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.

2. Proposed scheme

In this section, we give the formal the model of RIVCS firstly. Afterwards, we give the model of RIVCS for GAS. Finally, we show how to implement secrecy levels allocation and construct the encoding matrices.

2.1. Model of RIVCS

In the proposed model of RIVCS, the regions are recovered using the qualified set. The recover rules can be allocated associated with the sharing strategy. For each minimal qualified set Q_0, we allocate Q_0 with a primary secrecy levels. The remaining qualified set X in $\{\Gamma_{Qual}-\Gamma_0\}$ can decode the related security regions corresponding to the minimal qualified sets Q ($Q \subset X$), while the forbidden set F cannot reveal any regions. The novel definition of RIVCS for GAS is as follows.

Definition 1 (GAS) [3] Let $\Gamma_{Qual} \subseteq 2^P$, and $\Gamma_{Forb} \subseteq 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. We call the pair ($\Gamma_{Qual}$, Γ_{Forb}) as the AS. Define $\Gamma_0 = \{Q \in \Gamma_{Qual} : Q' \notin \Gamma_{Qual} \text{ for all } Q' \subset Q\}$, and we call the members of Γ_0 as the minimal qualified sets. If Γ_{Qual} is monotonically increasing and Γ_{Forb} is monotonically decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$, the AS is strong.

Definition 2 Let (Γ_{Qua}, Γ_{Forb}) be the AS with $\Gamma_0 = \{Q_1, Q_2, \cdots, Q_q\}$ for encoding the secret image. The secret image is comprised of d secrecy levels $L = \{l_1, l_2, \cdots, l_d\}$ among n participants. The function $f(\Gamma_{Qual}, L) : \Gamma_{Qual} \to L$ decides the associated secrecy levels with certain qualified sets. Allocating the secrecy level L_X to the corresponding qualified set $X \in \Gamma_{Qual}$, where $L_X \subset L$. The encoding matrices LK_i^0 and LK_i^1 of RIVCS for GAS is valid if the following conditions hold.

(1) $\left|LK_i^0\right| = \left|LK_i^1\right|$, $1 \le i \le d$.

(2) $\forall F \in \Gamma_{Forb}$, $H\left(\mathrm{XOR}(LK_i^0[F])\right) = H\left(\mathrm{XOR}(LK_i^1[F])\right)$, $1 \le i \le d$.

(3) $\forall X \in \Gamma_{Qual}$, $H\left(\mathrm{XOR}(LK_i^1[X])\right) = H\left(\mathrm{XOR}(LK_i^0[X])\right)$, $l_i \notin L_X$.

(4) $\forall X \in \Gamma_{Qual}$, $H\left(\mathrm{XOR}(LK_i^1[X])\right) > H\left(\mathrm{XOR}(LK_i^0[X])\right)$, $l_i \in L_X$.

(5) $LK_1^0 = LK_2^0 = \cdots = LK_d^0$.

The 1st condition shows that all the encoding matrices for white and black pixels need to gain the same amount of columns. In the 2nd condition, XOR-ing all the shares in a forbidden set gives no clue about the secret. The 3rd and 4th conditions demonstrate that XOR-ing all the shares in a qualified set X can only decrypt the secrecy level l_i ($l_i \in L_X$). Meanwhile, the recovered secrecy levels are guaranteed to reveal the correct color by the 4th condition. By the 3rd condition, the not-yet-revealed secrecy levels remain imperceptible. The areas where no secret is revealed are noise-like due to the 5th condition, which assures that the number and locations of not-yet-revealed secrets are unknown to users. The pixel expansion m and contrast α_X of restored R_i by the qualified set X are as follows.

$$\begin{cases} m = \left|LK_i^0\right| \\ \alpha_X = H(\mathrm{XOR}(LK_i^1[X])) - H(\mathrm{XOR}(LK_i^0[X])) \big/ \left|LK_i^0\right| \end{cases}.$$

The former determines the size of shares and the latter reflects the clear of recovered images. Therefore, the VCS of a smaller pixel expansion and a larger contrast are better received.

