Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 185 – 191

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Cascade Forward Back-propagation Neural Network Based Group Authentication Using (n, n) Secret Sharing Scheme

Supriya Narad[a], Pallavi Chavan[b]

[a]*Supriya Narad, BDCE Sewagram, Wardha-442001 , India*

[b]*Pallavi Chavan, BDCE Sewagram, Wardha- 442001, India*

Abstract

Authentication is the important issue over the internet. It results in need of robust security services and schemes. This paper proposes the Shamir Secret Sharing Scheme along with Cascade forward back propagation neural network. The proposed (n, n) Shamir secret sharing scheme is implemented successfully for share encryption and decryption process. It reveals the secret only and only when all the n number of participants are available at the reconstruction process. The generated shares have a best quality so that human brain can't predict the original secret by any combination. The neural network is already trained for RGB image database and images are stored in particular group having a group category number which is to be predicted as output of neural network. For testing purpose, we take an image, store it in a group, create its shares and now identifies to which group it belongs. The neural network here provides the correct group of that image which we have trained earlier.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Group Authentication; Cascade Forward Backpropogation Neural Network; (n,n) Shamir Secret Sharing Scheme.

1. Introduction

Cryptography is widely spread and used almost at every security place, as the need for secured data is increasing. So, data must be made secured using encryption and decryption process. Various techniques are available today such as traditional RSA algorithm, DES algorithm, Visual Cryptography, etc. These techniques may be implemented

* Corresponding author. Tel.: +91-8908757907
E-mail address:ganeshpatra099@gmail.com

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.032

with gray images or binary images and shares can be generated for them using various secret sharing schemes. Variations in format of input image, size of image and image quality can be considered for input. The available Secret sharing schemes are (k, n) or (k, n-1), etc. We have threshold cryptography methods available in the field of cryptography, it also proves and gives best results. Most threshold systems are based on encryption with keys which are distributed in parts. Different combinations of threshold cryptography include (2, 2) threshold VCS where a secret image is encrypted into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure. (2, n) threshold VCS encrypts the secret image into n shares such that when any two or more of the shares are overlaid, the secret image is revealed. (n, n) threshold VCS encrypts the secret image into n shares such that only when all n of the shares are combined then only the secret image will be revealed.

The proposed Shamir Secret Sharing Scheme is (n, n) Group Authentication Scheme where, first n is the number of users participated in group authentication and second n is the number of shares generated for each user. The scheme works as dividing the secret into number of shares followed by reconstructing the secret. While reconstructing, an authorized subset of users collect the pieces and use them to reconstruct the original secret. It is required that after a reconstruction only the users participated in reconstruction will know the secret, and new users will not perform the communication. For simplicity, here a group of users participate in authentication process. The proposed scheme helps to remove some drawbacks of the existing scheme and provides more security to the communication system. The group authentication can be used to determine Many-to-many type of authentication, to generate common secret key and to achieve authentication mechanism by using Neural Network.

2. Related work

Lein Harn[1] have worked on Group Authentication Specially designed for Group oriented applications. It authenticates all users at once and provides many-to-many authentication. Here, a group manager is responsible to register all group members and issue a private token each time. The paper proposes synchronous and asynchronous Group Authentication Schemes. Here, author proposes (t, m, n) scheme, where t is the threshold, m is the number of users and n is the number of members. This threshold is taken for a single group, we may define number of such groups. It is based on Shamir's (t, n) secret sharing scheme. Asynchronous (t, m, n) is a secret sharing scheme with one-time authentication and the other scheme defined is a GAS with multiple authentications. The group authentication protocol allows users to reuse their tokens and the chances of providing security become less.

Sian-Jheng Lin, Wei-Ho Chung[2] have worked on (t, n) Visual cryptography Scheme with Dynamic Group. It works like a probabilistic model. This paper allows dynamic change of users in a user group, i.e. dynamically add users or delete them. A (t, n) visual cryptography scheme with unlimited n is proposed to reduce the overhead of generating and distributing transparencies. Then a (t, ∞) Visual cryptography scheme achieve maximum contrast with. The scheme is based on basis matrices and the basis matrices cannot be constructed with infinite size.

IlkerNadi Bozkurt, KamerKaya[3] have worked on Threshold Cryptography based on Blakley's Secret Sharing. Threshold Cryptography is conducted with Blakley's SSS and present a function sharing scheme for RSA cryptosystem. Blakley's Secret Sharing Scheme works in Dealing Phase and Share Combining Phase. The required values for the computation are distributed to the parties using a secret sharing scheme. The scheme is based on hyper plane geometry and the intersection point of the hyperplane is the secret.

