International Journal of Innovative Computing, Information and Control
Volume **7**, Number **9**, September **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 5175–5191

A GENERIC PROBABILISTIC VISUAL-SECRET-SHARING SCHEME USING OPTIMIZATION APPROACH

Pei-Ling Chiu[1] and Kai-Hui Lee[2,*]

[1]Department of Risk Management and Insurance
Ming Chuan University
No. 250, Zhong Shan N. Rd., Sec. 5, Taipei 111, Taiwan
plchiu@mail.mcu.edu.tw

[2]Department of Computer Science and Information Engineering
Ming Chuan University
No. 5, De Ming Rd., Gui Shan District, Taoyuan County 333, Taiwan
[*]Corresponding author: khlee@mail.mcu.edu.tw

Received April 2010; revised August 2010

Abstract. *In a (k, n)-VSS (visual secret sharing, $2 \leq k \leq n$) scheme, a secret image is encrypted into n shares that are distributed among n participants. Reducing pixel expansion and improving the quality of recovered images to enhance the usefulness are still major issues of VSS scheme constructions, especially for large k and n. Moreover, all existing constructions of VSS schemes have to be designed individually; developing a generic construction or method for VSS schemes is still an open question. In this study, an optimization technology is used to develop a generic probabilistic VSS (GProb-VSS) (k, n)-scheme without pixel expansion for binary secret images. First, we define a mathematical optimization model to maximize the contrast in recovered images under security constraints. Then, we develop a simulated-annealing-based algorithm for solving the difficult problem. Furthermore, we try to improve the display quality by relaxing the relative parameter. Experimental results show that the proposed generic approach significantly outperforms the previous methods in terms of the recovered image quality and pixel expansion.*

Keywords: Visual secret sharing, Generic probabilistic VSS, Optimization, Simulated annealing approach

1. **Introduction.** The threshold scheme of visual cryptography has been studied frequently; it is also known as the (k, n)-VSS (visual secret sharing, $2 \leq k \leq n$) scheme [1,2]. A secret image is encrypted into n meaningless shares (i.e., shadows) and printed on transparencies and then, the shares are distributed among n participants. The secret image cannot be decoded by combining shares of a forbidden set, which includes less than k participants. However, for a qualified set containing at least k participants, the stacked transparencies can be used to retrieve and visually decrypt the secret image. A major advantage of this scheme is that decoding can be performed by anyone without any knowledge of cryptography and computations. Moreover, visual cryptography has been widely applied in many different research and practical domains, such as digital watermarking [3,4], authentication [5], information hiding [6] and navigation applications [7].

The most conventional VSS schemes are classified as deterministic approaches because the black secret pixels in secret images can be deciphered accurately to the recovered images [8,9]. A specific codebook to encode one white/black secret pixel in a secret image into m sub-pixels has been drafted. In a (k, n)-VSS scheme, a secret pixel is mapped to n different blocks with m sub-pixels for each distributed n share images. By