2.2. Secrecy level allocation algorithm

Based on the former definition, we explore a secrecy level allocation algorithm using Γ_0 as the basis. Input a secret image with d secrecy levels and our AS. The total minimal qualified sets are allocated with certain original secrecy levels using the sharing strategy. The designed follow algorithm can calculate the secrecy regions for the remaining qualified sets.

```
Algorithm 1 Secrecy level allocation algorithm
Input: The secrecy levels $l_1, l_2, \cdots, l_d$, the $(\mathit{\Gamma}_{Qual}, \mathit{\Gamma}_{Forb})$, and the sharing strategy.
Output: The minimal qualified set $A_i$ for sharing $R_i$, $1 \le i \le d$.
Step1: Select each qualified set $X$ from the residual set $\{\mathit{\Gamma}_{Qual} - \mathit{\Gamma}_0\}$, calculate the total minimal qualified sets $Q_{i1}, Q_{i2}, \cdots, Q_{im} \subset X$.
Step2: Allocate the secrecy levels with $X$ using $L_X = L_{Q_{i1}} \bigcup L_{Q_{i2}} \bigcup \cdots \bigcup L_{Q_{im}}$.
Step3: Gain the minimal qualified set $A_i$ for encoding region $R_i$, $1 \le i \le d$.
```

2.3. Encoding matrix construction

Since RIVCS's construction is based on single-secret sharing VCS. We first present the encoding matrices construction for single-region, as shown in Step 1-Step 2. According to the secrecy level allocation algorithm, when sharing R_i $(1 \le i \le d)$, the minimal qualified is A_i. Let $T_0^{A_i}$ and $T_1^{A_i}$ be the white and black matrices of XOR-based VCS for sharing R_i. The result of any element in set {0. 1} XOR-ing "0" is invariable due to $0 \otimes 0 = 0,\ 1 \otimes 0 = 1$. Based on this, $T_0^{A_i}$ and $T_1^{A_i}$ can be generated using the matrices of $(a_i, a_i) -$ VCS, $a_i = |A_i|$.

To construct LK_i^0 and LK_i^1, we link total white matrices $T_0^{A_i}$ to generate LK_i^0. Using $T_1^{A_i}$ instead of $T_0^{A_i}$ in LK_i^0 to construct LK_i^1. The formal construction is shown as follows.

```
Algorithm 2 Encoding matrix construction algorithm
Input: The set $P = \{1, 2, \cdots, n\}$, the (Γ_{Qual}, Γ_{Forb}), and the sharing strategy.
Output: Encoding matrices $LK_i^0$ and $LK_i^1$, $1 \le i \le d$.
Step1: Employ the secrecy level allocation algorithm (Algorithm 1) to calculate the minimal qualified set $A_i$ for encoding $R_i$.
Step2: Select each minimal qualified set $A_i = \{i_1, i_2, \cdots, i_{a_i}\}$. Construct $a_i \times 2^{a_i - 1}$ encoding matrices $S_0^{(a_i, a_i)}$ ($S_1^{(a_i, a_i)}$) of optimal ($a_i$, $a_i$)-VCS [1].
Step3: Construct a $n \times 2^{a_i - 1}$ matrix $T_0^{A_i}$ ($T_1^{A_i}$, resp.), where the $i_x$-th $(1 \le x \le a_i)$ row of $T_0^{A_i}$ ($T_1^{A_i}$, resp.) is the $i_x$-th row of $B_0^{(a_i, a_i)}$ ($B_1^{(a_i, a_i)}$, resp.), and residual rows in set {P–A_i} with all elements = 0.
Step4: Concatenate $T_0^{A_i}$ ($T_1^{A_i}$, resp.), and get $LK_i^0$ ($LK_i^1$, resp.) as
    $LK_i^0 = \left[T_0^{A_1} \| T_0^{A_2} \| \cdots \| T_0^{A_d}\right], LK_i^1 = \left[T_1^{A_i} \middle| LK_i^0 - T_0^{A_i}\right]$.
```

3. Examples and discussions

This section exhibits the experiment results to illustrate the availability of our approaches. In addition, some comparisons as well as discussions are presented as well.

