

A SECURE IMAGE AUTHENTICATION SCHEME WITH TAMPERING PROOF AND REMEDY BASED ON HAMMING CODE

REN-DER LIN^{1,2}, TZUNG-HER CHEN^{3,*}, CHIEN-CHEN HUANG⁴
WEI-BIN LEE⁴ AND WEN-SHYEN E. CHEN¹

¹Department of Computer Science and Engineering
National Chung Hsing University
250, Kuo Kuang Rd., Taichung, 402 Taiwan
{ rld; echen }@cs.nchu.edu.tw

²Department of Information Management
Hsiuping Institute of Technology
11 Gongye Rd., Dali City, Taichung County, 412 Taiwan

³Department of Computer Science and Information Engineering
National Chiayi University
300 University Rd., Chia-Yi City, 600 Taiwan

*Corresponding author: thchen@mail.ncyu.edu.tw

⁴Department of Information Engineering and Computer Science
Feng Chia University
No. 100 Wenhwa Road, Seatwen, Taichung, 407 Taiwan
{ m9510601; wblee }@fcu.edu.tw

Received March 2008; revised September 2008

ABSTRACT. *Recently, there exist some schemes not only to localize tampered areas but also try to remedy with a rough approximation to damaged areas. Chan and Chang (2007) proposed a new scheme by Hamming code, which effectively detects and eliminates burst bit errors and the recovered pixels in detailed areas can actually gain very high clarity. In this paper, the potential weakness of the Chan-Chang scheme will be analyzed and the experimental results will show that the security problem does exist. Therefore, in order to benefit the excellent advantages of the Chan-Chang scheme, it is worthwhile to propose an improved scheme based on Hamming code to enhance security. The improved scheme not only overcomes the potential security weakness of the Chan-Chang scheme but also takes advantage of and enhances the property of (7,4) Hamming code rule. The experimental results show that the proposed scheme can withstand the noise-adding attack and tampering attack. Moreover, performances of detecting and recovering are with high accuracy and good quality. It is worthwhile to note that the ability of lossless image remedy is analyzed under different tampered size and transmission error.*

Keywords: Image authentication, Tampering proof, Tamper remedy, Hamming code

1. Introduction. With the quick development and progress in digital techniques, the reproduction, modification and distribution of digital multimedia become easier and easier. Of all kinds of digital multimedia, digital images are the most widespread. Therefore, the investigations of image authentication are in great demand in this decade while image copyright protection [20,21] is of special importance. Image authentication is a process used to ascertain the trustworthiness of digital images. An image authentication system uses a combination of techniques such as digital signature, digital watermarking, error correction coding, and cryptographic hash functions to ensure the integrity of images and verify whether it has been tampered with.