Tai- Wen Yue, Suchen Chiang[8] have worked on neural network approach in visual cryptography. This paper provides a novel approach for visual cryptography using Neural Network. To perform encrypting i/p is a set of gray level images and o/p is a set of binary images. Image half toning is used to convert gray image into binary image. The Neural Network model proposed is a Quantum Neural Network for (2, 2) scheme. It minimizes the energy function of a Quantum Neural Network and can solve the problem without any noise injection mechanism.

Smita Jhajharia[9] have worked on Public key cryptography using Neural Network and Genetic Algorithm. It proposes key generation for public key cryptosystem by the application of ANN with Genetic Algorithm. GA is applied for optimization in search problems. In Public Key cryptography, pseudo random number generator is used to generate unique key and random number used in artificial neural network. Neural network used in implementation is a feed forward neural network.

T. Goghawari, R. Soundarajan[10] have worked on Cryptography Using Neural Network. A neural network is used to generate common secret key. Both communicating networks receive an identical i/p vector; generate an o/p bit for training. The secret key generation over a public channel is studied and found some results. The generated key is used for encrypting and decrypting of the given message by using DES algorithm. Here, Hebbian rule is applied for key generation.

Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien[11] have worked on Survey Report on Cryptography Based on Neural Network. It proposes that Cryptography is the ability of changing information into obvious unintelligibility in a way allowing a secret method of un-mangling. For overcoming the drawbacks, artificial neural networks (ANNs) are applied to solve many problems. This paper gives a state-of-the-art review on the use ofartificial neural networks in cryptography and studies the performance on approximation problems related to cryptography.

3. Proposed work

The proposed methodology is based on Cascade forward back propagation neural network. Image shares are generated and stored with the system and encrypted using Shamir secrete sharing scheme. Now, reconstruction is performed with neural network. It will combine user share and system share to reconstruct original image, called as decrypted image. Finally authentication is performed to test whether decrypted image and original image in database is same or not.

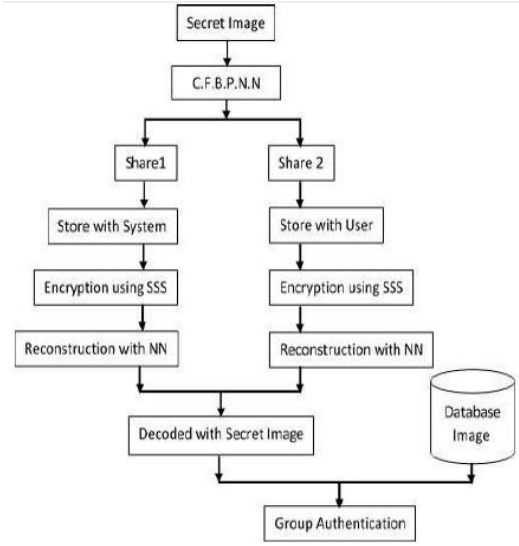


Fig. 1. Methodology of the proposed scheme

Shamir Secret Sharing Scheme is based on a linear polynomial. In (n, n) secret sharing scheme, first n is the number of users participated in group authentication and second n is the number of shares generated for each user. The (n, n) Group Authentication Scheme is very efficient since it authenticates all users at once if they are the group members. For nonmembers in a group, preprocess is used before applying user authentication to identify non-members. Also, if any of the users present in group authentication is absent then the group is not authenticated at all, as each share is distributed to each user. The proposed scheme works as follows.

3.1 Development of Shamir Secret Sharing Scheme

Shamir Secret Sharing Scheme consists of two phases, Share Generation and Secret Reconstruction.

3.1.1 Share Generation

Share Generation process takes a secret as an input and generates n number of shares U= {U_1, U_2, U_3……, U_n} and a dealer D. Now the share is distributed to n number of users that is each user should have one share.
Dealer D
picks a random polynomial f(x) of degree (t-1):

$$f(x) = a_0 + a_1x + \ldots\ldots + a_{t-1}\, x_{t-1} \bmod p \quad (1)$$

such that the secret is,

$$s = f(0) = a_0 \quad (2)$$

and all coefficients, a_i, i = 0, 1, …….. , t-1. D computes n shares, $y_i = f(x_i)$, where i = 1,2,……., n, where x_i is the public information associated with shareholder U_i. Then dealer distributes each share yi to corresponding shareholder U_i secretly. The process works for encryption. Algorithm is as follows:

1. Enter n = no. of parts to distribute as shares, k = no. of parts for reconstruction.
2. n, k has to be a positive integer and n = k.
3. Initialize random coefficient.
4. Perform inversion of shares using initially created random coefficient.
5. Generate pieces of partial information. Enter part number to use.
6. Shares created.
7. STOP.

