Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 131 (2018) 204–212

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Congress of Information and Communication Technology (ICICT-2018)

Visual Cryptography Based Multilevel Protection Scheme for Visualization of Network Security Situation

Hao Hua[a], Yuling Liu[b]—, Yongwei Wang[a], Dexian Chang[a], Qiang Leng[a]

[a]*Information Science and Technology Institute, Zhengzhou 45001, China*
[b]*Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*

Abstract

Visualization technology for network security situation adopts images to present the massive abstract data regarding network events. It reduces the workload of data analysis and benefits the manager to grasp the overall network status and trend. Secret information in the visual image requires confidentiality protection while transmitting. Comparing with some conventional methods realized by complicated encryptions such as DES and AES, we present a novel multilevel protection scheme based on visual cryptography (VC) with the beauty of decryption done only via the human eyes without using more computing devices. Essentially, a region incrementing VC scheme (RIVCS) is proposed in this paper dealing with the encoding of a secret situation image regarding network security. The secret image includes a number of regions, where each region is allocated with a certain secrecy level. Different secrecy levels can be decoded incrementally when different combinations of participants are gained. Firstly, we develop the model called the general AS (GAS) based RIVCS. Secondly, we design the algorithm for allocating secrecy levels. Thirdly, we construct the encoding matrices for sharing the secret pixels. Experimental results show that our method is more suitable to visualization data protection for network security situation with lower cost, higher reliability and richer application scenarios.

Keywords: multilevel protection, network security situation, visualization, visual cryptography, region increment

1. Introduction

In the visualization system of network security situation, confidential data protections have to face all kinds of

* Corresponding author.
*E-mail address:*ylliu@tca.iscas.ac.cn

10.1016/j.procs.2018.04.204

security challenge. How to protect these data from being modified or destructed during transmission becomes an essential issue. Conventionally, confidential data can be protected by classical cryptographic methods, in other words, is the enciphering and deciphering of data and information using cipher text.

Network data usually contain some confidential information such as the network topology, device configuration and service vulnerability, which is vulnerable to be the potential attackers. Besides, the situation images of network security such as the risks distribution curves, alerts change charts, threat events frequency diagrams contain sensitive information. Meanwhile, different information usually have different secrecy levels such as the devices information in Outreach access area, which is lower significant compared with the that in the DMZ area, while the devices information in the Trusted area is the most sensitive. Similarity, the historical security data is less sensitive than the real-time data. For page limitation, we just name a few. With the development of information system, XOR operation can be easily available in network communication system with low cost. Meanwhile, XOR and OR operations have the same computational complexity, which does not resist the easy-decryption principle of VCS. Therefore, using XOR operation to decode instead of OR operation is promising for network system in the near future.

A (k, n) Visual cryptography scheme (VCS), proposed by Naor and Shamir [1], is an interesting cryptography scheme decoding without any complex computation. A secret image S is encoded into n shares in a (k, n)-VCS [2]. The dealer distributes them among n participants, respectively. After stacking together any k or more shares, the secret image can be recognized by human visual system directly. However, stacking less than k shares gives any no clue about the secret image. An ideal VC method should have more generalized access structure (AS), bigger contrast and smaller pixel expansion, which can provide richer application scenarios, fewer storage costs and clearer visual effects [3].

As a novel branch of VCS, the multi-regions in a secret image can be decoded region by region in the region incrementing VCS (RIVCS), which can be used to multilevel security protection. In the RIVCS, the contents in a secret image are divided into multiple regions according to the application of the dealer, where each region R is allocated with a certain secrecy level l. When decrypting, more shares can be stacked to reveal more regions. The first (2, n)-RIVCS was proposed by Wang [4] in 2009, where the secret image contains n-1 regions. By superimposing (equal to OR operation) any i ($2 \le i \le n$) shares, one can visually decode up to i-1 regions of the secret, but n is limited to 3, 4 and 5, and no construction method was discussed. From this aim, Shyu et al. [5] proposed an efficient construction for (2, n) scheme based on an objective optimization model for minimizing the pixel expansion. However, colors of original black and white pixels are reversed in the recovered image. The general construction method for (k, n)- RIVCS is designed by Yang et al. [6], where k and n can be any integers. Hu et al. [7] further extended the capability of RIVCS. The limitation of reverse-color is broken in his scheme. Unfortunately, with the increasing of n, the pixel expansion improves rapidly and the recovery effect reduces poorly. To overcome this shortcoming, Zhong et al. [8] introduced a random grids based scheme for (k, n) threshold AS. However, the recovered image suffers the drawback of information loss problem. Actually, the original secret pixels are correctly recovered with certain probability by using random grids as demonstrated in [9], which have been investigated particularity in [10, 11]. Recently, In summary, the mentioned RIVCSs are mainly confined to threshold AS, where each share has the same priority. Therefore, further improvement in the aspect of general AS (GAS) to provide flexible sharing strategies for practical applications is necessary. Besides, the low visual performance needs enhancement in existing works. Moreover, further exploits for practical application is significant.

Based on the above consideration, a new RIVCS is presented with two main constructions have been achieved:

1) The secrecy levels are decoded according to the qualified set instead of the number of shares.

2) We introduce XOR operation to RIVCS instead of OR operation to realize an XOR-based scheme with some favorable features such as perfect recovery of white pixels, high contrast and good resolution of secret image.

Experiment results indicate that our method outperforms previous RIVCSs significantly in visual performance, and is more suitable to confidentiality protection of visualization towards network security situation with improved feasibility and flexibility.

The rest of this paper is organized as follows. Section 2 briefly introduces the motivation for our research. In Section 3, we propose the general construction for our proposed RIVCS. Section 4 shows the experiments and discussions. Section 5 concludes our work.