JOURNAL OF INFORMATION SECURITY AND APPLICATIONS ■■ (2016) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

Wave atom transform based image hashing using distributed source coding

Yanchao Yang [a], *Junwei Zhou* [a], *Feipeng Duan* [a], *Fang Liu* [b,*], *Lee-Ming Cheng* [b]

[a] *Hubei Key Laboratory of Transportation Internet of Things, School of Computer Science and Technology, Wuhan University of Technology, Wuhan, China*

[b] *Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China*

ARTICLE INFO

Article history:
Available online

Keywords:
Perceptual hashing
Image authentication
Distributed source coding
Wave atom transform

ABSTRACT

To reduce the size of hash code and enhance the security of wave atom transform (WAT) based image authentication system, a low-density parity-check code based distributed source coding (DSC) is employed to compress the hash code. With the help of a legitimately modified image, the compressed hash value could be correctly decoded while it will fail with the help of a maliciously attacked image. Therefore, the employed DSC provides a desired robustness to image authentication. Simulation results indicate that the proposed scheme provides a better performance with less hash code than existing WAT based image hash without using DSC. Moreover, the proposed scheme outperforms the random projection based approach in terms of authentication accuracy and data size.

1. Introduction

Along with the rapid development of information technologies, the broad popularity of image manipulation tools has led to an explosive growth of image illegal use, which makes image authentication more and more important. Three kinds of image authentication techniques, namely digital forensics (Zhao and Zhao, 2013), image watermarking (Chetan and Nirmala, 2015; Ghosal and Mandal, 2014) and perceptual hashing (Zhao et al., 2013), have been carried out on image authentication. Perceptual hashing is the transformation of an image into a usually shorter fixed-length value that represents the original image. It could verify the originality of an image by comparing the hash codes of the original image and the target image. Swaminathan et al. (2006) have developed a perceptual hashing scheme based on Fourier transform features and controlled randomization. By embedding the detected local features into shape-context-based descriptors, Lv and Wang (2012) used the most stable scale-invariant feature transform key points as the hash code. Zhao et al. (2013) employed Zernike moments to represent the luminance and chrominance of an image as global features, while they took position and texture information of salient regions as local features to produce the hash code.

Since target images are usually correlated to original image in the image authentication system, the hash codes of original image and target image are correlated, thus it is possible to compress hash code of the original image using distributed source coding (DSC). The redundancy of hash code can be further reduced and the compressed hash code will be statistically independent of the target image. Motivated by the potential benefits of using DSC such as reducing size of the

* *Corresponding author.* Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China. Fax: +852 34424151.
Email address: fangliu2@my.cityu.edu.hk (F. Liu).

http://dx.doi.org/10.1016/j.jisa.2016.09.001

Please cite this article in press as: Yanchao Yang, Junwei Zhou, Feipeng Duan, Fang Liu, Lee-Ming Cheng, Wave atom transform based image hashing using distributed source coding, journal of information security and applications (2016), doi: 10.1016/j.jisa.2016.09.001

hash code and improving the security of the authentication system, some researchers studied the compression processing for the follow-up procedures of hash construction (Lin et al., 2012; Sun et al., 2002; Tagliasacchi et al., 2009; Venkatesan et al., 2000). An error-correcting code is employed in Venkatesan et al. (2000) by projecting the hash into syndrome bits which are used to verify the authentication directly. The parity check bits of the binary feature vectors, which are produced by a systematic Hamming code, are taken as the hash code in Sun et al. (2002). In addition, DSC is combined with compressive sensing to identify sparse image tampering (Tagliasacchi et al., 2009). The hash code is produced by encoding the quantized random projections using a LDPC-based DSC encoder (Varodayan et al., 2012), while a DSC decoder is employed to decode the hash value with the help of target image. A training procedure is usually applied to find the minimum decodable rate (MDR) for all the legitimately modified images. Thus, if a legitimately modified image is taken as side information, the decoding will be successful, but it will fail with the help of illegitimately modified image due to the weak correlation between the original image and the illegitimately modified image.