3.1. Experiments

Let $P = \{1, 2, 3, 4\}$, $L = \{l_1, l_2, l_3\}$ and $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}$. From our sharing rules, the sets {1, 2}, {1, 3} and {1, 4} are initially allocated with l_1, l_2, and l_3 respectively. The set {2, 3, 4} is initially allocated with both initial l_2 and l_3. The secret image containing three secrecy levels is prepared.

The secret image adopts three different halftone situation images regarding network security as the confidential patterns for three regions. More specifically, the low-level region R_1 is the pie chart indicating the amount distribution of attack types such as the worm attacks, DoS attacks, brute attacks and the scanning attacks. The mid-level region R_2 reflects the amount distribution of security events in the recent year for different subnets of business services i.e., the Web servers area, the File servers area and the User host area, etc. The high-level region R_3 illustrates the cure in terms of real-time network traffic.

In practical application, assume that the master security manager is P_1 and three assistant managers are P_2, P_3 and P_4. Let R_1 has a higher order of secrecy compared with R_2, R_3 and R_4. Based on our sharing strategy, the master manager has the highest priority. That is to say, he can decode any secrecy levels with his individual assistants. However, any two assistants cannot recover any secrecy levels. Two secrecy levels can be exactly decrypted when any three shares from are obtained. All of them can restore all three secrecy levels together. The above complicated sharing strategies cannot be executed using the previous approaches, while is solved in this paper.

We first employ the Algorithm 1 to complete the security allocation, the quantified sets {1, 2, 3}, {1, 2, 4} and {1, 3, 4} are allocated with $\{l_1, l_2\}$, $\{l_1, l_3\}$ and $\{l_2, l_3\}$ respectively, and {1, 2, 3, 4} is allocated with $\{l_1, l_2, l_3\}$. Furthermore, we calculate that the minimal qualified sets for decoding R_1, R_2 and R_3 are {1, 2}, {{1, 3}, {2, 3, 4}} and {{1, 4}, {2, 3, 4}} respectively. Namely, A_1={1, 2}, A_2={{1, 3}, {2, 3, 4}} and A_3={{1, 4}, {2, 3, 4}}. Obviously, not every share is with the same priority. In addition, the encoding matrices for RIVCS using Algorithm 2 are generated as follows.

We construct the encoding matrices with (2, 2)-VCS and (3, 3)-VCS using the Step 1 of Algorithm 1 as follows.

$$B_0^{\{2,2\}}=\begin{bmatrix}1&0\\1&0\end{bmatrix},B_1^{\{2,2\}}=\begin{bmatrix}1&0\\0&1\end{bmatrix},B_0^{\{3,3\}}=\begin{bmatrix}0&1&1&0\\0&1&0&1\\0&0&1&1\end{bmatrix},B_1^{\{3,3\}}=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}.$$

Then we can get $(T_0^{A_1},T_1^{A_1})$, $(T_0^{A_2},T_1^{A_2})$ and $(T_0^{A_3},T_1^{A_3})$ using the Step 3 of Algorithm 1 as follows.

$$T_0^{A_1}=\begin{bmatrix}1&0\\1&0\\0&0\\0&0\end{bmatrix},T_1^{A_1}=\begin{bmatrix}1&0\\0&1\\0&0\\0&0\end{bmatrix},T_0^{A_2}=\begin{bmatrix}1&0&0&0&0&0\\0&0&0&1&1&0\\1&0&0&1&0&1\\0&0&0&0&1&1\end{bmatrix},T_1^{A_2}=\begin{bmatrix}1&0&0&0&0&0\\0&0&1&0&0&1\\0&1&0&1&0&1\\0&0&0&0&1&1\end{bmatrix},$$

$$T_0^{A_3}=\begin{bmatrix}1&0&0&0&0&0\\0&0&0&1&1&0\\0&0&0&1&0&1\\1&0&0&0&1&1\end{bmatrix},T_1^{A_3}=\begin{bmatrix}1&0&0&0&0&0\\0&0&1&0&0&1\\0&0&0&1&0&1\\0&1&0&0&1&1\end{bmatrix}.$$

