A Verifiable Visual Cryptography Scheme Using Neural Networks

Deng Yuqiao  
Guangdong University of Business Studies,  
Mathematics and Computer Science College  
Guangzhou, China  
e-mail: dengyuqiao80@yahoo.cn

Song Ge  
Harbin Institute of Technology Shenzhen Graduate School  
Shenzhen, China  
e-mail: carroll0708@qq.com

Abstract—This paper proposes a new verifiable visual cryptography scheme for general access structures using pi-sigma neural networks (VVCS-PN), which is based on probabilistic signature scheme (PSS), which is considered as security and effective verification method. Compared to other high-order networks, PSN has a highly regular structure, needs a much smaller number of weights and less training time. Using PSN’s capability of large-scale parallel classification, VVCS-PN reduces the information communication rate greatly, makes best known upper bound polynomial, and distinguishes the deferent information in secret image. 

Keywords- Pi-sigma neural networks, visual cryptography, general access structure

I. INTRODUCTION

The visual cryptography scheme (VCS) is firstly presented by Naor [1], it’s no need for the scheme to any cryptology knowledge and computation, so it aroused the experts’ interest. Subsequently, a visual cryptography scheme is constructed by Eric R. Verheul et al. for general access structures by expanding Naor’s scheme [2], and studied its related properties, and then presented color VCS [3]. Yi Feng et al. also proposed the color VCS for general access structure with minimal expanded pixels [4]. Moreover, after the concept of verifiable secret sharing (VSS) was first introduced in 1985 by B. Chor [5], many verifiable secret sharing and verifiable multi-secret sharing are proposed. the two classic non-interactive schemes are proposed by Feldman [6] and its improve scheme by Pedersen [7][8], which use a commitment scheme to guard credibility of dealer and participants. Theodore M. Wong et al. presented a new verifiable secret sharing which can guard against dynamic adversaries and can dynamic update, that is new participant can dynamic update, that is new participant and of considering importance of all part in secret image as the same, the most known VCS has large limitation in flexibility and security in practical application.

In order to solve the above problem, this paper presents a new verifiable visual cryptography scheme (VVCS) for general access structures using pi-sigma neural networks (VVCS-PN) [17]. The scheme combine the technology of pi-sigma neural network to complete the procedure of sharing and the concept of RSA digital signature to verification. RSA digital signature can confirm the participants identification, ensure the validity of message, and validate the compilikation of information. Using neural networks to solve secret sharing problem is not only the important aspect of application of neural networks, but also a new aspect of secret sharing theoretical study. It provides a new angle and thinking on secret sharing theory. VVCS-PN considers the procedure of visual secret sharing as a classification procedure. The obvious advantages of this scheme are the smaller redundancy of the size of shares, the polynomial best known upper bound, and the simply recovering processing. In addition, because of omitting the weight of participant and of considering importance of all part in secret image as the same, the most known VCS has large limitation in flexibility and security in practical application.

This paper firstly introduces the structure of PSN, and then construct the VVCS-PN, and analysis its security and capability.
Hypothesis 2: According to the property of secret image, divide it into m sub-image $I_1, I_2, \ldots, I_m$ using region-based segmentation, and label sub-image $I_i$ again according to its importance, as $I_1 \geq I_2 \geq \ldots \geq I_m$, where $I_1 \cup I_2 \cup \ldots \cup I_m = I$.

Hypothesis 3: Define participant set $P = \{P_1, P_2, \ldots, P_n\}$, and participant identification set $A_i = \{p_{i1}, p_{i2}, \ldots, p_{ik}\}$, where $p_{ij}$ is a participant in $A_i$, $k$ is threshold. $A_j \cup A_k \cup \ldots \cup A_t = P$ and $A_i \cap A_j = \emptyset$, where $1 \leq i, j \leq k$.

Divide $(A_1, A_2, \ldots, A_t)$ into $r$ ranks by their importance, and remark $A_j$ represents the $j$-th component of the $i$-th rank. Definition the importance of $A_{ij}$, which is given by:

$A_{ij} = \begin{bmatrix} A_{i1} & A_{i2} & \ldots & A_{iD_1} \\ A_{i2} & A_{i2} & \ldots & A_{iD_2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{ir} & A_{ir} & \ldots & A_{irD_r} \end{bmatrix}$

(1)

Where $D_1', D_2', \ldots, D_r'$ is the number of each rank, $A_{ij}$ represents the $j$-th component of the $i$-th rank. Definition the importance of $A_{ij}$: $A_j > A_{j+1} > \ldots > A_t$ and $A_j = A_{ik}$. Note that each participant only belongs to one identification set.

Hypothesis 4: A minimal qualified component in each sub-image $I_i$ is given by:

$\phi_i^t = \left\{ \bigcup_{A_{jk}} \bigcup_{A'_{k'}} \mid A_{jk} \in F_{qual}-, \text{ for all } A'_{k'} \subset \bigcup A_{jk}, A'_{k'} \in F_{qual}^t \right\}$

(2)

Where $1 \leq i \leq m, 1 \leq k \leq r, 1 \leq j \leq D_k'$. $A_{jk}$ represents the $j$-th rank of $A_k$, which can recover the $i$-th sub-image, in the $k$-th rank. $\Gamma_{qual}^t$ denotes the qualified set of $I_i$.

B. Image segmentation

Using region-based segmentation to split the image, the steps are as follows: firstly, select a suitable predicate $P$, and then divide the image into quadrants at a time until all are areas $I_i, P(I_i) = \text{TURE}$. Note that, for $I_i, I_j, I_i \cup I_j = \emptyset$. As the secret image divided two times for example, the result is shown in figure 2. Finally, encode all the sub-image $I_i$ using decimalization encoding method.

