptual hashing studies mainly focus on extracting robust visual features and then use them during authentication step. They believe that robustness is ensured by extracting a set of robust visual features that resist (or stay relatively constant) to content-preserving manipulations, and at the same time, should detect malicious manipulations that modify the image content, is the most important goal in perceptual image hashing framework. Since the selected robust visual features are usually publicly calculated, an adversary can adjust them maliciously to match that of another perceptually different image. In this case, the security of the perceptual image hashing scheme is threatened. Current schemes in literature can be classified into two categories. Some works focus on the nearest neighbor search and content-based image retrieval, such as (Wang, Kumar, & Chang, 2012; Kulis & Grauman, 2012; Gorisse, Cord, & Precioso, 2012; Liu, Wu, Yang, Zhuang, & Hauptmann, 2012; Song, Yang, Li, Huang, & Yang, 2014), others are hash methods used for image content authentication (Li, Lu, Zhu, & Niu, 2012; Lv & Wang, 2012; Zhao, Wang, Zhang, & Yao, 2013; Lin, Varodayan, & Girod, 2012). About the latter, according to the difference of extracted feature, existing methods in literature can be classified into three categories, global-feature-based methods, local-feature-based methods, and hybrid-feature-based methods. The Proposed method in (Zhang, Tang, & Li, 2007) is a block-based hash method that was generated via the statistical value of DCT coefficients of image block. The schemes proposed in (Lu & Lia, 2003); Sumalatha, Venkata, & Vijaya, 2012) are also block-based image hash methods. In these methods, hash codes were generated from the statistical feature of the DWT coefficients of image blocks. The scheme (Qin, Chen, Dong, & Zhang, 2016) integrated principal DCT coefficients of the sampled blocks and their corresponding position information to generate robust features. After the compression with dimensionality reduction for the concatenated features, the final image hash was obtained. An image hashing method by using the statistics of wavelet coefficients is presented in (Venkatesan, Koon, Jakubowski, & Moulin, 2000). The scheme in (Swaminathan, Mao, & Wu, 2006) was good at perceptual robustness toward several digital operations, including moderate geometric transform and filtering, however, its performance of discrimination was not good enough. A robust mesh-based hashing method is proposed in (Lu C. S., Hsu C. Y., Sun S. W. & Chang P. C. 2004) that aims at resisting more geometrical distortions by firstly, extracting robust mesh and secondly, extracting mesh-based robust hash and finally matching hash for similarity measurement. However, they still allow limited resistance to geometrical distortions.

Previous schemes considered the security of the system, i.e. the use of a crypto-compression stage to generate the finale perceptual hash. In (Sun & Chang, 2005), for example, the authors proposed to use an error correction coding (ECC). In (Fawad, Siyal, & Abbas, 2010), they proposed to send an additional information beside the perceptual hash in order to adjust contaminated extracted features during the image verification stage before performing quantization. The main disadvantage of such schemes is that they need to send or store additional information in order to correct errors of extracted features, which is too costly in storage space. In the perceptual image hashing field, the robustness and security of a perceptual image hashing system that generates a signature of a fixed length (just few bytes) are very important and must be taken seriously into account. To not wast the storage space and for more efficacity while preserving security, the system should send only the final perceptual hash to the receiver via a secure channel without sending any additional information.

3. Proposed Method

In this Section, we describe our proposed perceptual hashing scheme. Our aim is to develop a perceptual image hashing system that encompasses the two core components, *i.e.,* robustness and security obtained by the use of a crypto-compression function such as SHA1. To meet these requirements, a transformation of the original image into a robust one is presented. In previous work, a statistical analysis of the extracted features behavior under some attacks (Hadmi, Puech, Ait Essaid, & Ait ouahman, 2011). This analysis has motivated the presented approach. In Section 3.1, we give a description of how we generate the robust image and then we present in Section 3.2 the proposed perceptual image hashing system.

3.1 Robust Image Generation

Based on the idea adopted in (Puech, Montesinos, & Dumas 2002), we propose a new method to enhance the robustness of the extracted features used by SHA1 to generate the final hash of 160 bits. Since the exact values of pixels are insignificant in regard to the human vision system, we propose to modify the pixel values of the original image to generate a robust image to a tolerate changes modeled by the threshold, B. The proper selection of B defines the boundary between non-malicious distortion and malicious tampering. The procedure of robust image generation is (Fig. 1) as follows:

• **Step 1**: In the *Transformation stage T(.),* the input image undergoes spatial and/or frequency transformation to generate a transformed image allowing the extraction of the proper image features.

• **Step 2**: In the *Feature Extraction stage E(.)*, the image features are extracted from the transformed image to generate a continuous intermediate hash vector.

