ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

A Novel Approach of Visual Secret Sharing Schemes for Encrypting Multiple Images using ANFIS

Ms.C.Sujatha M.E[#1], S.Archana[#2], K.Tharani[#3], C.Yuvaniya[#4]

Assistant Professor, Department of CSE, ULTRA College of Engineering & Technology, Madurai, Tamilnadu, India[#1]

UG Scholar, Department of CSE, ULTRA College of Engineering & Technology, Madurai, Tamilnadu, India[#2, #3, #4]

ABSTRACT: Secret sharing is a method of generating multiple shares from secret information so that only a qualified set of shares can be employed to recover this secret information. Visual secret sharing (VSS) is an example of secret sharing; its decryption can be performed by using human eyes without a computer. This paper provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones, and also a general method of constructing VSS schemes encrypting multiple secret images using ANFIS approach. In proposed method ,we get performance metrics improved than existing approach and improved quality of image and security thread .

I. INTRODUCTION

A secret sharing (SS) scheme is a method of generating multiple shares from a secret so that any qualified set of shares can be employed to recover the secret, but no forbidden set of shares reveals any information about the secret. Therefore, an SS scheme can be used to control participants' access to secret information and to diversify risks of leaking of secret information. A (k, n)-threshold SS scheme is a typical example of the SS schemes; this is a method of sharing a secret among

n participants in such a way that any k or more participants can recover the secret with their shares, but no $k - 1$ or less participants can obtain any information about the secret from their shares. There exist SS schemes whose decryption requires no numerical computations but can be performed by a human. A visual secret sharing (VSS) scheme is an example of such SS schemes. In VSS schemes, secrets and shares are both visual data such as printed texts, hand written notes, pictures, and so on. The VSS schemes encrypt a visual secret into visual shares so that humans can recover the visual secret with their eyes by superposing a qualified set of visual shares printed on transparencies.

The secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret. Here, the sets of the qualified combinations and the forbidden combinations are called a qualified set and a forbidden set, respectively, and the pair of the qualified and forbidden sets is called an access structure. A typical example of SS schemes is the (k, n) -threshold SS scheme ,in which a secret is encrypted into n shares so that any k or more shares can reconstruct the secret, while anyk−1or less shares leak no information about the secret.In contrast to the ordinary cryptosystems, there exist SS schemes whose decryption can be performed by humans without any numerical computations. The visual secret sharing (VSS) scheme is an example of such SS schemes. This scheme encrypts a visual secret into visual shares so that humans can visually reconstruct the secret with their eyes by superposing a qualified combination of visual shares each printed on a transparency. One of the applications in which VSS schemes are essential is for the authentication by a human recipient without any trusted communication channels.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

More precisely, the problem here is to authenticate a message from an informant to a human recipient through an insecure channel which is under full control of an adversary. This arises, for example, in the interactions between a human and an electronic device without screen such as a smartcard. It is hard to provide a solution to this problem without assuming a secure channel,1and the authentication based on VSS schemes, called the visual authentication, has been the only secure solution so far.

II. RELATED WORKS

The SS scheme encrypting multiple secrets can trivially be realized by a collection of multiple SS schemes each encrypting each secret. Therefore, this work considers the VSS scheme encrypting multiple secrets in which each participant receives a single visual share and any qualified combination
of participants for each visual secret can reconstruct the secret by superposing their visual shares. So far there have been proposed the following VSS schemes encrypting multiple secrets: extended visual cryptographic schemes (EVCS), visual secret sharing schemes for plural secret images (VSS-*q*-PI) and threshold multiple-secret visual cryptographic schemes (MVCS) . Here, EVCS assumes an access structure $(A)_0 = \{a \in A | \forall a' \in A(a' \not\subset a)\}$ such that all but one of its qualified sets consist of (the combination of) a single share, VSS-*q*-PI an access structure whose forbidden sets are identical for all secrets3 (although its qualified sets can be arbitrary) and MVCS a threshold access structure. This work provides the formulation and constructions of VSS schemes realizing a general access structure for multiple secrets without any
restrictions .It should be stated that there has been proposed another type of VSS schemes encrypting multiple images in which additional operations in the decryption, such as the rotation of shares with multiple relative angles, are introduced. In VSS schemes of this type, different operations correspond to different secret images, while in the VSS schemes, different combinations of shares correspond to different secret images. Therefore, from a point of view of the access control, which is the goal of the secret sharing, the former schemes can be reduced to a single VSS scheme encrypting a single secret (into which multiple secret images are connected), while there exist no such simple reductions for the latter ones even for the simplest access structures. Using ANFIS in VSS scheme which reduces error and time complexity to increase the image quality than the former construction .