On the other hand, wave atom transform (WAT) is a recent addition to the repertoire of mathematical transforms of computational harmonic analysis, which is introduced by Demanet and Ying (2007). WAT is constructed from tensor products of adequately chosen 1-D wave packets, and the 2-D orthonormal basis functions with four bumps can be formed by individually utilizing products of 1-D wave packets in the frequency plane. As a variant of 2-D wavelet packets, WAT could adapt to arbitrary local directions of a pattern, and sparsely represent anisotropic patterns aligned with the axes. Oscillatory functions and oriented textures in WAT have been proven to have a dramatically sparser expansion compared to some other fixed standard representations, such as Gabor filters, wavelets, and curvelets. A WAT based perceptual hashing was studied in Liu et al. (2012), which has reported that WAT based perceptual hash could outperform discrete cosine transform or discrete wavelet transform based schemes in terms of robustness and fragility. In order to reduce the size of hash code and improve the security of the WAT based perceptual hashing, this work employs a LDPC-based DSC (Varodayan et al., 2012) to compress the randomized wave atom features of the original image, which is also expected to show better performance than the scheme without DSC. The contributions of this work are listed as follows: (1) Since the compressed hash value could be correctly decoded but it will fail with the help of a maliciously attacked image, the employed DSC provides a desired robustness to image authentication. (2) The correlation between the hash value and images is removed by DSC, which certainly improves the security of the existing hash scheme. (3) The length of hash value is shortened.

The rest of this paper is structured as follows. The proposed authentication system is described in Section 2, and the experimental analyses are presented in Section 3. The conclusions are given in Section 4.

2. Proposed authentication system

The proposed authentication system is composed of two steps: In the first step, the randomized wave atoms are extracted from the original image (Liu et al., 2012). The randomized wave atoms will be further encoded by LDPC-based DSC in the second step. The encoded wave atoms are taken as the hash code. The target images are produced by two channels which include a legitimate channel and a tampered channel (Lin et al., 2012). In the legitimate channel, the target image is only processed with legitimate operations, such as lossy compression including JPEG and JPEG2000. While in tampered channel, a further malicious modification is applied. The examples of two channels' outputs are shown in Fig. 1, the original image (a) is fragment of "Lena", the target image (b) is the output of the legitimate channel, and the target image (c) is the output of the tampered channel. The aim of the image authentication system is to distinguish the images of the tampered channel from the legitimate channel ones.

2.1. *WAT based perceptual hashing*

In WAT, the image is decomposed into several scale bands. In each scale band, there are different numbers of sub-blocks and each sub-block consists of various wave atom coefficients. With the increasing of scale band, the number of coefficients in scale

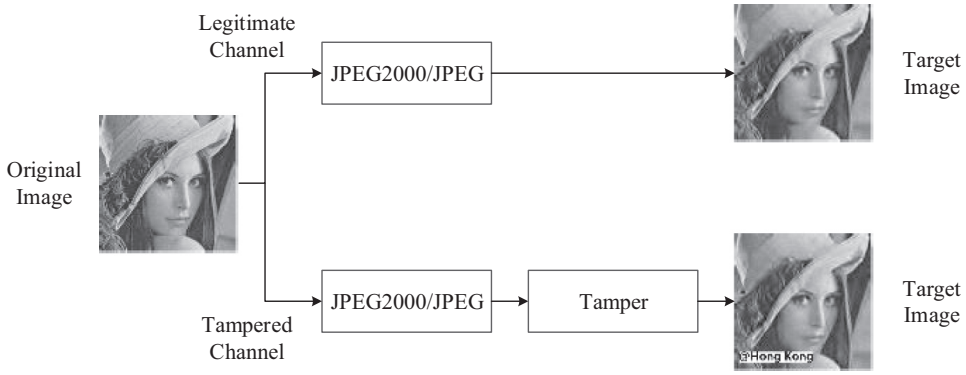

Fig. 1 – Examples of original image and target images. The target images are modeled as output of two channels. In the legitimate channel, the image is processed by legitimate operations, such as JPEG2000/JPEG. In the tampered channel, the images are further tampered.

Please cite this article in press as: Yanchao Yang, Junwei Zhou, Feipeng Duan, Fang Liu, Lee-Ming Cheng, Wave atom transform based image hashing using distributed source coding, journal of information security and applications (2016), doi: 10.1016/j.jisa.2016.09.001