计算机工程与应用 2009 45 (31): 77-80 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种二值图像的阈值可视密码方案

徐永平，胡予濮，王 明，刘书盼

西安电子科技大学 计算机网络与信息安全教育部重点实验室，西安 710071

收稿日期 2009-5-22 修回日期 2009-6-29 网络版发布日期 2009-11-19 接受日期

摘要 目前提出的许多关于二值可视密码方案的论文都致力于研究在可视秘密共享方案里如何使像素扩展比较小或恢复图像的对比度比较高的问题。基于Shamir的秘密共享方案的思想，提出一种新的二值图像（k，n）-VCS可视密码方案。该方案利用二元域上线性方程组解的特征及多层（k，k）-VCS构造基础矩阵S^0，S^1，给出一个强的访问结构，从而获得（k，n）-VCS可视密码方案更小的像素扩展。

关键词 可视密码 可视秘密共享方案 一般访问结构 阈值方案

分类号 TP391

Threshold scheme for binary image visual cryptography

XU Yong-ping，HU Yu-pu，WANG Ming，LIU Shu-pan

Key Laboratory of Computer Network and Information Security，Xidian University，Xi’an 710071，China

Abstract

Most recent papers about binary visual cryptography schemes are dedicated to study a higher contrast of recovered images or a smaller share size in visual secret sharing schemes.This paper proposes a new binary （k，n）-VCS based on the secret sharing schemes.A strong access structure is given which uses the feature of the solution of a system of linear equations over the binary field and hierarchical method for constructing basis binary matrices S^0，S^1，and the （k，n）-VCS is obtained and in almost all the case a much smaller pixel expansion is gained from this method.

Key words visual cryptography visual secret sharing scheme general access structure threshold scheme

DOI: 10.3778/j.issn.1002-8331.2009.31.024

通讯作者 徐永平 xyplh@sohu.com