III. EXISTING APPROACH

A. Basic Definitions and Notations

For n ∈N, let[n] denote the set of natural numbers less than or equal to n ;i.e. [n]={k ∈N|k ≤n}. The power set of a set S is denoted by 2S;i.e.2S={a|a⊆S}.For a subset A of a power set partially ordered by inclusion ,let A0denote the set of the minimal elements of A with respect to this order;(where we have used the symbol ⊂to represent the strict inclusion). For an ordered set S={s1,s2,⋯,sn}, the order of si in S is denoted by ord S (si) ;i.e. ordS(si)=i. For random variables X and Y over the same domain ,we write X =Y if X and Y are equal almost surely(i.e. Pr[X =Y]=1), and X ~Y if X and Y have the same probability distribution. For a set S ,let S U denote a probabilistic function which outputs an element of S according to the uniform distribution over S.
For x∈{0,1}n, b∈{0,1}and i ∈[n],let x xi=b denote the string x with the i-th element xi replaced by b; i.e.

$$x_{x_i=b} = (x_1, \cdots, x_{i-1}, b, x_{i+1}, \cdots, x_n).$$

For x∈{0,1}n, let Gray(x)denote the gray level of x ;i.e.

$$\mathrm{Gray}(x) = \frac{|\{i\,|x_i = 1\}|}{n}.$$

The gray level of the empty string ε is defined to be 0; i.e. Gray(ε)=0.

B. Access Structure and Secret Sharing

Let S={s1,s2,⋯,sn} be the set of all the shares. The subset of 2Sany of whose elements can decrypt the secret is called a qualified set and is denoted by A Q. The subset of 2Sany of whose elements leaks no information about the secret is called a forbidden set and is denoted by AF. The pair of the qualified and forbidden sets, =(AQ,AF), is called an access structure on S. The access structure has to satisfy the monotonicity:

$$A \in A_Q \wedge A \subseteq B \Rightarrow B \in A_Q,$$
$$B \in A_F \wedge A \subseteq B \Rightarrow A \in A_F,$$

for all A,B⊆S. A qualified set A Q is uniquely determined by its minimal elements

---

AQ0

$$(A_Q)_0 = (A'_Q)_0 \Rightarrow A_Q = A'_Q$$ for all qualified sets A Q and A Q on S. An access structure is called perfect if every subsets of the shares are included in either the qualified set or the forbidden set. The perfect access structure can be determined by only a qualified set

C. Visual Secret Sharing

In the ordinary SS schemes, the secrets and shares are both numerical data, and their decryption is performed by computers. In contrast, in the VSS schemes, the secrets and shares are both visual, and their decryption can visually be performed by human eyes.8Each black-white pixel in a secret image is encrypted into a set of black-white sub pixels in shares. Hence, the encryption of each pixel can be represented as a pair of matrices Cb=(cbij) with b∈{0,1},where b=0for a white pixel in a secret image and b=1otherwise,andcbij =0 for a white j-th sub pixel in the i-th share and cbij =1otherwiseFor an illustrative purpose, let us consider a(2,2)-threshold VSS scheme. A secret image is encrypted into two shares .Each share is indistinguishable from noise images, and so leaks no information about the secret. On the other hand,the secret image can be reconstructed when both of the shares are superposed. Tis can be constructed as follows. A pixel in the secret image is encrypted into two sub pixels in each of the two shares. If is white (resp. black), then Pattern 1or Pattern 2 in the upper (resp. lower) row of Table II is chosen at random. The superposition of the two shares has one black sub pixel and one white sub pixel (resp. two black sub pixels) if e is white (resp. black). This construction can be represented by the setsC0andC1of matrices in Table II ;more precisely, the above encryption and decryption can be represented by the functions Enc :{0,1}→{0,1}2×2andDec:{0,1}2×2→{0,1}2given by