After concatenating the above matrices according to the Step 4 of Algorithm 1, we can generate the final encoding matrices as follows.

$$LK_1^0=LK_2^0=LK_3^0=\left[T_0^{A_1}\,||T_0^{A_2}\,||T_0^{A_3}\right]=\begin{bmatrix}1&1&1&0&0&0&0&0\\1&0&0&0&0&1&1&0\\0&1&0&0&0&1&0&1\\0&0&1&0&0&0&1&1\end{bmatrix},$$

$$LK_1^1=\left[T_1^{A_1}\left|LK_1^0-T_0^{A_1}\right.\right]=\begin{bmatrix}1&1&1&0&0&0&0&0\\0&0&0&1&0&1&1&0\\0&1&0&0&0&1&0&1\\0&0&1&0&0&0&1&1\end{bmatrix}$$

$$LK_2^1=\left[T_1^{A_2}\left|LK_2^0-T_0^{A_2}\right.\right]=\begin{bmatrix}1&1&1&0&0&0&0&0\\1&0&0&0&1&0&0&1\\0&0&0&1&0&1&0&1\\0&0&1&0&0&0&1&1\end{bmatrix},LK_3^1=\left[T_1^{A_3}\left|LK_3^0-T_0^{A_3}\right.\right]=\begin{bmatrix}1&1&1&0&0&0&0&0\\1&0&0&0&1&0&0&1\\0&1&0&0&0&1&0&1\\0&0&0&1&0&0&1&1\end{bmatrix}.$$

According to LK_1^0, we can observe that the pixel expansion m=8. The calculations of $H\left(\text{XOR}(LK_i^t[X])\right)$ is shown in Table 1. When X = {1, 2}, only R_1 is revealed with contrast 1/4, when X = {1, 3}, R_2 is restored with contrast 1/4. For X={1, 4}, R_2 is restored with the same contrast 1/4. Both R_1 and R_2 can be recovered with $a=1/4$

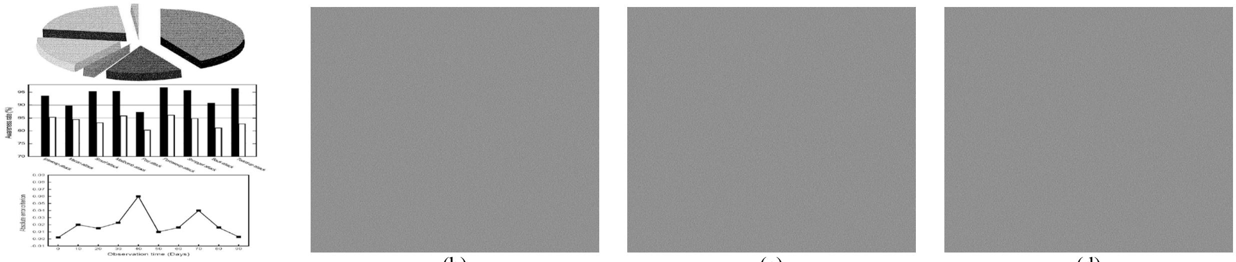
by {1, 2, 3}. R_1 and R_3 can be decoded with $a = 1/4$ by {1,2,4}. When X = {1, 3, 4} and {2, 3, 4}, both R_2 and R_3 can be restored with $a = 1/4$ and $a = 1/2$ respectively. R_1, R_2 and R_3 are decoded with 1/8, 3/4 and 3/4 respectively when XOR-ing all the generated shares. Otherwise, the secret image cannot be recovered.