• **Step 3**: The distribution of the continuous intermediate hash issue from step 2 is calculated. This step allows us to get information about the distribution of the original features in order to locate those that are close to the quantization boundaries when the quantization step size Q is informed in the *Quantization stage*.

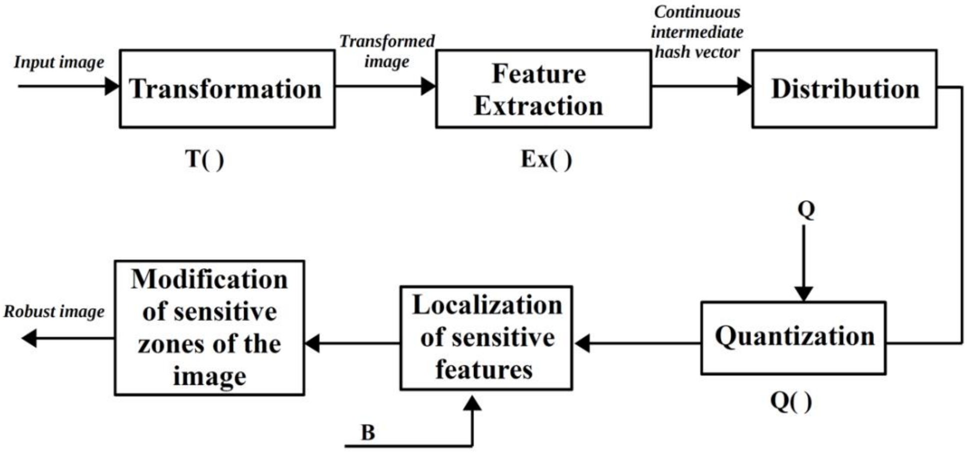

Input image
Transformation
T( )
Transformed image
Feature Extraction
Ex( )
Continuous intermediate hash vector
Distribution
Q
Quantization
Q( )
Localization of sensitive features
B
Modification of sensitive zones of the image
Robust image

Figure 1. Robust image generation

• **Step 4**: Assuming that the quantization step size Q verifies $Q > 2B$, B is the threshold that defines the boundary between non-malicious distortion and malicious tampering. We locate the original features points that beyond the dead zones $[nQ, nQ + B[$ and $](n + 1)Q - B, (n + 1)Q]$ in each quantization interval. We determine the spatial image sensitive zones that result each continuous feature in the dead zone. The modification of each sensitive zone in the original image is based on the change of pixels zone values. If the original continuous feature xo beyond the dead zone $[nQ, nQ + B[$ or $](n + 1)Q - B, (n + 1)Q]$, we increase or decrease the corresponding grey level of pixels zone in order to push xo in the confidence zone $[nQ + B, (n + 1)Q - B]$. The distances $d^+ = (nQ + B) - x_o$,when $x_o \in [nQ, nQ + B[$ or

$d^- = x_o - ((n+1)Q - B))$, when $x_o \in](n+1)Q - B, (n+1)Q]$ determine the number of pixels and the right ones to modify in each sensitive zone.

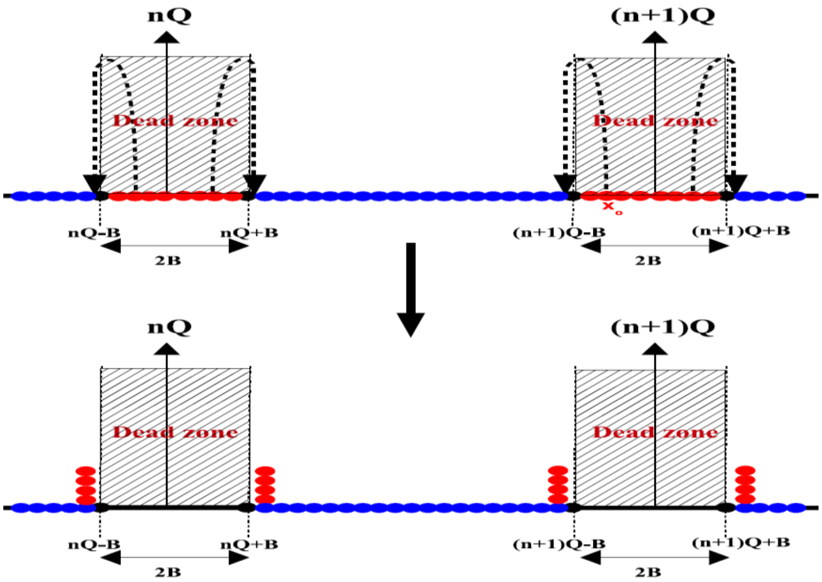


Figure 2. Localization and pushing away the features that are in the dead zones

• **Step 5**: When each sensitive zone of the original image is modified to have robust features, we finally generate the robust image that ensures the extraction of robust features. The robust image will be used as input image in the perceptual image hashing system to generate the final hash value.