$$\mathrm{Enc}(b) = \mathcal{C}_U^b \quad \text{and} \quad \mathrm{Dec}(M) = (m_{11} \vee m_{21}, m_{12} \vee m_{22})$$

For b∈{0,1}and M=(mij)∈{0,1}2×2, respectively, where ∨ denotes the OR operation. The relative difference in gray level between superposed shares that come from a white pixel and a black pixel in the secret image is called the contrast. In the above example, there constructed pixel has a gray level of22 =1ifeis black, andagraylevelof12ifeis white; therefore, Contrast=22−12 =12.The higher contrast makes it easier to recognize reconstructed images .

The number of sub pixels in shares encrypted from a pixel in a secret is called the pixel expansion. In the above example ,a pixel in a secret is encrypted into two sub pixels in shares ;therefore, Pixel expansion =2. The lower pixel expansion allows the more practical resolution of share images. A VSS scheme and its encryption are called optimal if they have the lowest pixel expansion.

D. Notations for Matrices

For two matrices A and B of the same number of rows, let A |B denote the concatenation of A and B. In the same way, we introduce an equivalence relation on the set M of matrices; for two matrices A and B of the same size, we write A~B if A can be obtained by a column permutation of B .For R∈M ,let R denote the set of all the matrices A such that A~R ;i.e.

$$\langle R \rangle = \{A \in \mathcal{M} \mid A \sim R\}.$$

VISUAL SECRET SHARING SCHEMES ENCRYPTING MULTIPLE IMAGES

Formulation and construction

We first extend the definition of an access structure to the case for multiple secrets
Definition 1 (Access structure for multiple secrets).
Let P be a finite set, and q ∈ N. For i ∈ [q], let Ai Q and Ai F be subsets of 2 P such that Ai Q ∩Ai F = ∅. The pairs Γ q of the subsets Ai Q and Ai F , Γ q = { (Ai Q, Ai F) }q i=1, is called an access structure on P for q secrets if Ai Q and Ai F satisfy the monotonicity

$$A \in A_Q^i \wedge A \subseteq B \Rightarrow B \in A_Q^i,$$
$$B \in A_F^i \wedge A \subseteq B \Rightarrow A \in A_F^i,$$

for any A, B ⊆ P and i ∈ [q], and the uniqueness:

$$(A_Q^i)_- \cap (A_Q^j)_- = \emptyset$$

for any i, j ∈ [q] such that i 6= j. For an access structure Γ q = { (Ai Q, Ai F) }q i=1, Ai Q and Ai F are called the qualified set and the forbidden set for the i-th secret, respectively. An access structure Γ q = { (Ai Q, Ai F) }q i=1 is called minimally refined if |(Ai Q)−| = 1 for any i ∈ [q]. If we pose the restriction

$$(A_Q^i)_- = \{\{P_i\}\} \text{ with } q = |\mathcal{P}| + 1 \quad (\text{resp. } A_F^i = A_F)$$

for all i, then the above definition coincides with that introduced. Therefore, the above definition can be considered as a generalization of the existing ones. We next give a definition of VSS schemes encrypting multiple secret images

Construction 1.