Table 1.Calculations of $H\left(\mathrm{XOR}(LK_i^t[X])\right)$ in the experiment

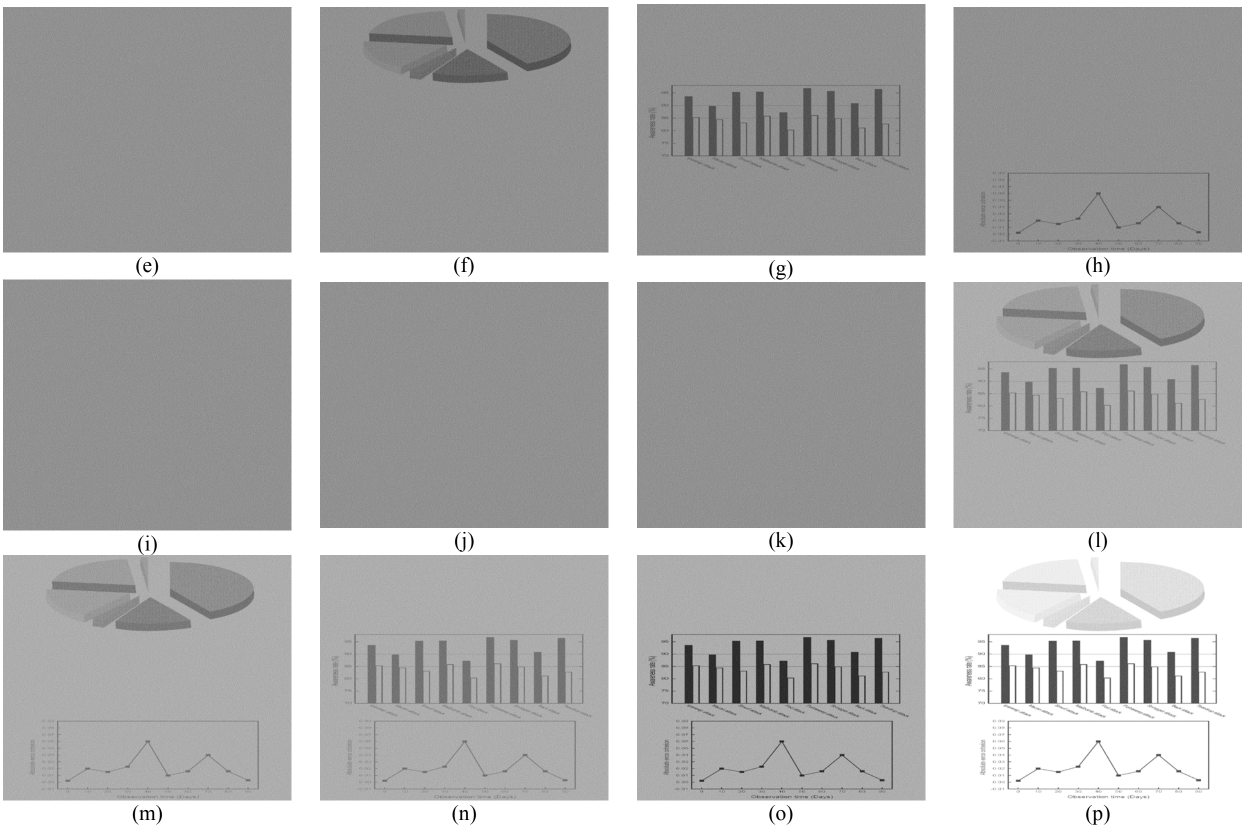
H(V)	Participant set *X*				
	{1}	{2}	{3}	{4}	{1, 2}
LK_1^0	3	3	3	3	4
LK_1^1	3	3	3	3	6
LK_2^1	3	3	3	3	4
LK_3^1	3	3	3	3	4
	{1, 3}	{1, 4}	{2, 3}	{2, 4}	{3, 4}
LK_1^0	4	4	4	4	4
LK_1^1	4	4	4	4	4
LK_2^1	6	4	4	4	4
LK_3^1	4	6	4	4	4
	{1, 2, 3}	{1, 2, 4}	{1, 3, 4}	{2, 3, 4}	{1, 2, 3, 4}
LK_1^0	3	3	3	3	0
LK_1^1	5	5	3	3	1
LK_2^1	5	3	5	7	6
LK_3^1	3	5	5	7	6

The simulated results are presented in Fig. 1. The four generated shares are distributed through the public communication network to the corresponding master security manager and his assistants respectively. After receiving the shares, different combinations of participants can decode certain regions by XOR-ing their shares together.

