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 (VVCSPSN), 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, VCSPSN 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 schemes 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 guards against dynamic adversaries and can dynamic update, that is new participant should verify the validity of their shares after redistribution between different shreshold schemes[9]. Hsu el at.[10] present a new authenticated scheme based on discrete logarithms, which combine the merits of digital signature scheme and verifiable secret sharing scheme.

However, though having verifiable secret sharing schemes, most of the visual cryptography schemes nowadays are non-verifiable, that is , the schemes are based on the hypothesis –the dealer and participant trust each other completely and all of them are assumed to be honest. Obviously, its hypothesis is not secure in practical application. Moreover, the best known upper bound on the share size of the most known VCS is exponential[11]. That means the size of the shares is expanded exponentially as the secret image expanded, the amount of the shares is increased exponentially as the secret image increased, and the amount of expended pixels (that is the subtraction between the size of the secret image and of its one share) is very large. Besides, the high complexity of the recovering image leads to the less efficiency of VCS. 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.

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 (VVCSPSN)[17]. The scheme combine the technology of pi-sigma netural 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 complication 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. VCSPSN 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. All of these contribute to decreasing the times of computation and communication, advancing the efficiency of VCS. Moreover, the sub-image trained in PSN is independent and parallel, so it is available to rank the sub-image and improve the flexibility of scheme.

This paper firstly introduces the structure of PSN, and then construct the VVCSPSN, and analysis its security and capability.

II. A VISUAL CRYPTOGRAPHY SCHEME USING PI-SIGMA NEURAL NETWORKS

A. Visual cryptography schemes hypothesis

Hypothesis 1: The pixel matrix of secret image $I=\{I_{ij}\}$ is defined in finite field F_q, where $q=2$, when I is B&W image; $q=2^8$, and $I_{ij}=\{R,G,B\}$, $0\le\{R,G,B\}\le 255$ and $R=G=B$, when I is grey level image; $q=2^{24}$, and $I_{ij}=\{R,G,B\}$, $0\le(R,G,B)\le 255$, when I is color image.

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. $A_1 \cup A_2 \cup \ldots \cup A_l = P$ and $A_i \cap A_j = \varnothing$, where $1 \leq i, j \leq K$. Divide $(A_1, A_2, \ldots A_l)$ into r ranks by their importance, and remark A_i

$$\begin{Bmatrix} A_{11} & A_{12} & \ldots & A_{1D^1} \\ A_{21} & A_{22} & \ldots & A_{2D^2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{rl} & A_{rl} & \ldots & A_{rD^r} \end{Bmatrix} \quad (1)$$

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} : $A_1 \cdot > A_2 \cdot > \ldots > A_r \cdot$. and $A_{ij} = A_{ik}$. 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:

$$\phi_i^t = \left\{ \cup A_{jk}^i \middle| \cup A_{jk}^i \in F_{Qual}^i, for \ \ all \ \ A^{i'} \subset \cup A_{jk}^i, A^{i'} \notin F_{Qual}^i \right\} \quad (2)$$

Where $1 \leq i \leq m, 1 \leq k \leq r, 1 \leq j \leq D^k$. A_{jk}^i represents the j-th identification set, which can recover the i-th sub-image, in the k-th rank. Γ_{Qual}^i denotes the qualified set of I_i.

B. **Image segmentation**

Using region-based segmentation[16] 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 for all the areas I_i, $P(I_i) = TURE$. Note that, for I_i, I_j, $I_i \cup I_j = \varnothing$. 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 ϕ_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_i is corresponded with an participant P_i, so there are $n+1$ input units in this layer; in hidden layer, after remarking all identification sets A_{ij} to A_j, each hidden unit A_j is corresponded with an identification set A_j. This layer has l 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 w0j which is between input unit P0 and the j-th hidden unit Aj , is the threshold of Aj. Weight links between all the input units except P0 and hidden units represent the participant is affiliated with one identification set. wij represents the weight from i-th input unit to j-th hidden unit.

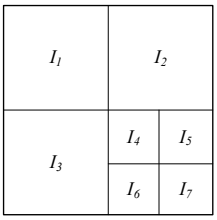

Figure 1. the result of region-based segmentation

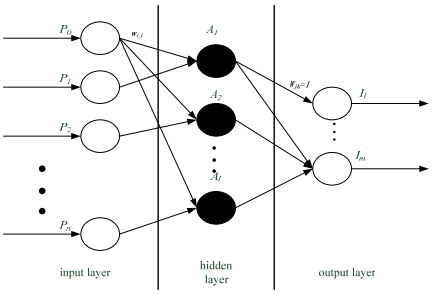

Figure 2. the suitable PSN architecture

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 *1*.