The threshold B draws the boundary between robustness and security of the authentication system.

3.2 Robust Perceptual Image Hashing System

The proposed perceptual image hashing system contains a cryptographic hash function i.e. SHA1 to generate a final perceptual hash of 160 bits as shown in Fig. 3. In the *Transformation stage*, the robust image undergoes spatial and/or frequency transformation. In the *Feature Extraction stage*, a continuous intermediate hash vector is generated from the transformed image extracted features. The continuous values of this vector are then quantized in the *Quantization stage* to form an intermediate binary perceptual signature vector. At the end, this intermediate binary perceptual signature vector is compressed and encrypted into a short and a final perceptual hash at the *Crypto-compression stage*. By extracting the continuous intermediate hash vector from the robust image, we effectively increase robustness against attacks (JPEG compression and Additive white Gaussian noise).

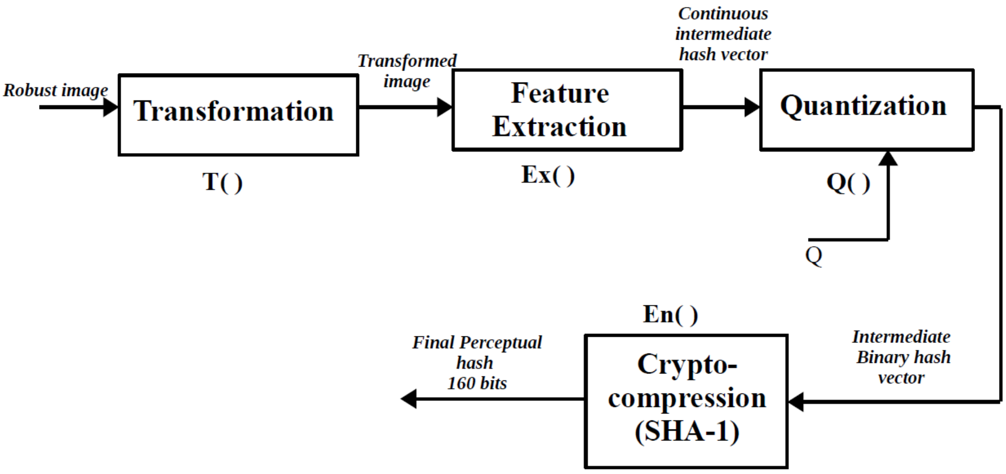

Robust image
Transformation
T( )
Transformed image
Feature Extraction
Ex( )
Continuous intermediate hash vector
Quantization
Q( )
Q
Intermediate Binary hash vector
En( )
Crypto-compression (SHA-1)
Final Perceptual hash 160 bits

Figure 3. Perceptual hashing system

During the authentication procedure, when the robust image undergoes content-preserving manipulations, the extracted features will not exceed the dead zones fixed by B. Thus, we get the same discrete hash vector as the original image during the *Quantization stage*, which makes the robustness of the perceptual hash guaranteed. When the changes that undergoes the robust image are significant (malicious attacks), the distorted features will exceed the dead zones even after B adjustment and drop in the neighboring quantization intervals. However, the final perceptual hash definitely will be changed, because the quantized values are changed.

4. Experimental Results

In this section, we present a number of experiments on which the proposed perceptual image hashing approach has been tested. The tests have been performed considering the image block mean features. The original input image I of size $N \times M$ pixels is split to non-overlapping blocks of size $p \times q$ pixels that we denote by $B_{i,j}$, where $1 \leq i \leq \frac{N}{p}$ and $1 \leq j \leq \frac{M}{q}$. Let $P_{m,n}$ denote the gray value of a pixel at spatial location (m, n) in the block $B_{i,j}$, where $1 \leq m \leq p$ and $1 \leq n \leq q$. The float mean value $m_{i,j} = \frac{1}{p \times q} \sum_{k=1}^{p} \sum_{l=1}^{q} P_{k,l}$ of each block $B_{i,j}$ is computed and stored in a one dimensional vector that we denote by $\boldsymbol{V_m(k)}$, where $k \in \{1, \ldots, \frac{N}{p} \times \frac{M}{q}\}$. Elements of $\boldsymbol{V_m(k)}$ present the continuous intermediate hash.