In this way, if an image share falls into the wrong hands, it would look like an image of random noise to guarantee that its secret is inaccessible. By Table 1 and Fig. 1, we can see that our method is feasible as expected. Besides, when XOR-ing all the shares as shown in Fig. 1 (p), we can see that the original white pixels can be revealed perfectly. In summary, the experiments present the feasibility and flexibility of the proposed RIVCS for confidentiality protection of situation visualization in network security.



(a) (b) (c) (d)



(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

Fig. 1. The experiment with 3 secrecy levels. (a) secret image, (b)-(e) four shares S_1, S_2, S_3, S_4, (f) $S_1 \otimes S_2$, (g) $S_1 \otimes S_3$, (h) $S_1 \otimes S_4$, (i) $S_2 \otimes S_3$, (j) $S_2 \otimes S_4$, (k) $S_3 \otimes S_4$, (l) $S_1 \otimes S_2 \otimes S_3$, (m) $S_1 \otimes S_2 \otimes S_4$, (n) $S_1 \otimes S_3 \otimes S_4$, (o) $S_2 \otimes S_3 \otimes S_4$, (p) $S_1 \otimes S_2 \otimes S_3 \otimes S_4$.

We forward give the visual quality of different regions using our technology for different access structures. Contrast results of secrecy levels using our approach are presented in Table 2, where various cases are taken into account. The calculations of contrast are achieved based on the Definition 2, which is marked using α in Table 2. We organize the set Γ_0 with different original secrecy levels in the 2nd column of Table 2. From Table 2, major contrasts are over 0.1, which implies that good resolution is achieved. Moreover, our scheme is suitable to different occasions, which further introduce the flexibility of our proposed method.

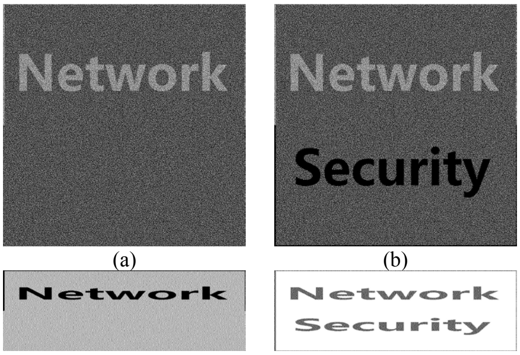
Table 2.Contrasts of the proposed RIVCS for different GASs

$\lvert P \rvert$	Γ_0 with initial secrecy levels	Contrast		
		L_1	L_2	L_3
3	$\{1,2\}=L_1$ $\{1,3\}=L_2$	$\alpha_{1,2}=1/2$ $\alpha_{1,2,3}=1/2$	$\alpha_{1,3}=1/2$ $\alpha_{1,2,3}=1/2$	–
3	$\{1,2\}=L_1$ $\{2,3\}=\{L_1, L_2\}$	$\alpha_{1,2}=1/3, \alpha_{2,3}=1/3, \alpha_{1,2,3}=2/3$	$\alpha_{2,3}=1/3, \alpha_{1,2,3}=1/3$	–
3	$\{1,2\}=L_1$ $\{1,3\}=L_2$ $\{2,3\}=L_3$	$\alpha_{1,2}=1/3$, $\alpha_{1,2,3}=1/3$	$\alpha_{1,3}=1/3$, $\alpha_{1,2,3}=1/3$	$\alpha_{2,3}=1/3$, $\alpha_{1,2,3}=1/3$
3	$\{1,2\}=L_1$ $\{1,3\}=L_2$ $\{2,3\}=\{L_1, L_3\}$	$\alpha_{1,2}=1/4, \alpha_{2,3}=1/4, \alpha_{1,2,3}=1/2$	$\alpha_{1,3}=1/4, \alpha_{1,2,3}=1/4$	$\alpha_{2,3}=1/4, \alpha_{1,2,3}=1/4$
4	$\{1,2\}=L_1$ $\{1,3\}=L_2$	$\alpha_{1,2}=1/2, \alpha_{1,2,3}=1/2$ $\alpha_{1,2,4}=1/2, \alpha_{1,2,3,4}=1/2$	$\alpha_{1,3}=1/2, \alpha_{1,2,3}=1/2$ $\alpha_{1,3,4}=1/2, \alpha_{1,2,3,4}=1/2$	–

