Regular paper

Watermarking based image authentication and tamper detection algorithm using vector quantization approach

Archana Tiwari, Manisha Sharma, Raunak Kumar Tamrakar

PII: S1434-8411(16)31029-9
DOI: http://dx.doi.org/10.1016/j.aeue.2017.05.027
Reference: AEUE 51898

To appear in: *International Journal of Electronics and Communications*

Received Date: 19 October 2016
Revised Date: 14 March 2017
Accepted Date: 17 May 2017

Please cite this article as: A. Tiwari, M. Sharma, R.K. Tamrakar, Watermarking based image authentication and tamper detection algorithm using vector quantization approach, *International Journal of Electronics and Communications* (2017), doi: http://dx.doi.org/10.1016/j.aeue.2017.05.027

Watermarking based image authentication and tamper detection algorithm using vector quantization approach

Archana Tiwari[1], Manisha Sharma[2*] and Raunak kumar Tamrakar[3]

[1,2]Department of Electronics & Telecommunication, Bhilai Institute of Technology, Durg

[3]Department of Applied Physics, Bhilai Institute of Technology, Durg

*Corresponding Author: manishasharma1@rediffmail.com

Abstract- In the present work, a novel image watermarking algorithm using vector quantization (VQ) approach is presented for digital image authentication. Watermarks are embedded in two successive stages for image integrity verification and authentication. In the first stage, a key based approach is used to embed robust zero level watermark using properties of indices of vector quantized image. In the second stage,semifragile watermark is embedded by using modified index key based (MIKB) method. Random keys are used to improve the integrity and security of the designed system. Further, to classify an attack quantitatively as acceptable or as a malicious attack, pixel neighborhood clustering approach is introduced. Proposed approach is evaluated on 250 standard test images using performance measures such as peak signal to noise ratio (PSNR) and normalized hamming similarity (NHS). The experimental results shows that propose approach achieve average false positive rate 0.00024 and the average false negative rate 0.0012. Further, the average PSNR and tamper detection/localization accuracy of watermarked image is 42 dB and 99.8% respectively; while tamper localization sensitivity is very high. The proposed model is found to be robust to common content preserving attacks while fragile to content altering attacks.

Index Terms -Attack classification; Biometric verification watermark; Image authentication; Robust watermarking; Semifragile watermarking; Vector quantization.

1. INTRODUCTION

With development of the digital technology recreation of digitally generated information has become very easy, and can be transmitted by digital media with ease among other medias of message conveyance images are most common. Therefore protection of these images and its content authentication is important. To authenticate the integrity and authenticity of a digital image, digital watermarking techniques have been considered an effective technique [1-5].The watermarking technique for authentication purpose can be classified as Robust, fragile and semifragile watermarking techniques based on their level of security. A robust watermark