3.1.2 Secret Reconstruction

Secret reconstruction process reconstructs the correct input secret. Let us assume that t shareholders recover the secret s then, shareholders release their shares and use the Lagrange interpolation formula and recover the secret. While reconstruction, all the shares should take part in reconstruction process. The process works for decryption. Algorithm is as follows:

1. Check if insufficient pieces of information parts available for reconstruction.
2. Obtain pieces of information for reconstruction (n = k)
3. Generate Lagrange Polynomial.
4. Reconstruct secret information.

3.2 Optimizing Shamir Secret Sharing Scheme with Neural Network

Artificial neural networks are massively parallel, adaptive networks of simple nonlinear computing elements called neurons which are intended to abstract and model some of the functionality of the human nervous system capture some of its computational strengths. A novel phenomenon of dynamic neural network is applied in cryptography systems. The limitation in the general cryptographic process led to the development of cryptographic systems with shorter keys called the secret key systems. The security of such cryptographic system depends on the secrecy of the key. A Secret Sharing Scheme is represented by using Backpropagation Neural Network. A Neural Network is also used to generate common secret key. So the special characteristic of neural networks can be used in generating secret key over public channel.

3.3 Development of Group Authentication Scheme

Assume that there are m users, P_i, i= 1; 2; . . . ; m, participated in a group-oriented application. These users want to make sure whether they all belongs to the same group, for $U_i \varepsilon U$, i= 1; 2; . . . ; n, at the beginning of the application. Development of Group Authentication Scheme is described as follows:

i. Initialization: The system parameters are generated by the Group Manager in initialization phase.

ii. Distribution: The Group Manager generates and distributes token for each group member U_i, i= 1; 2; . . . ; n.

iii. Authentication: Each user computes and releases a value, c_i, using his token. After receiving all c_i, i =1 ; 2 ; . . . ; n, users verify whether these values are released by members of the group. If the verification fails, additional authentication is needed to identify non-members.

4. Experimental results

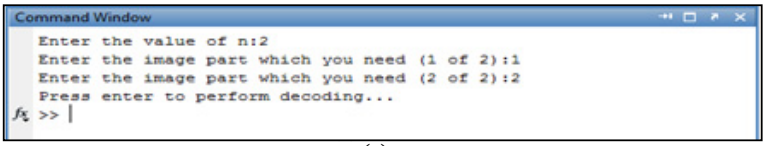
The input to the scheme may be an image, a text message, a character, a number or any special symbol. The existing scheme is compared with the implemented scheme and following results are found.

Table 1. Implemented SSS

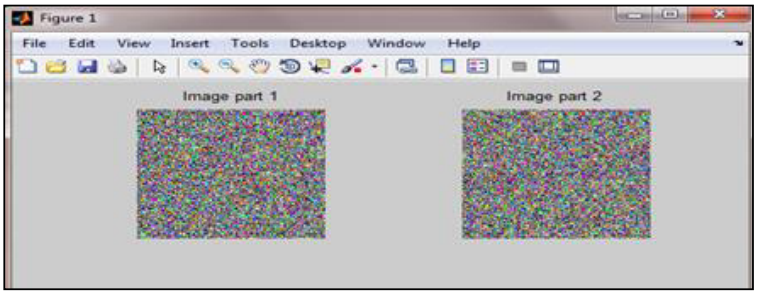
Scheme Used	No. of shares produced	Efficiency
Shamir SSS	n- shares for each character	Less
Implemented Shamir SSS	n- shares for each part	More