4	{1,2}=L_1 {1,3,4}=L_2	$\alpha_{1,2}=1/3, \alpha_{1,2,3}=1/3$ $\alpha_{1,2,4}=1/3, \alpha_{1,2,3,4}=1/3$	$\alpha_{1,3,4}=2/3, \alpha_{1,2,3,4}=2/3$	–
4	{1,2}=L_1 {1,3}=L_2 {1,4}=L_3	$\alpha_{1,2}=1/3, \alpha_{1,2,3}=1/3$ $\alpha_{1,2,4}=1/3, \alpha_{1,2,3,4}=1/3$	$\alpha_{1,3}=1/3, \alpha_{1,2,3}=1/3$ $\alpha_{1,3,4}=1/3, \alpha_{1,2,3,4}=1/3$	$\alpha_{1,4}=1/3$, $\alpha_{1,2,4}=1/3$ $\alpha_{1,3,4}=1/3, \alpha_{1,2,3,4}=1/3$
4	{1,2,3}=L_1 {1,2,4}=L_2 {2,3,4}=L_3	$\alpha_{1,2,3}=2/17$, $\alpha_{1,2,3,4}=2/17$	$\alpha_{1,2,4}=2/17, \alpha_{1,2,3,4}=2/17$	$\alpha_{2,3,4}=2/17$, $\alpha_{1,2,3,4}=2/17$
3	{1,2,3}=L_1 {1,2,4}=L_2 {1,3,4}={L_1,L_3}	$\alpha_{1,2,3}=1/4$ $\alpha_{1,3,4}=1/4, \alpha_{1,2,3,4}=1/2$	$\alpha_{1,2,4}=1/4, \alpha_{1,2,3,4}=1/4$	$\alpha_{1,3,4}=1/4, \alpha_{1,2,3,4}=1/4$
4	{1,2}=L_1 {1,3}=L_2 {1,4}=L_3 {2,3,4}={L_2,L_3}	$\alpha_{1,2}=1/7, \alpha_{1,2,3}=1/7$ $\alpha_{1,2,4}=1/7, \alpha_{1,2,3,4}=1/7$	$\alpha_{1,3}=1/7$ $\alpha_{1,2,3}=1/7, \alpha_{1,3,4}=1/7$ $\alpha_{2,3,4}=2/7, \alpha_{1,2,3,4}=3/7$	$\alpha_{1,4}=1/7, \alpha_{1,2,4}=1/7$ $\alpha_{1,3,4}=1/7, \alpha_{2,3,4}=2/7$ $\alpha_{1,2,3,4}=3/7$

3.2. Comparisons and discussions

Fig. 2 illustrates the comparison of visual performance between our approach with Shyu et al's scheme [5] for three participants sharing a secret image with two secret level regions (by using halftone security situation graph as secret patternes for two regions). We can see that the color of first region (**Network**) is incorrect in [5] (Fig. 2 (a) (b)), while it is overcame in our scheme (Fig. 2 (c) (d)). Meanwhile, the background of secret image in the proposed method (Fig. 2 (d)) can be restored perfectly by collecting all the three shares. Besides, the size of restored image of our scheme is also smaller than Shyu et al's scheme. Therefore, the storage and transmission cost of shares can be decreased efficiently by the proposed method.



