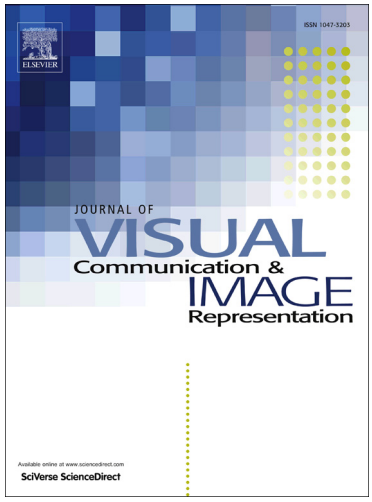

Targeted Attack and Security Enhancement on Texture Synthesis Based Steganography

Hang Zhou, Kejiang Chen, Weiming Zhang, Zhenxing Qian, Nenghai Yu

PII: S1047-3203(18)30087-7
DOI: https://doi.org/10.1016/j.jvcir.2018.04.011
Reference: YJVCI 2178

To appear in: *J. Vis. Commun. Image R.*

Please cite this article as: H. Zhou, K. Chen, W. Zhang, Z. Qian, N. Yu, Targeted Attack and Security Enhancement on Texture Synthesis Based Steganography, *J. Vis. Commun. Image R.* (2018), doi: https://doi.org/10.1016/j.jvcir.2018.04.011

Targeted Attack and Security Enhancement on Texture Synthesis Based Steganography

Hang Zhou[a], Kejiang Chen[a], Weiming Zhang[a,*], Zhenxing Qian[b], Nenghai Yu[a]

[a]*CAS Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230027, China.*
[b]*School of Computer Science, Fudan University, 201203, China.*

Abstract

We describe an effective and efficient strategy building steganography detector for patch synthesis based steganography, one case of which is reversible texture synthesis based steganography method proposed by Wu *et al.* [12]. By exploiting the observation that steganography destroys optimization of matching extent between the synthetic patch and optimal candidate patch, we reconstruct the two patches from an overlapped region to extract the existence of optimality, which are distinct between cover and stego images, to form features. Support vector machine (SVM) is implemented for classification. Meanwhile, a variant of Wu *et al.*'s steganographic method is proposed with reinforced security, by padding redundant regions carrying no message around the periphery of the synthesized image and generating additional candidate patches to increase capacity. Experiments demonstrate that the modified algorithm offers not only better resistance against the state-of-the-art steganalysis methods and steganalytic attack we developed, but also a larger embedding capacity.

Keywords: Texture image, steganalysis, texture synthesis, steganography.

1. Introduction

Steganography is a technique for covert communication and privacy protection, which is now a fairly standard concept in computer science. The process of modern steganography is that a steganographic system embeds hidden content in unremarkable cover media so as not to arouse the suspicion of an eavesdripper [1].

Currently, the majority of image steganographic methods adopt natural images as cover images to embed data, where the most successful approach to design content adaptive steganography is based on minimizing the distortion between the cover and the corresponding stego object, which is acquired by assigning a cost

*Corresponding author. Tel.: +86 0551 3600683
Email addresses: zh2991@mail.ustc.edu.cn (Hang Zhou), chenkj@mail.ustc.edu.cn (Kejiang Chen), zhangwm@ustc.edu.cn (Weiming Zhang), zxqian@fudan.edu.cn (Zhenxing Qian), ynh@ustc.edu.cn (Nenghai Yu)
[1]This work was supported in part by the Natural Science Foundation of China under Grant U1636201, Grant 61572452, Grant U1536108, Grant 61572308 and Grant U1736213.