4.1 Shamir Secret Sharing Scheme:

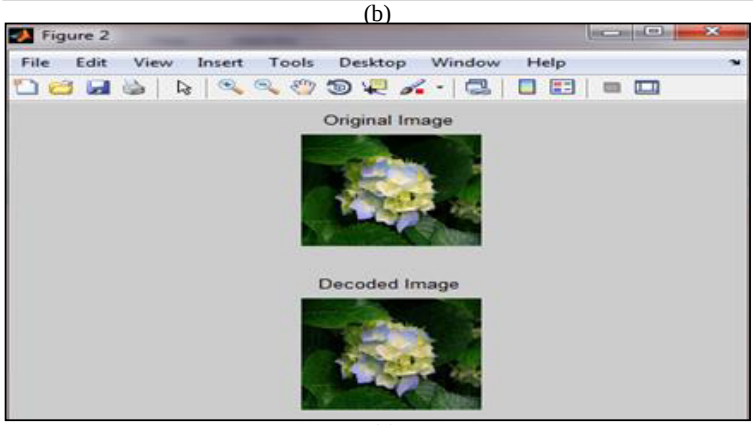
Encryption and decryption of a message by using implemented Shamir Secret Sharing Scheme is more efficient. The share generation process is optimized with the given number of parts to distribute the shares only. The same process is applied to the RGB images using (n, n) Secret Sharing Scheme and the process works as follows.



(a)



(b)



(c)

Fig. 2. (a) Share generation and reconstruction for RGB image; (b) Generated Shares; (c) Reconstruction of original Image

4.2 Training Neural Network

Cascade Forward Back-propagation neural network (CFBPNN) is implemented for training the input data. For training the neural network, images should be stored in database initially. The purpose is to find features and texture of the image and it is passed to the network as input. Cascade – forward Back-propagation network consist of layers using the DOTPROD weight function, NETSUM net input function, and the specified transfer functions. The first layer has a weight coming from the input and each subsequent layer has weight coming from the inputs with all previous layers. The last layer is the network output, called as output layer. Every layer is having biases. Each layers weights and biases are initialized using INITNW function. Adaption is done with TRAINS function and updates weights with the specified learning function. Training is done with the specified training function and corresponding performance is measured according to the specified performance function. Figure no. 4 shows the architecture of cascade forward back-propagation neural network. CFBPNN operates in Forward input signal and backward error signal

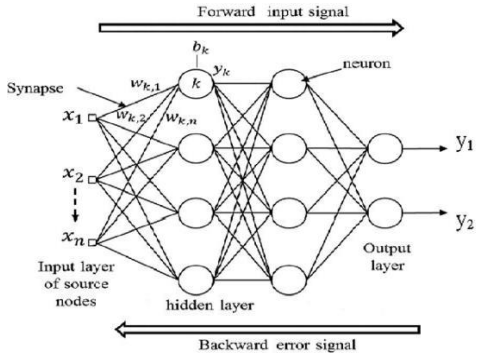
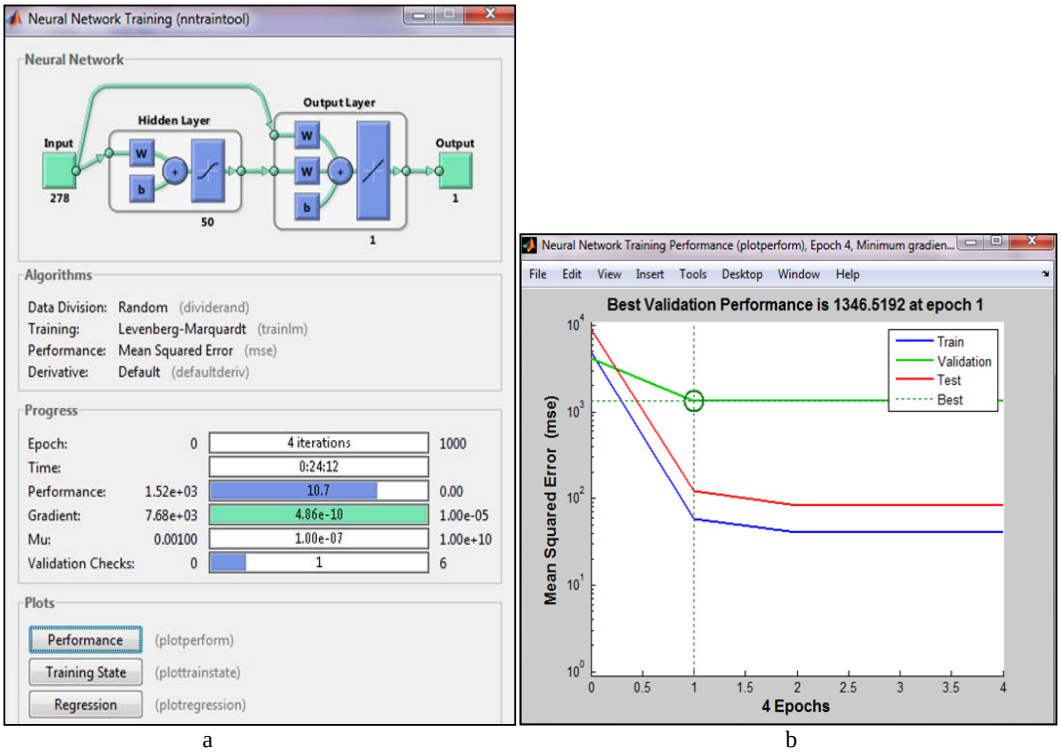


