

Accepted Manuscript

Image steganography in spatial domain: A survey

Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris,
Anthony T.S. Ho, Ki-Hyun Jung



PII: S0923-5965(18)30256-X
DOI: <https://doi.org/10.1016/j.image.2018.03.012>
Reference: IMAGE 15355

To appear in: *Signal Processing: Image Communication*

Received date : 13 December 2016
Revised date : 25 December 2017
Accepted date : 19 March 2018

Please cite this article as: M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T.S. Ho, K.-H. Jung, Image steganography in spatial domain: A survey, *Signal Processing: Image Communication* (2018), <https://doi.org/10.1016/j.image.2018.03.012>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Image Steganography in Spatial Domain: A Survey

Mehdi Hussain^{a,b*}, Ainuddin Wahid Abdul Wahab^a, Yamani Idna Bin Idris^a, Anthony T. S. Ho^{c,d,e}, Ki-Hyun Jung^{f,*}

^a Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

^b School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, Pakistan

^c Department of Computer Science, University of Surrey, Guildford, Surrey, UK

^d Tianjin University of Science and Technology, Tianjin, China

^e China Wuhan University of Technology, Wuhan, China

^f Department of Cyber Security, Kyungil University, Republic of Korea

* Corresponding authors: mehdi.hussain@seecs.edu.pk, khanny.jung@gmail.com

ARTICLE INFO

Article history

Keywords:

Image Steganography
Spatial Domain Steganography
Adaptive Steganography
Data Hiding
Security
Digital Spatial Domain

ABSTRACT

This paper presents a literature review of image steganography techniques in the spatial domain for last 5 years. The research community has already done lots of noteworthy research in image steganography. Even though it is interesting to highlight that the existing embedding techniques may not be perfect, the objective of this paper is to provide a comprehensive survey and to highlight the pros and cons of existing up-to-date techniques for researchers that are involved in the designing of image steganographic system. In this article, the general structure of the steganographic system and classifications of image steganographic techniques with its properties in spatial domain are exploited. Furthermore, different performance matrices and steganalysis detection attacks are also discussed. The paper concludes with recommendations and good practices drawn from the reviewed techniques.

1. Introduction

Internet revolution provides the easiness in digital communication; meanwhile, it also becomes a challenge for securing the information over the open network. In order to address the security of information, numerous approaches have been proposed in the field of security systems under information encryption and information hiding as depicted in Fig. 1. Information encryption known as cryptography scrambles the secret message in such a way that it becomes an unintelligent message to eavesdroppers. However, this is always incapable of being encrypted the secret message, it draws attention. Therefore, it is required an invisible communication without noticing to anyone the communication will happen in some cases. This is the reason why information hiding mechanism is needed. Information hiding consists of two subdisciplines, i.e. steganography and watermarking [1]. Both steganography and watermarking are used to hide the secret message and are closely related to each other, but both lies on different objectives. The main concern of steganography is to conceal the existence of communication and protection of secret data. In contrast, watermarking is to protect the integrity of secret data with or

without concealing the existence of communication from eavesdroppers. The main purpose of watermarking applications is to protect the intellectual property of the contents. However, Table 1 (an extension of Cheddad et al.) shows basic characteristic between information encryption and information hiding systems.

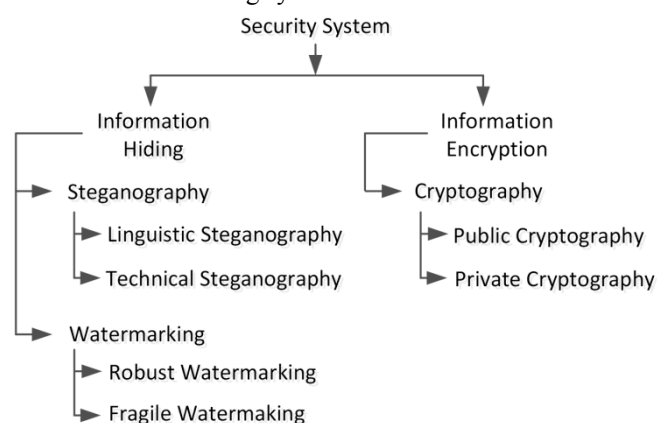


Fig. 1 Basic security system branches (based on Cheddad et al.)

Researchers have shown a great interest in image steganography for last decade. It becomes the most widespread research area due to easy of multimedia content

Download English Version:

<https://daneshyari.com/en/article/6941495>

Download Persian Version:

<https://daneshyari.com/article/6941495>

[Daneshyari.com](https://daneshyari.com)