Generation of robust image in case of mean block features:

- When $m_{i,j} \in](n+1)Q - B, (n+1)Q]$, the pixels $P_{m,n}$ of the block $B_{i,j}$will be sorted in decreasing order. Let N_d be the number of pixels to modify in the block $B_{i,j}$.

N_d is given by the following formula:

$$\begin{aligned} N_d &= \lceil d^- \times (p \times q) \rceil \\ &= \lceil (m_{i,j} - ((n+1)Q - B)) \times (p \times q) \rceil \end{aligned} \tag{1}$$

where $\lceil . \rceil$ is ceiling function.

In case of $N_d \leq p \times q$, we select the N_d biggest pixel values in the block $B_{i,j}$ and we decrease their corresponding grey levels by 1, *i.e.* $P'_{m,n} = P_{m,n} - 1$, where $P_{m,n}$ is the new pixel value at the spatial location (m, n). When N_d is bigger than $p \times q$, we modify the N'_d selected biggest pixels values by more than one grey level, where N'_d is the new number of pixels to modify that satisfies $N'_d < p \times q$.

For example, if $2(p \times q) < N_d \leq 3(p \times q)$, the number of pixels to modify will be $N'_d = \frac{N_d}{3}$ and the N'_d new pixel values will be $P'_{m,n} = P_{m,n} - 3$

- When $m_{i,j} \in]nQ, nQ + B]$, the pixels $P_{m,n}$ of the block $B_{i,j}$will be sorted in increasing order. Let N_i be the number of pixels to modify in the block $B_{i,j}$.

N_i is given by the following formula:

$$\begin{aligned} N_i &= \lceil d^+ \times (p \times q) \rceil \\ &= \lceil ((nQ + B) - m_{i,j}) \times (p \times q) \rceil \end{aligned} \tag{2}$$

where $\lceil . \rceil$ is ceiling function.

In case of $N_i \leq p \times q$, we select the N_i smallest pixel values in the block $B_{i,j}$ and we increase their corresponding grey levels by1, i.e., $P'_{m,n} = P_{m,n} + 1$, where $P'_{m,n}$ is the new pixel value at the spatial location (m, n). When N_i is bigger than $p \times q$, we modify the N'_i selected smallest pixels values by more than one grey level, where N'_i is the new number of pixels to modify that satisfies $N'_i < p \times q$.. For example, if $p \times q < N_i \leq 2(p \times q)$, the number of the pixels to modify will be $N'_i = \frac{N_i}{2}$ and the N'_i new pixel values will be $P'_{m,n} = P_{m,n} + 2$.

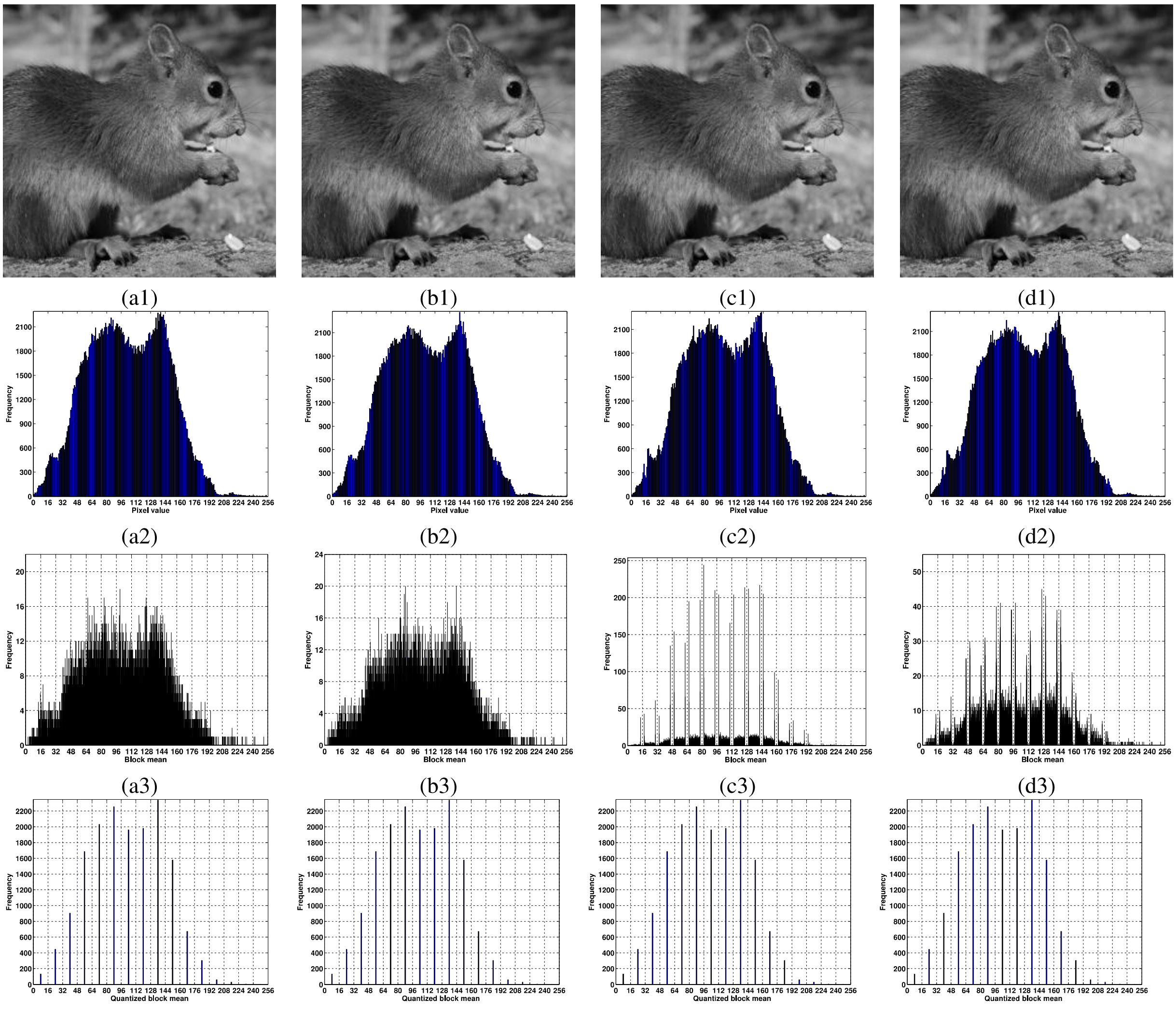
Finally, after modifying suitably all selected pixels by increasing or decreasing their corresponding grey levels, we guarantee that all later extracted features from the robust image belong the confidence zone $]nQ + B, (n+1)Q - B]$. We note that increasing B will increase the system's robustness while decreasing the robust image quality. Indeed, when B is high, the number of pixels N_d (Eq. 1) or N_i (Eq. 2) to modify is also high, which decrease the robust image quality in comparison to the original one.