Fig. 3. Architecture of Cascade Forward Back-propagation Neural Network

For database of 200 images, the Cascade Forward Back-propagation Neural Network is trained and following observations are found for complete training. Best validation performance is found at epoch 4 when plotted against MSE. After epoch 4, there is a constant validation in neural network.

Table 2. Simulation Parameters of Neural Network

Simulation Parameter	Value
Epoch	1 to 7 Iterations
Time	00:05:50 to 01:52:42
Performance	55 to 55.6
Gradient	1.67e + 03 to 1.25e-06
Mu	1.00e-04 to 1.00e-07
Validation Checks	0 to 4



a b

Fig 3. (a) Simulation of Cascade Forward Back-propagation Neural Network; (b) Validation Graph;

Following results are found from the above work for successful user authentication. The observations are found with one group communication having four group members.

Table 3. Observations for 4 group members.

No. of parts for Encoding	No. of parts for reconstruction	User Authentication	Expected output
4	4	Yes	Yes
4	3	No	No
4	2	No	No
4	1	No	No

5. Conclusion

Providing much security to the secret data that is shared in day to day life is one of the important issues in real life. In proposed scheme of (n, n) SSS, encryption of the original image and decryption with generated shares is done with 0.0000 MSE and best performance. The authentication is implemented for group-oriented applications using (n, n) Shamir Secret Sharing Scheme. It provides many-to-many type of authentication where group activities can be securely done. The encryption and decryption of messages and images is done and the accuracy is increased in experimental results using the Cascade Forward Back-propagation Neural Network. It provides complete security for the secret images and text messages. From the experimental results it as observed that no loss occurs in decrypted image as compared to original image. So, it proves to be a complete authenticated system. Also the implemented scheme requires no complex computations for decryption.

References

1. Lein Harn.Group authentication.*IEEE Transactions on computers*, vol. 62, no. 9;September 2013.
2. Sian-Jheng Lin and Wei-Ho Chung.A probabilistic model of (t, n) visual cryptography scheme with dynamic group.*IEEE Transactions on Information Forensics and Security*, vol. 7, No. 1;February 2012.
3. Ilker Nadi Bozkurt, Kamer Kaya and Ali Aydın Selcuk.Threshold cryptography based on blakley's secret sharing.*IEEE Transactions*, vol. 22, pp: 612-613;January 2011.
4. Mitsugu Iwamoto.A weak security notion for visual secret sharing scheme.*IEEE Transactions on Information Forensics and Security*, vol. 7, No. 2;April 2012.
5. Marin Bertier.Low cost secret sharing in sensor networks.*IEEE Symposium on High Assuarance Systems Engineering*;March 2010.
6. Xiang Wang, Qingqi Pei and Hui Li.A lossless tagged visual cryptography scheme.*IEEE Signal Processing Letters*, Vol. 22, No. 7;July 2014.
7. Manghui Tu.Secure data objects replication in data grid.*IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 1;January 2010.
8. Tai- Wen Yue and Suchen Chiang.A neural network approach for visual cryptography.*IEEE*, Vol. 8;March 2012.
9. Smitha Jhajharia.Public key cryptography using neural networks and genetic algorithms.*IEEE*, Vol. 45;May 2013.
10. T. Godhawari.Cryptography using neural network.*IEEE Indicon*, Dec 2005.
11. Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien.Survey report on cryptography based on neural network.*IJETAE*, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 12, December 2013.
12. Rajendra AB and Sheshadri HS.A new approach to analyze visual secret sharing schemes for biometric authentication -a Survey.*International Journal in Foundations of Computer Science & Technology (IJFCST)*, Vol. 3, No.6;November 2013.
13. Niansheng Liu, Donghui Guo.Security analysis of public-key encryption scheme based on neural networks and its implementation.*IEEE*, Vol. No. 6;May 2006.
14. Xiali Hei and Xiaojiang Du.Two matrices for blakley's secret sharing scheme.vol. 24;April 2012.