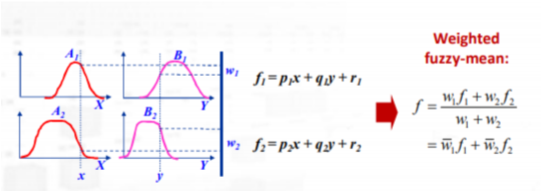
Let P be a finite set, and q ∈ N. Let Γ q = { (Ai Q, Ai F) }q i=1 be a minimally refined access structure on P for q secrets. For i ∈ [q], let a i q be the element of (Ai Q)−: (Ai Q)− = {a i q} with a i q ⊆ P. For b ∈ {0, 1} and i ∈ [q], let C b i = [C b (ni,ni)] a i q with ni = |a i q |. Define Enc by

$$\mathrm{Enc}(b) := \langle C_1^{b_1} | C_2^{b_2} | \cdots | C_q^{b_q} \rangle_U$$

IV. PROPOSED METHODOLOGY

Adaptive Neuro-Fuzzy Inference Systems (ANFIS)

Takagi-Sugeno fuzzy system mapped onto a neural network structure.
Different representations are possible, but one with 5 layers is the most common.
Network nodes in different layers have different structures.
Consider a first-order Sugeno fuzzy model, with two inputs, x and y, and one output, z.
Rule set Rule 1: If x is A1 and y is B1 , then f1 = p1x + q1y + r1
Rule 2: If x is A2 and y is B2 , then f2 = p2x + q2y + r2


A_1
B_1
A_2
B_2
X
Y
X
Y
x
y
w_1
w_2
$f_1 = p_1x + q_1y + r_1$
$f_2 = p_2x + q_2y + r_2$
Weighted fuzzy-mean:
$f = \frac{w_1 f_1 + w_2 f_2}{w_1 + w_2} = \bar{w}_1 f_1 + \bar{w}_2 f_2$

Corresponding equivalent ANFIS architecture:

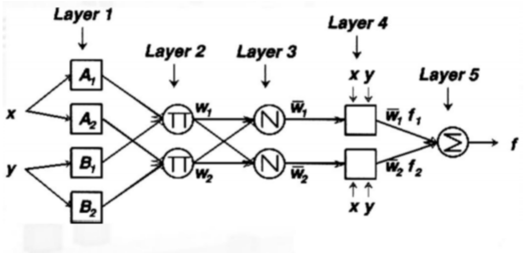
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019



Layer 1: every node is an adaptive node with node function:

$$O_{1,i} = \mu_i(x_i)$$

Parameters in this layer are called premise parameters.
Layer 2: every node is fixed whose output (representing firing strength) is the product of the inputs:

$$O_{2,i} = w_i = \prod_j \mu_j$$

Layer 3: every node is fixed (normalization):

$$O_{3,i} = \overline{w}_i = \frac{w_i}{\sum_j w_j}$$

Layer 4: every node is adaptive (consequent parameters) :

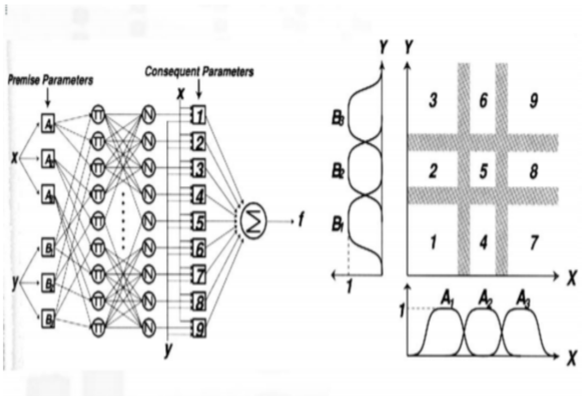
$$O_{4,i} = O_{3,i} f_i = \overline{w}_i (p_0 + p_1 x_1 + \ldots + p_n x_n)$$

Layer 5: single node, sums up inputs:

$$O_{5,i} = \sum_i \overline{w}_i f_i = \frac{\sum_i w_i f_i}{\sum_i w_i}$$

Adaptive network is functionally equivalent to a Sugeno fuzzy model!

