IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Group Authentication Using Back-propagation Neural Network

Ms. Supriya K. Narad

Lecturer, CSE, D.M.I.E.T.R. Sawangi (Meghe), Wardha (M.S.), India

Abstract: In recent days, usage of internet is increasing so; authentication becomes the most important security services for communication purpose. Keeping this into consideration, there is need of robust security services and schemes. This paper proposes Group Authentication authenticates all users at a time belonging to the same group. The (n, n) Group Authentication Scheme is very efficient since it authenticates all users if they are group members. If they are nonmembers, then it may be used as a preprocess and apply authentication before and it identifies the 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. It results in best authenticated system as the Group Authentication is implemented with Neural Network. So it becomes complicated for hackers to hack each neuron in a neural network. The Neural Network based group authentication is specially designed for applications performing group activities using Shamir Secret Sharing Scheme.

Keywords: Group Authentication; Backpropogation Neural Network; Shamir Secret Sharing Scheme.

I. INTRODUCTION

In recent years the security of operations and authentication provided over the computer network has become very important. It is necessary to protect these actions against attackers who misuse the system. Many cryptographic protocols and schemes were designed to solve problems of this type. Out of these techniques, secret sharing schemes provide an efficient solution. The secret sharing scheme is used for providing authentication to a group communication. These schemes make it possible to store secret information in a network, such that only authorized users can take its advantage and only they can reconstruct the secret.

Different secret sharing schemes available are Shamir Secret Sharing Scheme based on polynomial interpolation, Blakely Secret Sharing Scheme based on hyperplane geometry and Asmuth - Bloom Secret Sharing Scheme based on Chinese Remainder Theorem. This paper proposes the Shamir Secret Sharing Scheme. 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.

Security and authentication plays an important role in every application of computer networks. The real-time data like bank details, personal information, etc, needs more security on public channel. Thus, Secret Sharing provides a security mechanism for network applications. The communication in a group requires a secure channel and an authenticated service. Thus, group communication has motivated from secret sharing schemes available today. Earlier authentication was provided to one-to-one or one-to-many communication. Group Authentication provides authentication for many-to-many communication. It goes beyond unicast and multicast communication. In a group oriented applications, there are multiple members who want to form a private network and to exchange messages among themselves. In such a network, every user participated in the application need to authenticate other users in a same group.

Group Authentication is implemented with Neural Network so it becomes complicated for hackers to hack each neuron in a neural network. Network applications not only work for one-to-one communication, but involve multiple users. So, it results in a secure and authenticated group communication. The proposed scheme helps to remove some drawbacks of the existing scheme and provides more security to the communication system. A Shamir secret sharing scheme is based on linear polynomial and the scheme used previously is (t, m, n) including three tuples. Here, scheme is t-secure, m- user, n- group authentication. Here, security is restricted for m- users out of n- group members. Here, a secret is divided into some number of shares. For reconstruction, if ‘m’ users are available then they can reconstruct the secret. A situation may occur when there is more number of users in a group and only some of them participate in reconstruction phase.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

II. 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 type of authentication. Here, a group manager is responsible to register all group members & 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.

Mitsugu Iwamoto, [4] have worked on A Weak Security (WS) Notion for Visual Secret Sharing Scheme (VSSS). It deals with Weakly Secure and Unconditionally Secure (US) VSSS to be secure against attacker's eyesight. In (k, n) WS-VSSS, the classical unconditional security notion of (k, n) threshold scheme is relaxed in such a way that it is secure if the image obtained by stacking k-1 or fewer shares seems to be a random dot picture. So, the system is effective to analyze combination of sub pixels.

Marin Bertier, [5] have worked on Low Cost Secret Sharing in Sensor Networks. It exchanges secret keys between neighbor nodes not using Cryptography and provides a protected communication in a sensor network and hence provides secure communication. It does not require initial configurations. Based only on exchanges between neighbors, it is very efficient in terms of the number of messages. It also proposes an algorithm that extends the secret key to nodes that are not direct neighbors of each other. Finally the algorithm generates few messages, scales and requires no initial configuration.