Fig. 4 presents a comparison in term of robustness between the generation of a perceptual hash directly from the original image and the generation of a perceptual hash from the robust image in case of JPEG compression with a quality factor QF = 90.

Fig. 4.(a1) and 4.(b1) show the original image of size 512 × 512 and its JPEG compressed version with JPEG quality factor QF = 90, respectively. Fig. 4.(a2) and 4.(b2) show histograms of the original and its JPEG compressed version while Fig. 4.(a3) and 4.(b3) show distributions of the continuous intermediate hashes, in case of p = 4 and q = 4, of images in Fig. 4.(a1) and 4.(b1). After applying an uniform quantization with a quantization step size Q = 16, the intermediate binary perceptual hash of the JPEG compressed image (Fig. 4.(b4)) contains 1.18% erroneous quantized features to that of the original image (Fig. 4.(a4)), which will cause a false authentication during the crypto-compression stage. Fig. 4.(c1) shows the robust image generated from the original image (Fig. 4.(a1)) in case of B = 2. The distribution of the continuous intermediate hash of the robust image is shown in Fig. 4.(c3), where we can see that all the continuous features are taken away from the death zones in each quantization interval. When the JPEG compression with QF = 90 is applied to the robust image, we are sure that all elements of the continuous intermediate hash will not exceed each quantization interval death zones after the B = 2 adjustment, as shown in Fig. 4.(d3). This allow us, after the uniform quantization, to get two identical binary intermediate hashes of the robust image and its JPEG compressed version, as shown in Fig. 4.(c4) and Fig. 4.(d4). Thus, the JPEG compressed image (QF = 90) will be positively authenticated.

In case of an Additive white Gaussian noise, Fig. 5 presents a comparison in terms of robustness between the generation of a perceptual hash directly from the Gaussian noisy original image (Fig. 5(a)) and the generation of a perceptual hash from the robust Gaussian noisy image (B = 3) (Fig. 5(b)) in case of an Additive white Gaussian noise of a standard deviation σ = 3.

As observed in Fig. 5(a), when an Additive white Gaussian noise of standard deviation σ = 3 is applied, the Gaussian noisy image remains perceptually identical to the original image (Fig. 4.(a1)), but it causes changes in the extracted features distribution as we can see in Fig. 5(e). Thus, the intermediate binary perceptual hash of the Gaussian noisy image (Fig. 5(g)) contains 3.84% erroneous quantized features to that of the original image (Fig. 4.(a4)) which will cause a false authentication during the crypto-compression stage. When extracting features from the Gaussian noisy robust image (Fig. 5(b)), we get two identical binary intermediate hashes of the Gaussian noisy robust image (Fig. 5(h)) and the original image (Fig. 4.(a4)). Thus, the Gaussian noisy image (σ = 3) will positively be authenticated.