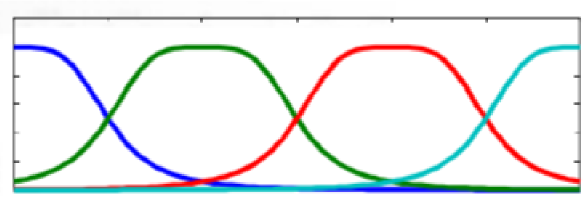
ANFIS with multiple rules



Model building guidelines

Select number of fuzzy sets per variable: empirically by examining data or trial and error using clustering techniques
using regression trees (CART)

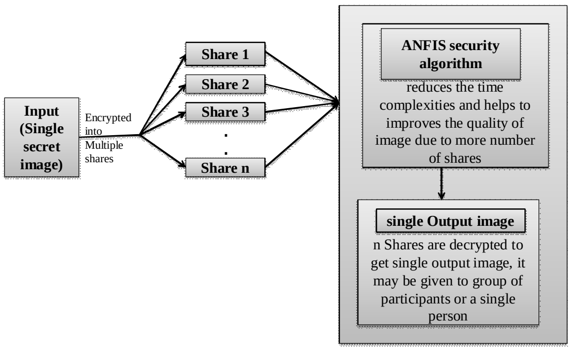
Initially, distribute bell-shaped membership functions evenly:



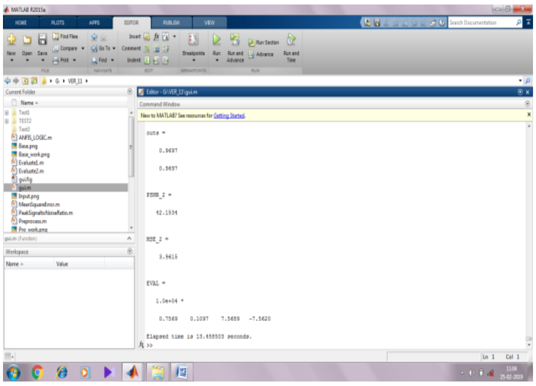
Using an adaptive step size can speed up training

PROPOSED ARCHITECTURE

BLOCK DIAGRAM


Input (Single secret image)
Encrypted into Multiple shares
Share 1
Share 2
Share 3
.
.
Share n
ANFIS security algorithm
reduces the time complexities and helps to improves the quality of image due to more number of shares
single Output image
n Shares are decrypted to get single output image, it may be given to group of participants or a single person

V. RESULT



New to MATLAB? See resources for Getting Started.

```
outs =

    0.9697

    0.9697


PSNR_2 =

   42.1534


MSE_2 =

    3.9615


EVAL =

   1.0e+04 *

    0.7569    0.1097    7.5689   -7.5620

Elapsed time is 13.458503 seconds.
>>
```

It provides better quality image and it reduces the error and time consumption than the existing one .

VI. CONCLUSION

In this paper, we generalized the formulation of VSS encryption based on ANFIS for multiple secret images so that those of the existing schemes, VSS, may be included as a special case. We then provided a general method of constructing VSS schemes encrypting multiple secret images. We also provided an example of VSS schemes which cannot be formulated as the existing ones. Anfis algorithm used for decrypting and improved security level and quality of image.