Xiang Wang, Qingqi Pei, Hui Li, [6] have worked on A Lossless Tagged Visual Cryptography (LTVC) Scheme. It deals with multi-secret Visual Cryptography Scheme for tag images and prevents the loss in tagged images. The proposed scheme uses Naor and Shamir's technique for a (k, n) scheme. The Lossless Tagged Visual Cryptography Scheme (LTVC) works with Probabilistic P-LTVC Scheme to solve the potential security problem of LTVC. The experimental results prove that LTVC and P-LTVC has a higher Contrast.

Manghui Tu, Peng Li, [7] have worked on Secure Data Objects Replication in Data Grid. It implements secret sharing and dynamic replication to achieve data security in data grid, survivability and access performance. Replicating data shares improves access performance but degrades security. The problem of optimal allocation of data objects partitioned by using secret sharing scheme is also solved here. The proposed approach minimizes the access cost of partitioned data in data grids.

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 & 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 of artificial neural networks in cryptography and studies the performance on approximation problems related to cryptography.

Rajendra A. B. and Sheshadri H. S., [12] have worked on New Approach to Analyze Visual Secret Sharing Schemes for Biometric Authentication - A Survey. This paper proposes theoretical view of Biometric characteristics in image format provided for unique natural signature of a person. Each biometric technique has some advantages and disadvantages and biometrics have been identified as the two most important aspects of digital security. By using this survey, a new method to analyze Visual Secret Sharing Scheme for biometric authentication is given.

Niansheng Liu, Donghui Guo, [13] have worked on Security Analysis of Public - key Encryption Scheme Based on Neural Networks and Its Implementation. It proposes a Cryptography methodology named Diffie-Hellman public-key Cryptography based on chaotic - attractors. They are available in artificial neural networks. It has found some experimental results to show that the proposed cryptography is better, and has a good performance on encryption and decryption process. Also, speed ensures the real time of IPng secure communications. A Hopfield neural network is used with simple structure.

For implementation, secret sharing scheme is reduced to (n, n) i.e. ‘n’ number of users and ‘n’ number of shares. The share generation process divides the secret into ‘n’ number of shares for ‘n’ users. The system is not restricted for particular number of users instead it can process ‘n’ users. All the users take part in secret reconstruction process and if any user is absent then the process cannot work. The goal of authentication system is to provide the exchange of information among the group users who are authorised without any leakage of information to outside users who may have unauthorized access to it. The group authentication can be used to determine following things:

A. Many-to-many type of authentication

The group authentication is a many-to-many type of authentication having multiple number of provers and multiple number of verifiers, for providing more security. There are only two possible outcomes of the group authentication, that are, either all users belong to the same group or there are nonmembers. Thus, the group authentication is implemented for group members only. For nonmembers, it can be used as a preprocess and implements before applying basic user authentication to identify the nonmembers.

B. Generate common secret key

A group of members interact over an open network to establish a common secret key to be used to achieve secure broadcast. Once a secret key is provided to a group, this secret key is shared by all group members. So, only the users in one group can interact with each other and the non-group members can’t. This secret key acts as input to the neural network.
The different stages in the common secret key generation procedure which is based on neural networks can be stated as follows:

1. Determination of neural network parameters. Where the number of hidden layer units and the input layer units for each hidden layer unit.
2. The network weights to be initialized.

C. Achieve authentication mechanism by using Neural Network.

Artificial Intelligence (AI) is a branch of computer science that is based on developing intelligent smart machines and different software using applied logic. It claims the simulation of intelligence of humans by using a machine by employing various factors like reasoning, learning, communication and manipulation. AI is found to have intense applications in various fields. Artificial Neural Networks (ANN) consists of neurons and weights and it is assigned to inter neuron connections and it helps in storing the acquired knowledge. ANN is a nonlinear and parallel adaptive system that is used to model relationships between inputs and outputs. The output is decided by I/O characteristics while the overall working of ANN is determined by its structure and the training algorithm implemented on NN. Advantages of ANN include adaptive interaction between different elements, self-organization, real time operation, parallel computations, and Fault Tolerance. ANN helps in handling critical problems and is used in robotics, pattern recognition, medicine, manufacturing, and optimization; signal processing, system modeling & identification, control of power-generation systems.

