DOI:10.16136/j.joel.2016.04.0735

一种可验证的基于超混沌系统的灰度图像多密钥共享算法

高 航,程仁洪,高铁杠*

(南开大学 软件学院 天津 300071)

摘要:提出一种可验证的图像多密钥共享方案。算法中,灰度图像首先被置乱,而后划分为多个图像子块,利用图像子块的哈希值作为超混沌系统的初始值,生成多个随机网格(RG),最后利用RG和图像子块的异或生成共享的多个子密钥。提出的算法具有共享密钥空间小、能够无损恢复秘密图像,同时能够验证密钥的持有者是否对密钥进行了恶意篡改,能应用于重要领域如医学以及军事图像的保护。实验结果和对算法的比较分析,验证了算法的有效性。

关键词:密钥共享;超混沌系统;无损恢复;随机网格(RG)

中图分类号:TP309 **文献标识码**:A **文章编号**:1005-0086(2016)04-0413-08

Verifiable multi-secret sharing scheme based on hyper-chaotic system for grey image

GAO Hang, CHEN Ren-hong, GAO Tie-gang*

(College of Software, Nankai University, Tianjin 300071, China)

Abstract: A novel verifiable multi-secret sharing scheme for grey image is proposed in this paper. In the scheme, the grey image is firstly shuffled, then the shuffled image is divided into multiple image blocks, and the hash of every image block is converted into the initial value of the hyper-chaotic system, thus Runge-Kutta iteration algorithm is used for hyper-chaos to generate random grid for each image block. Lastly, the generated random grid and image block are operated with XOR operation, and the result is merged with hash value to get the final sharing secret. The proposed scheme has the advantage of small space of sharing secret and has the ability of restoring the original without any loss of pixel. In the meantime, it can also verify whether the holder of the secret has tampered the secret. All of the above characteristics make it suitable for some important fields such as the protection of military and medical image. Experimental results and sufficient analysis are given to verify the effectiveness of the proposed method.

Key words: secret sharing; hyper-chaotic system; lossless restoration; random grid (RG)

1 引 言

多媒体信息的安全是信息安全领域的一个热点课题。如何安全地在网络环境下传输信息,不仅需要构造安全的网络环境,保证传输信息的及时有效,更要保证信息在传输过程中没有遭到任何的篡改。作为一种有效的多媒体信息的安全防护手段,视觉密码共享(VSS)技术得到关注,并在图像加密以及图像数字水印等方面得到良好应用[1~3]。对VSS的研究,Kafri等[4]提出一种基于随机网格(RG)的VSS实现方法[6];Naor等[5]提出一种基于视觉密码(VC)的VSS的实现方法。目前,在VSS的算法方面提出了多种研究方案。例如,基于VC的VSS研究,Wu等[8]提出了适用于彩色图像的VSS方法;Shyu[9]则提出了适用于彩色和灰度图像的VSS方法;为了提高算法的可用性以及改进图像的视觉质量,提出将生成的类似噪声的共享图像改进成生成有意义的共享图

* E-mail:gaotiegang@nankai.edu.cn

收稿日期:2015-11-05 修订日期:2016-02-03

基金项目:天津市科技发展计划重点(11JCZDJC16000)资助项目