(a1) (b1) (c1) (d1)

(a2) (b2) (c2) (d2)

(a3) (b3) (c3) (d3)

(a4) (b4) (c4) (d4)

Figure 4. a1) Original image; b1) JPEG compressed image (QF=90) of the original image; c1) Robust Image (B=2) (PSNR = 51.49 db, SSIM = 0.998); d1) JPEG compressed image (QF=90) of the robust image; a2-d2) Histograms of the corresponding images; a3-d3) Distributions of the continuous intermediate hashes of the corresponding images; a4-d4) Distributions of the binary intermediate hashes (Q = 16) of the corresponding images (1.18% erroneous quantized features for image in b1) and 0% erroneous quantized features for image in d1)).

It is important to note that robustness characteristics vary from image to image. To explore this fact, we formed a database (BOSSBase v1.00 available on: http://agents.cz/boss/BOSSFinal/.) of 100 grayscale different images of size 512 × 512 pixels. Fig. 6 shows the percentage of correct perceptual hashes generated from the original images and the robust images in case of B = 4 and B = 6 as a function of the JPEG compression quality factor (QF). The original perceptual hashes are generated directly from the original images without compression. When we apply directly a JPEG compression with QF = 100, we have 0% of correct perceptual hashes. When we generate perceptual hashes from the robust image, we increase the robustness of the system, for example with QF = 100 and QF = 90, 100% of the extracted perceptual hashes are correct. Note that when increasing B the system robustness increases while decreasing the robust image quality (in term of PSNR), as shown in Fig. 7. Note also that the robust image keeps always good quality: PSNR = 43.08 db in case of B = 4 and PSNR = 38 db in case of B = 6.

