

# Preface

“A picture is worth a thousand words,” is a well-known proverb by Confucius. Images help in the communication of ideas, events or memories very efficiently and effectively.

Data communications involve transmission over noisy channels. Due to the nature of modern communications, intentional modifications or unintentional errors might be introduced into images by noise during the transmission over a communication channel, a human or by source encoders and decoders. In order to prevent intentional modifications, images are protected more and more against manipulations by authentication mechanisms. Most of the unintentional errors can be corrected using channel coding, but the complete elimination of all the errors cannot be ensured. Such erroneous images cannot be processed, as they are recognized as untrustworthy by authentication mechanisms.

This fact raises lots of questions and expresses a need for new algorithms which support authentication of images in the *presence of noise*, i.e., unintentional modifications of images. Standard authentication mechanisms are extremely fragile to the existence of errors and therefore they very often fail in communications in noisy environments. Therefore, *robustness* is an important property which new algorithms have to support.

This book consists of six chapters presenting different aspects of its main contribution, which is the introduction of the robustness into image authentication in noisy communications.

The advancement of digital technology implicated the development of sophisticated tools to tamper digital images. Therefore, a number of techniques using digital image watermarking and hashing have been proposed. In Chapter 1, the problem of image authentication is introduced and a wavelet-based technique is presented to address robustness, security and tamper detection issues in hash-based image authentication schemes. Unlike other hashing schemes that apply randomness to select image features from a known feature space, a randomized pixel modulation method is used to randomly transform the entire feature space. The key dependent transformed feature space is used to calculate the image hash. To reduce the size of the hash, 3-bit and 4-bit quantization schemes are also presented. A number of experimental results

along with analysis are reported to show how an image hashing scheme is practically evaluated to gauge its robustness, security and tamper detection capability.

Chapter 2 is concerned with the digital multimedia content which is susceptible to malicious manipulations and alterations. There are two widely used image authentication techniques, i.e., digital signatures and digital watermarking. Digital signatures based authentication is quite mature and already in wide use. However, its shortcoming is that the signature needs extra transmission capacity or establishing a separate secure channel for transmission. Additionally, due to the usage of secure hash functions, digital signatures are also susceptible to failed authentication because of the avalanche effect, which might occur due to many reasons such as channel noise, quantization or compression. Digital watermarking can perform content authentication without the aforementioned shortcomings and it is difficult to be detached or tampered. An overview of digital watermarking techniques is given in this chapter, followed by the state of the art and the introduction of a new algorithm.

Chapter 3 investigates the feasibility of content based image authentication using the perceptual image hashing technique as an alternative data authentication scheme in Wireless Multimedia Sensor Networks (WMSNs). High level requirements for image authentication in WMSNs are addressed, and the previously published literature regarding data authentication schemes for WMSNs as well as content based image authentication using the perceptual image hashing technique is discussed as well. Furthermore, the performance of five selected perceptual image hashing algorithms are measured and compared in terms of robustness, discriminability and security in order to provide a perspective on the potential feasibility as an alternative solution to the existing data authentication scheme in WMSNs.

Chapter 4 gives a brief and explicit survey on generic approximate (fuzzy) message authentication codes. The presented schemes are described and categorized according to their design methods. The main design methods are based on computational complexity and unconditional security viewpoints. The corresponding analysis of each category is given, including the performance and security consideration. A short comparison result is given at the end of the first part of the chapter. The second part shows some applications of generic approximate message authentication codes on image authentication techniques.

Chapter 5 addresses the sensitivity of standard message authentication codes (MACs) which makes them unsuitable for application in multimedia applications. Specific algorithms for image authentication, so called fuzzy image authentication algorithms, are discussed in this chapter. These algorithms are tolerant to a certain degree of modifications introduced by channel noise or image processing operations. Fuzzy image authentication algorithms should be designed in a manner that they can differentiate allowed manipulations from manipulations which are not allowed. The fuzzy authentication algorithms should have an additional desirable property of error localization and correction. Once the modifications in the image are localized to a specific region within the image, they can be corrected using the error correcting codes embedded in the authentication algorithms.

The robustness of biometric systems under affine transformations is important for precise user authentication. Most systems are using alignment to compensate

for occurring transformations. Chapter 6 analyses the robustness of alignment-free biometric features in fingerprint and vein biometrics, motivated by the drawbacks of alignment-based biometrics. Various approaches from the fields of pattern recognition as well as biometrics are described, aggregated and assessed. Based on the similarities of the involved disciplines, an evaluation strategy from the field of digital image processing is proposed to assess the performance and invariance of biometrical feature extraction.

The future communications will be developed in the direction of integrated and secure techniques which need to be fast and reliable. The rapid progress specifically in wireless communications needs solutions for the biggest enemy of communications, i.e., noise. The solutions which can support such development trends have to be robust against noise. This book presents and discusses some algorithms which contribute to an improved authentication of images subjected to noise from different sources.

Robust Image Authentication in the Presence of Noise

Zivic, N. (Ed.)

2015, XV, 187 p. 79 illus., 33 illus. in color., Hardcover

ISBN: 978-3-319-13155-9