REFERENCES

[1] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theor.Comput.Sci., vol. 250,nos. 1–2, pp. 143–161, 2001.
[2] A. Beimel, “Secret-sharing schemes: A survey,” in Proc. 3rd Int.Workshop Coding Cryptol. (IWCC), vol. 6639. 2011, pp. 11–46.
[3] A. Beimel and I. Orlov, “Secret sharing and non-Shannon informationinequalities,” IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 5634–5649,Sep. 2011.
[4] G. R. Blakley, “Safeguarding cryptographic keys,” inProc. Nat. Comput.Conf., Monval, NJ, USA, 1979, pp. 313–317.
[5] C. Blundo, P. D’Arco, A. D. Santis, and D. R. Stinson, “Contrast optimalthreshold visual cryptography schemes,”SIAM J. Discrete Math., vol. 16,no. 2, pp. 224–261, 2003.
[6] M. Bose and R. Mukerjee, “Optimal(k,n)visual cryptographic schemesfor general k,” Des., Codes Cryptogr., vol. 55, no. 1, pp. 19–35, 2010.
[7] Y.-C. Chen, “Fully incrementing visual cryptography from a succinct non-monotonic structure,”IEEE Trans. Inf. Forensics Security, vol. 12,no. 5, pp. 1082–1091, May 2017.
[8] S. Cimato, R. de Prisco, and A. de Santis, “Optimal colored thresholdvisual cryptography schemes,”Des., Codes Cryptogr., vol. 35, no. 3,pp. 311–335, 2005.
[9] T. M. Cover and J. A. Thomas,Elements of Information Theory, 2nd ed.Hoboken, NJ, USA: Wiley, 2006.
[10] L. Csirmaz, “The size of a share must be large,” J. Cryptol., vol. 10,no. 4, pp. 223–231, 1997.
[11] Y. Desmedt, S. Hou, and J.-J.Quisquater, “Audio and optical cryptography,” in Advances in Cryptology—ASIACRYPT(Lecture Notes inComputer Science), vol. 1514. Berlin, Germany: Springer-Verlag, 1998,pp. 392–404.
[12] O. Farràs, T. Hansen, T. Kaced, and C. Padró, “Optimal non-perfectuniform secret sharing schemes,” inAdvances in Cryptology—CRYPTO(Lecture Notes in Computer Science), vol. 8617. Berlin, Germany:Springer-Verlag, 2014, pp. 217–234.
[13] M. Iwamoto and H. Yamamoto, “A construction method of visualsecret sharing schemes for plural secret images,”IEICE Trans. Fundam.,vol. 86, no. 10, pp. 2577–2588, 2003.
[14] M. Naor and B. Pinkas, “Visual authentication and identification,” inAdvances in Cryptology—CRYPTO(Lecture Notes in Computer Science), vol. 1294. Berlin, Germany: Springer-Verlag, 1997, pp. 322–336.
[15] M. Naor and A. Shamir, “Visual cryptography,” in Advances inCryptology—EUROCRYPT (Lecture Notes in Computer Science),vol. 950. Berlin, Germany: Springer-Verlag, 1994, pp. 1–12.
[16] M. Sasaki and Y. Watanabe, *“Formulation of visual secret sharingschemes encrypting multiple images,” in Proc. 39th IEEE Int. Conf.Acoust., Speech Signal Process. (ICASSP), Jun. 2014, pp. 7391–7395.
[17] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11,pp. 612–613, Nov. 1979.
[18] S. J. Shyu, “Threshold visual cryptographic scheme with meaningfulshares,” IEEE Signal Process. Lett., vol. 21, no. 12, pp. 1521–1525,Dec. 2014.
[19] S. J. Shyu and K. Chen, “Visual multiple-secret sharing by circle randomgrids,”SIAM J. Imag. Sci., vol. 3, no. 4, pp. 926–953, 2010.
[20] S. J. Shyu, S.-Y.Huang, Y.-K.Lee,R.-Z. Wang, and K. Chen, “Sharingmultiple secrets in visual cryptography,”PatternRecognit., vol. 40,no. 12, pp. 3633–3651, 2007.
[21] S. J. Shyu and H.-W.Jiang, “General constructions for thresholdmultiple-secret visual cryptographic schemes,”IEEE Trans. Inf. Forensics Security, vol. 8, no. 5, pp. 733–743, May 2013.
[22] D. R. Stinson, Cryptography: Theory and Practice, 3rd ed. London,U.K.: Chapman & Hall, 2005.
[23] E. R. Verheul and H. C. van Tilborg, “Constructions and properties ofkout ofnvisual secret sharing schemes,”Des., Codes Cryptogr., vol. 11,no. 2, pp. 179–196, 1997.
[24] R. Z. Wang, “Region incrementing visual cryptography,” IEEE SignalProcess. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009.
[25] S. Washio and Y. Watanabe, “Security of audio secret sharing schemeencrypting audio secrets with bounded shares,” in Proc. 39th IEEEInt. Conf. Acoust., Speech Signal Process. (ICASSP), May 2014,pp. 7396–7400.

DOI: 10.15680/IJIRCCE.2019. 0702127