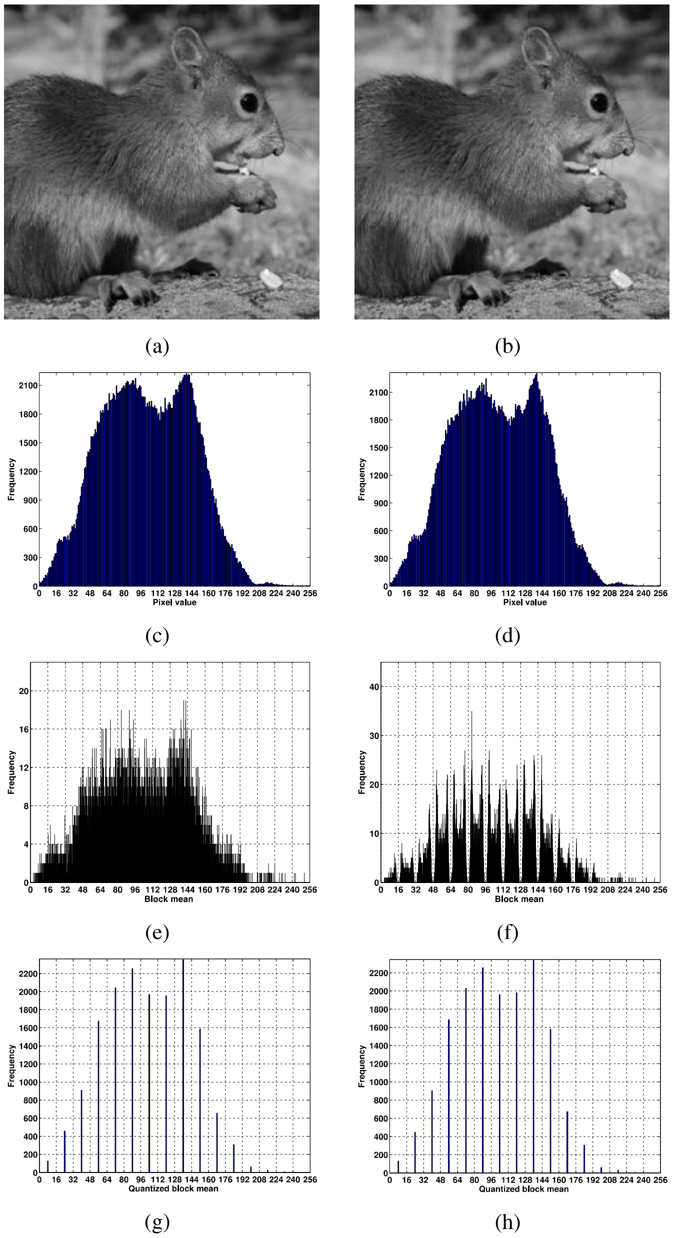


Figure 5. a) Gaussian noisy image (σ = 3), Robust Gaussian noisy image (B = 3); c) Histogram of the original image; d) Histogram of the Gaussian noisy image (σ = 3); e) Distribution of the continuous intermediate hash of the Gaussian noisy image; f) Distribution of the continuous intermediate hash of the robust Gaussian noisy image; g) Distribution of the binary intermediate hash (Q = 16) of the Gaussian noisy image (3.86% erroneous quantized features); h) Distribution of the binary intermediate hash (Q = 16) of the robust Gaussian noisy image (0% erroneous quantized features).

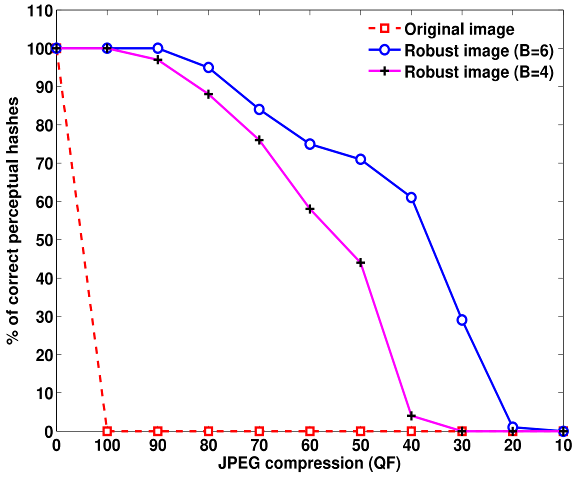


Figure 6. Percentage of correct perceptual hashes as a function of the JPEG compression (QF) and B

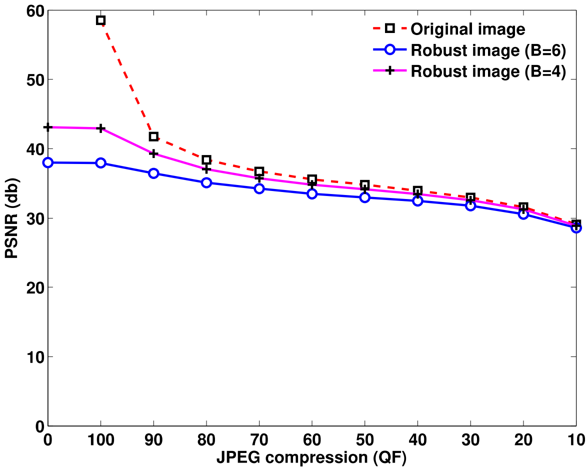


Figure 7. Comparison of PSNR between the original and robust compressed images as a function of the JPEG compression (QF) and B

5. Conclusion

In this paper, we have presented a new method for image perceptual hashing to generate a more robust perceptual hash. In our scheme, we construct a robust image allowing the extraction of robust features to desired content-preserving manipulations. The choice of the threshold B depends of the used method of features extraction, the applied quantization step size Q and the type of the content-preserving manipulation. In the experiment results, we presented our method for block mean features and we tested its robustness in case of JPEG compression. Our future research will explore other types of content-preserving manipulations and other methods of feature extraction.

References

Fawad, A., Siyal, M. Y., & Abbas, V. U. (2010). A secure and robust hash- based scheme for image authentication. *Signal Processing*, *90*, 1456-1470. https://doi.org/10.1016/j.sigpro.2009.05.024

Gorisse, D., Cord, M., & Precioso, F. (2012). Locality-sensitive hashing for Chi2 distance. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *34*(2), 402-409. https://doi.org/10.1109/TPAMI.2011.193

Hadmi, A., Puech, W., Ait, E. B., & Ait, O. A. (2011). Statistical analysis of the quantization stage of robust perceptual image hashing. *IEEE 3rd European Workshop on Visual Information Processing*, pp. 274-279. https://doi.org/10.1109/EuVIP.2011.6045509

Kulis, B., & Grauman, K. (2012). Kernelized locality-sensitive hashing. *IEEE Transactions Pattern Analysis Machine Intelligence, 34*(6), 1092-1104. https://doi.org/10.1109/TPAMI.2011.219

Li, Y., Lu, Z., Zhu, C., & Niu, X. (2012). Robust image hashing based on random gabor filtering and dithered lattice vector quantization. *IEEE Transactions on Image Processing, 21*(4), 1963-1980. https://doi.org/10.1109/TIP.2011.2171698

