Chapter VI

Issues on Image Authentication

Ching-Yung Lin, IBM T.J. Watson Research Center, USA

ABSTRACT

Multimedia authentication distinguishes itself from other data integrity security issues because of its unique property of content integrity in several different levels — from signal syntax levels to semantic levels. In this section, we describe several image authentication issues, including the mathematical forms of optimal multimedia authentication systems, a description of robust digital signature, the theoretical bound of information hiding capacity of images, an introduction of the self-authentication-and-recovery image (SARI) system, and a novel technique for image/video authentication in the semantic level. This chapter provides an overview of these image authentication issues.

INTRODUCTION

The well-known adage that “seeing is believing” is no longer true due to the pervasive and powerful multimedia manipulation tools. Such development has decreased the credibility that multimedia data such as photos, video or audio clips, printed documents, and so forth used to command. To ensure trustworthiness, multimedia authentication techniques are being developed to protect multimedia data by verifying the information integrity, the alleged source of data, and the reality of data. This distinguishes from other generic message authentication in its unique requirements of integrity. Message authentication techniques usually cannot allow any single bit of data change. However, multimedia
data are generally compressed and quality enhanced. Thus, accepting lossy compressed multimedia and some content-preserving filtering is an essential requirement in many applications.

Multimedia authentication distinguishes itself from other data integrity security issues because of its unique property of content integrity in several different levels - from signal syntax levels to semantic levels. In contrast to the data integrity issues that do not allow any changes on the data, multimedia can be considered as authentic if it is manipulated in a sense that its “content” is preserved. Content, which is an ambiguous concept, can indicate several different meanings of multimedia data. Figure 1 shows several layers of content description (Jaimes & Chang, 2000). Among them, the first three layers in the syntax level may be explicitly described by machines. For instance, compression, filtering, or some other signal level manipulations can be explicitly modeled. Thus, it is possible to clearly distinguish them from malicious manipulations, such as crop-and-replacement, without any false alarm and with a negligible miss rate (Lin & Chang, 2001). However, an authentication system based on syntax-level modeling may meet its limits if the overall manipulation is a combination of various types of acceptable changes and the final manipulated multimedia data are still similar to the original in the semantic sense. For instance, a picture of President Clinton and the First Lady walking on the lawn may be semantically authentic even if the color of lawn changes or some background trees are removed, as long as the head of the First Lady is not changed. Therefore, we consider a semantic authentication system that checks the semantic content is required and is closer to the way human beings conduct authentication.

Several syntax level authentication methods have been discussed. Schneider and Chang first proposed the concept of salient feature extraction and similarity measure for image content authentication (Schneider & Chang, 1996). They also discussed issues of embedding such signatures into the image. However, their work lacked a comprehensive analysis of adequate features and embedding schemes. Bhattacha and Kutter proposed a method that extracts “salient” image feature points by using a scale interaction model and Mexican-hat wavelets (1998). Queluz proposed techniques to generate digital signature based on moments and edges of an image (Queluz, 1999). Fridrich divided images into 64x64 pixel blocks. For each block, quasi-VQ codes were embedded using the spread spectrum method (Fridirch, 1998). Lu and Liao proposed several schemes for structured digital signatures for authentication. Lin and Chang proposed a unique self-authentication-and-recovery image (SARI) system (2001). SARI utilizes a semi-fragile watermarking technique that distinguishes acceptable JPEG lossy compression, brightness and contrast changes from malicious attacks. The authenticator can identify the positions of corrupted blocks, and recover them with approximations of the original ones. SARI is based on the invariant feature codes and the zero-error information hiding capacity of images.
E-Mail, Web Service and Cryptography
www.igi-global.com/chapter/mail-web-service-cryptography/46238?camid=4v1a