C. Pi-sigma neural network architecture

Take one minimal qualified component $\phi_i^t$ for example, the pi-sigma neural networks applied to visual cryptography scheme are shown in figure 3.

In input layer, $P_0$ is fixed in 1, and other unit $P_j$ is corresponded with an participant $P_j$, so there are $n+1$ input units in this layer; in hidden layer, after remarking all identification sets $A_j$ to $P_j$, each hidden unit $A_j$ is corresponded with an identification set $A_j$. This layer has 1 neural networks in all; in output layer, each output unit $I_i$ represents a sub-image $I_i$, so this layer has $m$ neural networks in all.

The weight $w_{0j}$ which is between input unit $P_0$ and the $j$-th hidden unit $A_j$, is the threshold of $A_j$. Weight links between all the input units except $P_0$ and hidden units represent the participant is affiliated with one identification set. $w_{ij}$ represents the weight from i-th input unit to j-th hidden unit.

![Figure 1. the result of region-based segmentation](image1)

![Figure 2. the suitable PSN architecture](image2)

In accordance with the minimal qualified component for each sub-image, determine weight link between hidden layer and output layer. If $A_j \in \phi_i^t$, there is a weight link between hidden unit $A_j$ and output unit $I_i$, and the value of weight is fixed in $I_i$.

Considering sub-image $I_i$ is much smaller than secret image and the compression of PSN. Each share can be much smaller than that of traditional schemes. For example, if a secret image is 256*256, and splits into 16 sub-images (64*64). So the input unit should be prescribed not bigger than 64*64 which can satisfy the requirement. Obviously, this is more convenient to verifications and has lower information rate.

D. Training pi-sigma neural networks

1) The mean squared error (MSE): MSE is adopted as the aim error, which is given by:

$e^2 = \frac{1}{m} \sum_{j=1}^{m} (f_j^p - I_j^p)^2$.

(3)

Where $f^p$ represents the desired output for the $p$-th pattern, which is the code of the $j$-th sub-image. $f^p$ denotes the training output for the $p$-th pattern, that is

$I_j^p = f(\prod_{i=1}^{m} A_{i}^p)$.

(4)

2) Activation function: The PSN uses sigmoid activation function

$f(x) = \frac{1}{1+e^{-x}}$.

(5)
and modifies weights using conjugate gradient method. This method is gradient descent (which usually can acquire only local optimum solution) improvement method, and has comparatively less computation times. So it is an effective method.

3) Training arithmetic and shares generation

Step1: initialize parameter; define learning rate, maximal iteration times $N$, and permissible error $e$. etc.

Step2: dealer select input data $p = (I, p_1, p_2, ..., p_n)$ randomly, and initialize the weight of value $w_j^0 = 1$.

Step3: if $(n < N)$

Step4: for: compute the output data $I_i$ for each output unit, and compute $MSE$ $e^i$.

Step5: modify one set of $w_j = (w_{0j}, w_{1j}, ..., w_{nj})^T$ according to conjugate gradient method.

Step 6: until $e^2 < e$.

Step 7: end if.

Step 8: else carry though the step 2-7.

After pi-sigma network is stabile, shares are generated from each input unit, that is $S_i = (p_i, w_j)$

E. Dealer Signature Generation

All the parameter hypothesis is just like $w$

Dealer computes the signed function for each shares $S_i$ as follows:

Choose $r \in \{0, 1\}^k$ randomly, and compute $w = H(S_i || r)$;

Compute $r^* = G_1(w) \oplus r$;

Compute $y = 0||w||r*||G_2(w)$

Compute $U_i = \text{sig}(S_i) = yd \mod n$

publicize dealer’s public key $\text{keypub} = (N, e)$

F. Dealer verification and Share distribution

Distribute the shares-signature pairs $(S_i, U_i)$ to the i-th participant, where $S_i = (p_i, w_j)$ with $p_i$ a set of random numbers, $w_j$ the weight from the i-th input units to the j-th output units, and signed function $U_j$.

In order to ensure whether dealer is honest and the shares is credible, each participant use verified function as follows:

$y = U_i^r \mod N$

Parse $y = b||w||r^*||y'$, where $|b| = 1$, $|w| = k_1$, $|r^*| = k_0$, $|y'| = k-k_0-k_1-1$.

Compute $r = r^* \oplus G_j(w)$

If $(H(S_i || r) = w \land G_j(w) = y \land b = \theta)$

Return (TURE);

Else return (FALSE)

If the result is TURE, participants receive the shares, and verification is passed, otherwise they broadcast their complaint about dealer. When complaints are over threshold $\Theta$, dealer is inferred as dishonest.

If a participant not belongs to the minimal qualified component, his share is obtained randomly, and the size of it is similar to other participant who belongs to it.

G. Visual secret recovering

When secret image should be recovered, the participant, whose shares are trained with PSN, collect their shares together through secrecy channel (to avoid existential forgery). Each participant simultaneously compute verified function using $\text{keypub}$ to verify the creditability of the shares. If all the shares are considered as truth, recover the secret image.

The recovering efficiency of VCSPSN is high. Input the shares into the input layer, the output data is the recovering sub-image. After connecting all the sub-image and decoding it, we will get the recovering image.

III. CONCLUSION

This paper combines the technology of neural networks and the theory on visual cryptography, proposes the visual cryptography scheme using pi-sigma neural networks, and analysis this scheme. VCSPSN is not only a secure scheme, but also a lower communication rate, more flexible scheme. At present, neural networks have already been a new method in information security field, and have been a new technology with tremendous developing potential. As the deeply studying on theory and application of neural networks, it will infuse a new activity in visual cryptography researching.

IV. ACKNOWLEDGMENT

This work was supported by Foundation for Distinguished Young Talents in Higher Education of Guangdong under Grant No.LYM11068

REFERENCES


