Multimed Tools Appl (2008) 39:1–46
DOI 10.1007/s11042-007-0154-3

Methods for image authentication: a survey

Adil Haouzia · Rita Noumeir

Published online: 1 August 2007

Abstract Image authentication techniques have recently gained great attention due to its importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet. Therefore, military, medical and quality control images must be protected against attempts to manipulate them; such manipulations could tamper the decisions based on these images. To protect the authenticity of multimedia images, several approaches have been proposed. These approaches include conventional cryptography, fragile and semi-fragile watermarking and digital signatures that are based on the image content. The aim of this paper is to present a survey and a comparison of emerging techniques for image authentication. Methods are classified according to the service they provide, that is strict or selective authentication, tamper detection, localization and reconstruction capabilities and robustness against different desired image processing operations. Furthermore, we introduce the concept of image content and discuss the most important requirements for an effective image authentication system design. Different algorithms are described and we focus on their comparison according to the properties cited above.

Keywords Image authentication · Image content · Cryptography · Fragile watermarking · Semi-fragile watermarking · Digital image signature

1 Introduction

Information had a paramount role during history at all times [15]. Its control is synonymous of ability and power. It can represent battle plans, secret negotiations or current events and television news. Exploitation of information can bring richness. Information used to be transmitted by manuscript or by voice; now it can travel thousands of kilometres in some tenths of second thanks to waves and cables. These fast technological developments make

A. Haouzia · R. Noumeir (✉)
Electrical Engineering Department, École de Technologie Supérieure,
1100 Notre-Dame West, Montreal, Quebec, Canada, H3C 1K3
e-mail: rita.noumeir@etsmtl.ca

information extremely important in our life. However, this powerful information is now more volatile and can be easily intercepted or reproduced with all the consequences which we can imagine such as false medical diagnostic, false military targets or false proof of events [22]. Image authentication is important in many domains: military target images, images for evidence in court, digital notaries documents, and pharmaceutical research and quality control images. All these images have to be protected in order to avoid false judgements.

The wide availability of powerful digital image processing tools allows extensive access, manipulations and reuse of visual materials. In fact, lot of people could now easily make unauthorized copies and manipulate images in such a way that may lead to big financial or human lives losses. These problems can be better understood with a simple example. A patient with a serious illness, discovered from medical diagnostic images, may eventually get better due to medical treatments. The medical follow-up of that patient involves the interpretation of historic images to evaluate the progression of the illness in time. A possible false diagnosis can jeopardize the patient life, if the stored image underwent malevolent manipulations, storage errors or compression, such that the resulted distortions cannot be detected by the doctor. This is an example where modifications are not tolerated. However, in many other applications we need to tolerate some image processing operations for transmission, enhancement or restoration while we still need to detect at the same time any significant changes in the image content.

Therefore, there is an ambiguity since some changes must be tolerated while others not. Consequently, image authentication can be divided in two groups: strict and selective authentication. Strict authentication is used for applications where no modifications in the protected image are allowed. On the other hand, selective authentication is used especially when some image processing operations must be tolerate such as compression, different filtering algorithms and/or even some geometrical transformations...[92, 158]. For strict authentication, solutions including conventional cryptography and fragile watermarking provide good results that satisfy users, even though some researches still need to be done in order to enhance localization and reconstruction performances of the image regions that were tampered. Selective authentication on the other hand, uses techniques based on semi-fragile watermarking or image content signatures to provide some kind of robustness against specific and desired manipulations. Results are satisfying, but the problem is far from being solved. Researches are now more concentrated in the area of image content signatures and the number of proposed solutions has increased rapidly in last years due to the large number of applications. Nevertheless, more sophisticated solutions that allow combinations of several desired modifications are still to be discovered.

In this paper, we present, discuss, classify and compare different algorithms that provide solutions for both strict and selective authentication services. Comparisons are based on different criterions such as detection, localization, restoration and tolerance. The properties of each group of methods are provided with references to algorithms.

The rest of this paper is organised as follows. First, we tend to clarify the definition of image content. Second, we thought that some definitions would help some readers; therefore, a brief introduction to some mathematical tools and vocabulary that are used in image authentication is provided. Third, we present, classify, discuss and compare approaches that have been proposed for image authentication such as conventional cryptography, fragile/semi-fragile watermarking and content-based image signatures. Our approach focuses on comparing algorithms within each group and subgroup. Methods are divided into two groups: strict and selective authentication. Strict authentication methods are further divided into conventional cryptography and fragile watermarking subgroups. Selective authentication methods are further divided into semi-fragile watermarking and digital signature based