(a) (b)

(c) (d)

Fig. 2. Comparisons of visual quality of the recovered images for (2, 3)-RIVCS between Shyu et al. [5] and our approach. (a)-(b): stacking two and three shares by scheme [5] respectively. (c)-(d): stacking two and three shares by our scheme, respectively.

Table 3.Performance comparisons among our approach and other related methods

Performance	Schemes				
	Ref.[4]	Ref.[5]	Ref.[6]	Ref.[8]	Our scheme
Access structure	(2, n) n = 3, 4, 5	(2, n)	(k, n)	(k, n)	GAS
Right color	No	No	Yes	Yes	Yes

Lossless restore	No	No	No	No	Partial region
Secrecy levels restored based on	Amount of shares	Amount of shares	Amount of shares	Amount of shares	Qualified set
Shares with unequal priority	No	No	No	No	Yes

Table 3 organizes the performance comparisons among the proposed RIVCS and other related schemes. Some conclusions can be summarized as follows.

- Rich application scenarios. The proposed method is capable for general access structure. Moreover, different shares are with different preferences in our scheme, which is superior to [4-6] [8]. Meanwhile, the secrecy levels are recovered based on Γ_0. Therefore, complex sharing strategies can be executed by ours in visualization system.
- Better visual performance. Our method achieved the restored secret image with correct color. However, the reserve-color problem still exists in [4-5]. Moreover, enhanced contrast and perfect recovery of white pixels can be achieved by XOR operation, which is superior to [6] [8]. Therefore, the privata information in the secret image can be clearly and precisely identified by our method if it is applied to visualization system for nework security situation awareness.

4. Conclusion

Since transmitted image data in visualization system of network security situation usually bring different secrecy levels of confidential information, which directly related with the network behaviors information and network security situation. Since the existing protection mechanisms are limited in conventional cryptography need complex computational device and cryptographic knowledge in decryption. We present a multi-level security privacy protection scheme based on RIVCS. The general constructions for RIVCS are presented in detail in this paper. Our method obtains advantages including complex sharing strategies, lossless recovery of white pixels, high contrast and better visual performance. Experiments verify the feasibility and flexibility of the proposed scheme.

References

1. M. Naor, A. Shamir. 1995. Visual cryptography. Advances in Cryptology-Eurocrypt'94, Berlin, LNCS 950: 1–12.
2. S. Droste. 1996. New results on visual cryptography. In Proc. Advances in Cryptography-CRYPTO'96, :401–415.
3. G. Ateniese, C. Blundo, A. D. Santis, et al. 1996. Visual cryptography for general ASs. Information and Computation. 129(2):86–106.
4. R. Z. Wang. 2009. Region incrementing visual cryptography. IEEE Signal Process. Letter. 16(8):659–662.
5. S. J. Shyu, H. W. Jiang. 2012. Efficient construction for region incrementing visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology. 22(5):769–777.
6. C. N. Yang, H. W. Shih, C. C. Wu, L. Harn. 2012. k out of n region incrementing scheme in visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology. 22(5):799–810.
7. H. Hu, G. Shen, Z. Fu, B. Yu, et al. 2016. General construction for XOR-based visual cryptography and its extended capability. Multimedia Tools and Applications, 75(21), 13883-13911.
8. G. S. Zhong, J. J. Wang. 2013. Region incrementing visual secret sharing scheme based on random grids. Proceedings of IEEE International Symposium on Circuits and Systems, Los Alamitos: IEEE Computer Society Press, 2351–2354.
9. T. Chen, K. Tsao. 2011. Threshold visual secret sharing by random grids. The Journal of Systems and Software. 84:1197–1208.
10. R. D. Prisco, A. D. Santis. 2014. On the relation of random grid and deterministic visual cryptography. IEEE Transactions on Information Forensics and Security. 9(4):653–665.
11. C. N. Yang, C. C. Wu, D. S. Wang. 2014. A discussion on the relationship between probabilistic visual cryptography and Random Grid. Information Sciences. 278:141–143.