In this paper, Cascade - Forward Back-propagation Neural Network is used to achieve authentication and to optimize the processing of communication. ANN parameters include number of training iterations, the number of hidden neurons and the input layer units for each hidden layer unit. Neurons which are not present in input and output layer are hidden from view. Presence of hidden neurons enhances the flexibility of system and increases processing power, but if the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

number of hidden neurons is taken too small then robustness of the system can reduce due to improper fitting of input data. Neural Network works as follows:

Phase 1: Propagation

1. Training the neural network in Forward propagation of input and generate the propagation's output activations.
2. Backward propagation of the output activations through the neural network by using the training pattern.

Phase 2: Weight update

1. Multiply output and input activations for getting the gradient of the weight.
2. Subtracting a ratio i.e. percentage of the gradient from the weight.

This ratio affects the speed and quality of learning, so it is called as the learning rate. The greater is the ratio, the faster is the neuron trains; the lower is the ratio, more accurate the training is.

III. PROPOSED WORK

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.

A. Development of Shamir Secret Sharing Scheme

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

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):

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

such that the secret is,

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

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 & n = k
3. Initialize random coefficient
4. Generate pieces of partial information. Enter part number to use.
5. Shares created.

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.

B. 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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

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.

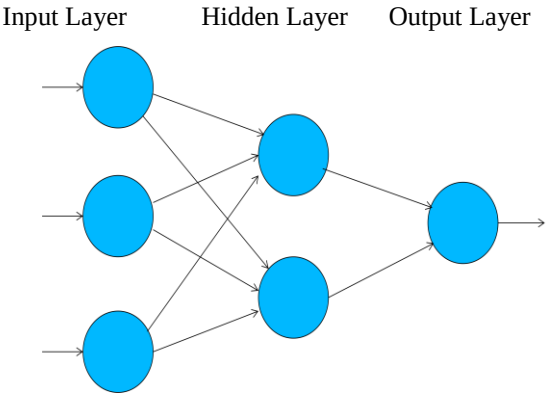


Fig1: Backpropogation Neural Network

C. 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 ε 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 s_i for each group member U_i, secretly, 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 nonmembers.

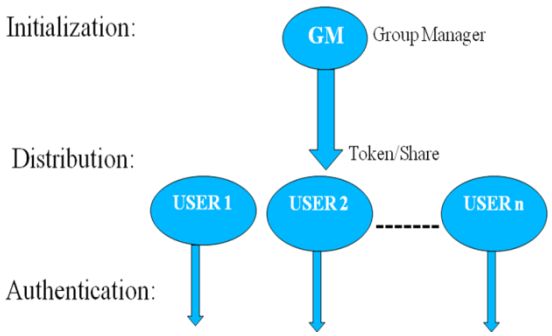


Fig2: Group Authentication Scheme

IV. Experimental Results

The input to the scheme may be an image, a text message, a character, a number or any special symbol.

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

Table 1: Comparison of Scheme.

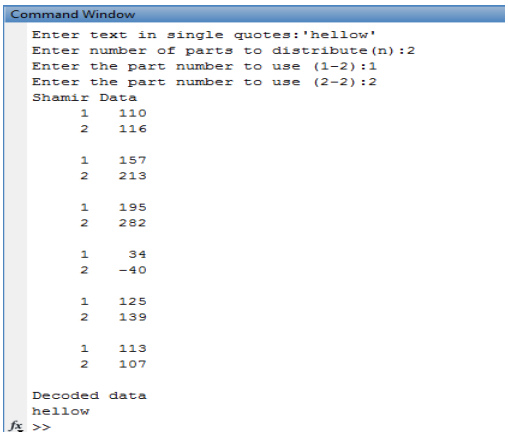
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

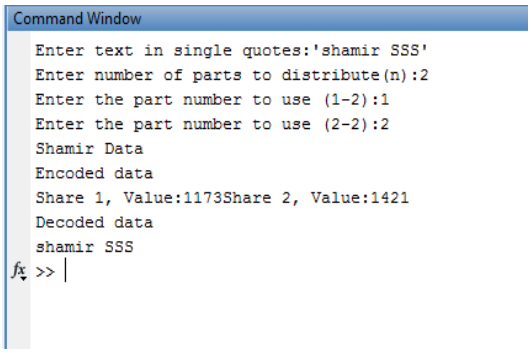
1. Shamir Secret Sharing Scheme:

Encryption and decryption of a message by using implemented Shamir Secret Sharing Scheme is more efficient. The conventional scheme works as follows:



