International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **6**, June **2012**

 ISSN 1349-4198
pp. 4147–4156

AN OWNERSHIP PROTECTION SCHEME BASED ON VISUAL CRYPTOGRAPHY AND THE LAW OF LARGE NUMBERS

Young-Chang Hou and Pei-Hsiu Huang

Department of Information Management
Tamkang University
No. 151, Yingzhuan Rd., Danshui Dist., New Taipei City 25137, Taiwan
{ ychou; mr.huang }@mail.im.tku.edu.tw

Received January 2011; revised September 2011

Abstract. *Digital watermarking is a technique for the protection of intellectual property rights. In this study, a novel ownership protection scheme based on visual cryptography and the law of large numbers is proposed, where 2 phases, namely an ownership construction phase and an ownership authentication phase, each with 3 steps, are designated to illustrate how it works. In our scheme, two pixels at a time are selected randomly from the host image, then compared with each other and the results determine the corresponding content of the shares. The law of large numbers is employed to ensure the random distribution of half-black-and-half-white shares, which satisfies the demand needed for security in visual cryptography. The proposed method enjoys several advantages over conventional methods such as it does not alter the host image, it can identify the ownership without the help of the original host image, and it allows multiple watermarks or larger watermarks to be registered in a smaller host image. Finally, experimental results are given to illustrate the robustness of our scheme against several common attacks.*
Keywords: Visual cryptography, Law of large numbers, Intellectual property rights protection, Unexpanded share

1. **Introduction.** In recent years, the rapid development and growth in popularity of the Internet have made it rather easy for digital data (whether text, voice, or images) to be transmitted and exchanged over the World Wide Web. However, the convenience of sharing and spreading digital data on the Internet has brought about the problems of abuse and violation of intellectual property rights. Therefore, finding a way to protect the ownership of digital data has become a very important issue. Digital watermarking is a method that inserts a digital signal sequence into the protected digital image for the purpose of copyright protection, integrity checking and captioning. Should the ownership of the image need to be verified, the hidden watermark can be extracted through the watermarking retrieval procedure to prove the ownership.

Naor and Shamir [1] introduced a perfectly secure method called visual cryptography (VC) for protecting the secret images. The prominent feature provided by the VC decryption method is that it can be done with the human eye, without the need of a complicated mathematical computation. The basic model of VC consists of "splitting" the image or watermark into two transparencies (shares). One share can be regarded as the ciphertext and the other one as the secret key (called the key share). Each share looks like random noise, without any clue to disclose the outlines of the secret image. However, the original image can be revealed simply by superimposing these two shares. Due to its simplicity, the model can be used by anyone, even without knowledge of cryptography and without performing any complex computations.