Considering sub-image Ii is much smaller than secret image and the compression of PSN. Each share can be much small than that of traditional schemes. For example, if a secret image is 256*256, and splites 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:

$$e^2 = \frac{1}{m} \sum_{j=1}^{m} (t_j^p - I_j^p)^2 . \quad (3)$$

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

$$I_j^p = f(\prod_{i=1}^{p} A_i^p) . \quad (4)$$

2) Activation function: The PSN uses sigmoid activation function

$$f(x) = \frac{1}{1+e^{-x}} , \quad (5)$$

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 $p = (1, p_1, p_2, \ldots p_n)$ randomly, and initialize the value of weight $w_{ij}^0 = 1$.

Step3: if ($n<N$)

Step4: for: compute the output data I_i for each output unit, and compute MSE e^2.

Step5: modify one set of $w_j = (w_{0j}, w_{1j}, \ldots w_{nj})^T$ 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 $S_i = (p_i, w_{ij})$

E. Dealer Signature Generation

All the parameter hypothesis is just like III

Dealer computes the signed function for each shares Si as follows:

Choose $r \in \{0,1\}^{k_0}$ randomly, and compute w=H(Si||r);

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

Compute y=0||w||r*||G2(w)

Compute Ui=sig(Si)=yd mod n

publicize dealer's public key keypub=(N,e)

F. Dealer verification and Share distribution

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

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

Compute $y = U_i^e \bmod N$;

Parse y=b||w||r*||γ, where |b|=1, |w|=k1, |r*|=k0, |γ|=k-k0-k1-1.

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

If ($H(S_i \| r) = w \wedge G_2(w) = \gamma \wedge b = 0$)

Return (TURE);

Else reture(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 θ, 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 key_{pub} 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

[1] Naor M and Shamir A, "Visual cryptography," Proceedings of Advances in Cryptology-Eurocrypt'94, Berlin, Spinger, pp. 179-196,1995.

[2] Ateniese G, Blundo C, De Santis A and Stinson D.R., "Visual cryptography for general access structures," Information and Computation, vol. 129(2), pp. 86-106,1996.

[3] Verheul E R and Van Tilborg H C A, "Constructions and properties of k out of n visual secret sharing schemes," Designs,Codes and Cryptography, vol. 11, pp. 179-196,1997.

[4] Feng YI, WANG D S, LUO P, et al, "Multi secret image color visual cryptography schemes for general access structures," Progress in Natural Science, vol. 16(4), pp. 431-436,2006.

[5] Chor, B.Goldwasser, S.Micali, et al, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults". Proc.26th IEEE Symposium. On Foundations of Computer Science, pp.372-382, 1985.

[6] P.Feldman, "a Practical Scheme for Non-interactive Verifiable Secret Sharing". Proc.28th IEEE Symposium on Foundation of Computer Science, IEEE Computer Society, pp.427-437, 1987.

[7] T.P.Pedersen, "Distributed Provers and Verifiable Secret Sharing Based on Discrete Logarithm Problem". PhD Thesis, Aarhus University, Computer Science Department, Aarhus, Denmark, 1992.

[8] T.P.Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing". Advances in Cryptology-CRYPTO'91, Lecture Notes in Computer Science, vol. 576, pp.129-140,1992.

[9] Theodore M. Wong, Chenxi Wang, Jeannette M. Wing, "Verifiable secret Redistribution for Threshold Sharing Schemes". Carnegie Mellon University Technical Report CMU-CS-02-114, February 2002.
[10] C.L.Hsu, T.C.Wu. "Authenticated Encryption Scheme with (t,n) Shared Verification". IEE.Proc.Computer.digit.tech, vol.145(2), pp.117-120, 1998.
[11] Talal Mousa Alkharobi, "Secret sharing using artificial neural networks," Texas A&M University. pp. 51-60,2004.
[12] Ghosh J and Shin Y, "Efficient higher-order neural networks for classification and function approximation" Int J Neural Syst, vol. 4(3), pp. 323-350,1992.
[13] Duch W and Jankowski N, "Survey of neural of neural transfer function," Neural Comput Surv, vol. 2(1), pp. 163-212, 1992.
[14] Schmitt M, "On the complexity of computing and learning with multiplicative neurous," Neural Comput, vol. 14(2), pp. 241-301, 2002.
[15] M.Bellare, P.Rogaway, "the Exact Security of Digital Signatures—How to Sign with RSA and Rabin". In U. Maurer, editor, Advances in Cryptology—Proceedings of EUROCRYPT'96,Lecture Notes in Computer Science 1070, pp.199-416,1996.
[16] Gonzalez R.C. and Woods R.E. Digital Image Processing(Second Edition). BeiJing: Publishing House of Electronics Industry, 2007.
[17] Song Ge, Peng Changgen. Visual Cryptography Scheme Using Pi-sigma Neural Networks. 2008 International Symposium on Computer Science and Computational Technology proceedings (ISCSCT2008)，pp.679-682.