Snapshot 1: Share Generation

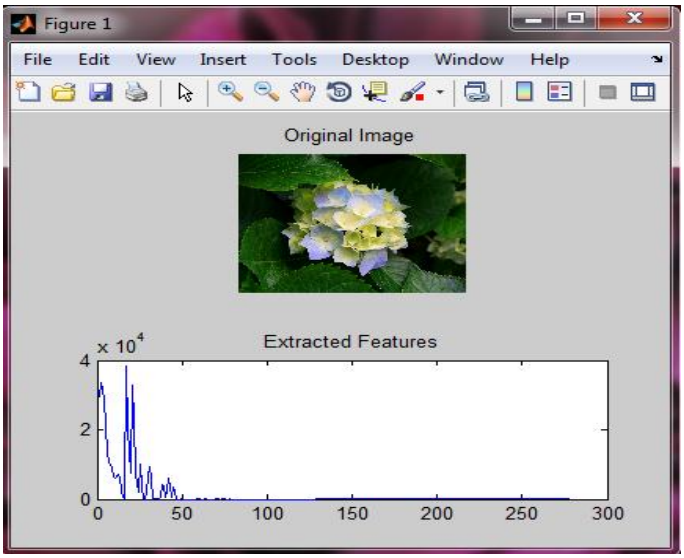
The share generation process is optimized with the given number of parts to distribute the shares only, as follows:



Snapshot 2: Optimized Share Generation

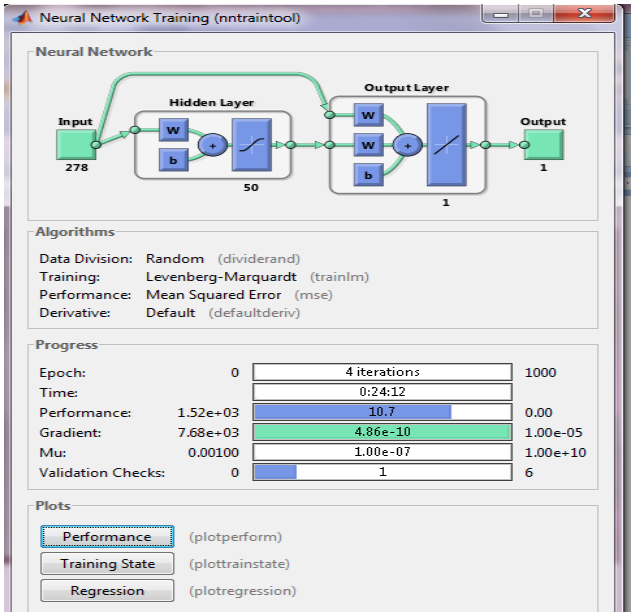
2. Training Neural Network:

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.



Snapshot 3: Feature extraction from original image

Cascade – forward network consist of N1 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 layers has weights coming from the inputs with all previous layers. All layers have biases. The last layer is the network output, called as output layer. Each layers weights and biases are initialized with INITNW. Adaption is done with TRAINS which 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.



Snapshot 4: Neural Network

V. CONCLUSION

The Neural Network based group authentication is designed for group-oriented applications using Shamir Secret Sharing Scheme. It provides many-to-many type of authentication where group activities can be securely done. For accuracy in experimental results, the Backpropogation Neural Network is used.

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.
[15] H. F. Huang and C. C. Chang, "A novel efficient (t,n) threshold proxy signature scheme", *Information Sciences,176(10):1338*–1349, 2006.
[16] Huy Hoang Ngo,Xianping Wu, Phu Dung Le and Campbell Wilson, "Dynamic key cryptography and applications", International Journal of Network Security, Vol. 10, No. 3, PP.161-174, May 2010.
[17] Mitsugu Iwamoto, "A weak security notion for visual secret sharing scheme", IEEE Transactions on Information Forensics and Security, vol. 7, No. 2, April 2012.
[18] Tao Shu, Sisi Liu and Marwan Krunz, "Secure data collection in wireless sensor networks using randomised dispersive routes", IEEE Communications Magzine, pp. 102-114, August 2004.
[19] Huaxiong Wang, Duncan S. Wong, "On secret reconstruction in secret sharing schemes", IEEE Transations on Information Theory, Vol. 54, No. 1, January 2008.