Lin, Y., Varodayan, D., & Girod, B. (2012). Authentication using distributed source coding. *IEEE Transactions on Image Processing, 21*(1), 273-283. https://doi.org/10.1109/ICIP.2008.4712453

Liu, Y., Wu, F., Yang, Y., Zhuang, Y., & Hauptmann, A. G. (2012). Spline regression hashing for fast image search. *IEEE Transactions on Image Processing, 21*(10), 4480-4491. https://doi.org/10.1109/TIP.2012.2207394

Lu, C. S. & Liao, H. Y. (2003). Structural digital signature for image authentication: an incidental distortion resistant scheme. *IEEE Transactions on Multimedia, 5*(2), 161-173. https://doi.org/10.1109/TMM.2003.811621

Lu, C. S., Hsu, C. Y., Sun, S. W., & Chang, P. C. (2004). Robust Mesh-based Hashing for Copy Detection and Tracing of Images. *IEEE International Conference on Multimedia and Expo (ICME).* https://doi.org/10.1109/ICME.2004.1394296

Lv, X. D., & Wang, Z. J. (2012). Perceptual image hashing based on shape contexts and local feature points. *IEEE Transactions on Information Forensics and Security, 7*(3) 1081-1093. https://doi.org/10.1109/TIFS.2012.2190594

Menezes, A. J., Oorschot, P. C. V., Vanstone, S. A., & Rivest, R. L. (1996). *Handbook of Applied Cryptography.* 1st edition Boca Raton, FL, USA: CRC Press, Inc.

Mihçak, M. K., & Venkatesan, R. (2001). A perceptual audio hashing algorithm: A tool for robust audio identification and information hiding. *Proceedings of the 4th International Workshop on Information Hiding. Springer-Verlag, 2001,* pp. 51-65.

National Institute of Standards and Technology (NIST). Secure Hash Standard (FIPS 180-1). April 1995. [Online]. Retrieved from http://csrc.nist.gov

Puech, W., Montesinos, P., & Dumas, M. (2002). Color image watermarking robust to jpeg compression. *1st European Conference on Color in Graphics, Image and Vision,* pp. 81-85. https://doi.org/10.1109/DESSERT.2018.8409206

Qin, C., Chen, X. Q., Dong, J., & Zhang, X. P. (2016). Perceptual image hashing with selective sampling for salient structure features. *Displays, 45,* 26-37. https://doi.org/10.1016/j.displa.2016.09.003

Qureshi, M. A., & Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. Signal Processing: *Image Communication, 39,* 46-74. https://doi.org/10.1016 /j.image.2015.08.008

Rivest R. L. (1992). The MD5 Message-Digest Algorithm, Internet Engineering Task Force (IETF). *Technical Report RFC 1321.*

Song, J., Yang, Y., Li, X., Huang, Z., & Yang, Y. (2014). Robust hashing with local models for approximate similarity search. *IEEE Transactions on Cybernetics, 44*(7), 1225-1236. https://doi.org/10.1109/TCYB.2013.2289351

Sumalatha, L., Venkata K. V., & Vijaya, K. V. (2012). Local content based image authentication for tamper localization. *International Journal of Image, Graphics and Signal Processing, 4*(9), 30-36. https://doi.org/10.5815 /IJIGSP.2012.09.05

Sun, Q., & Chang, S. F. (2005). A robust and secure media signature scheme for jpeg images. *VLSI Signal Processing, 41*(3), 305-317. https://doi.org/10.1007/s11265-005-4154-0

Swaminathan, A., Mao, Y., & Wu, M. (2006). Robust and secure image hashing. *IEEE Transactions on Information Forensics and Security, 1*(2), 215-230. https://doi.org/10.1109/TIFS.2006.873601

Venkatesan, R., Koon, S. M., Jakubowski, M. H., & Moulin, P. (2000). Robust image hashing. *Proceedings of IEEE International Conference on Image Processing,* 664-666. https://doi.org/10.1109/ICIP.2000.899541

Wang, J., Kumar, S., & Chang, S. F. (2012). Semi-supervised hashing for large-scale search. *IEEE Transactions Pattern Analysis Machine Intelligence, 34*(12), 2393-2406. https://doi.org/10.1109/TPAMI.2012.48

Zhang, Y., Tang, S., & Li, J. (2007) Secure and incidental distortion tolerant digital signature for image authentication. *Journal of Computer Science and Technology, 22*(4), 618-625. https://doi.org/10.1007/s11390-007-9079-6

Zhao, Y., Wang, S., Zhang, X., & Yao, H. (2013). Robust hashing for image authentication using zernike moments and local features. *IEEE Transactions on Information Forensics and Security, 8*(1), 55-63. https://doi.org/10.1109/TIFS.2012.2223680

Copyrights