International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 8921-8925
© Research India Publications
http://www.ripublication.com

Chiffrement and Achiffrement of An Image For Secured Wireless Communication Based on Artificial Neural Networks

Arthi.S[1], Jegan.G[2]
[1,2]Faculty of Electronics and Communication, Sathyabama University
[1]arthiraj01@gmail.com, [2]jjsfss@gmail.com

Abstract

in this fast moving society, security is the most important factor to transmit information through internet. There is a great demand for secured data storage and transmission in wireless communication networks. To provide reliable data storage and transmission various types of encryption and decryption algorithms are used at transmitter and receiver side. This paper mainly focuses on the different types of encryption and decryption standards of an image and data using neural networks. The cryptography provides security for bounty of applications against malicious attack in the field of defense, medical imaging and so on. The paper disclose about the survey of neural network cryptography which overcome the drawbacks of basic cryptographic techniques which leads to insecurity and revealed the new back propagation technique to enhance security. Transmission of key is also eliminated, thereby providing greater optimisation.It has many charecteristics: learning, requirement of less data, fast computation, and ease of implementation which secure the process. The proposed system has its applications in medical imaging, banking, satellite imaging, military imaging and other similar applications.

Keywords: Cryptography, Encryption, Decryption, Neural Networks.

Introduction

Cryptography

Cryptography is the science of information security, generating a secret code to transmit data and images securely. The cryptographic methods are of three types: symmetric key cryptography, asymmetric key cryptography and hash function.Generally,plain text is encrypted into cipher text along with secret keys.The process of converting plain text to cipher text is called enciphering or encryption,restoring the plain text is called deciphering or decryption.

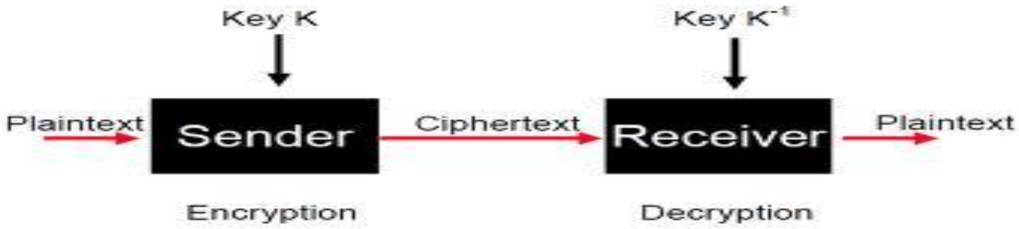

Figure 1.1: Block diagram of cryptography

Neural Networks

The brain is a highly complex,nonlinear and parallel information processing system.It has the capability to organize its structural constituents, known as neurons,so as to perform certain computations many times faster than the fastest digital computer in existence.A neural network is a massively parallel distributed processor made up of simple processing units,which has a natural propensity for storing experimental knowledge and makimg it available for use.It is a simple powerful technique which has the ability to emulate highly complex computational machines.

Neural Cryptography

Neural cryptography is the branch of cryptography dedicated to analyzing the application of stochastic algorithms, especially neural network algorithms, used in cryptanalysis.The three fundamental architectures of ANN are single layer feed forward, multilayer feed forward and recurrent network which is to be trained by learning laws to perform a task. Neural cryptography is carried out through Back Propagation, Multilayer feed forward network, generalized delta rule. The set of input, output data pairs which belongs to a task is given; ANN can learn and exhibit good performance. For these reasons, application of ANN in cryptography has the potential of convenience.

The encryption of data and image is processed by generating a key that is to be transmitted using key generation protocol, General regression neural network, chaotic neural network and Multilayer neural network. Neurons to be trained according to the data of texts and images by their weights and it will act as a key. Neural cryptography is the first algorithm for key generation over public channels which are not based on number theory.

Literature Review

A.Synchronisation Neural Networks, Neural Cryptography, 2003.

Wolfgang Kennel proposed a secret key over public channel using neural networks. The artificial neural network contains of two multi-layer neural networks trained on their mutual output bits and able to synchronize. The common identical weights of the two partners can be used as a key for encryption. The experimental result shows that the model is fast, simple and secure.

B.Cryptography Based On Delayed Chaotic Neural Networks, 2006.
Wensum Yu proposed an encryption techniques based on chaotic Hopfield network with time varying delay. The plaintext is masked by switching of the chaotic neural network maps and permutation of generating binary sequences. Simulation shows the chaotic cryptography is more functional in the secure transmission of large multi-media files over communication network

C.Noise Removal Using Hopfield Neural Network In Message Transmission Systems, 2008.
D.Gladis, P.Thangavel proposed a two-tier encryption with the removal of noise generated during transmission based on Hopfield network. The text and the image pattern are encrypted and pseudo noise is added to them before decoding it. Simulations are carried out with a data set of 50 patterns without noise when compared to patterns with noise. The results show the reduction in complexity of recognition of characters due to external distortion or diffusion.

D.Artificial Neural Network Based Chaotic Generator For Cryptology, 2010.
Ilker Dalkiran,Kenan Danis,Man proposed chaotic systems is sensitive to initial conditions, system parameters is used to train ANN by different learning process. The 24 sets of input are applied to 1800 input-output data. The experiment results show that the major weakness of analogue circuit and the numerical solution of chaotic circuit are eliminated.

E.Design Of An Efficient Neural Key Generation,2011
R.M.Jogdand proposed a common secret key generated based on neural networks. In this network model the weight is imitated randomly and the input object is generated by another source and the output bit is produced finally and exchange between patterns. The modified weights are obtained by matching and synchronizing is used as a secret key for encryption and decryption and decryption process. The results show that the cryptosystem based on ANN is secure.

F.Automatic Decryption Of Images Through Artificial Neural Networks, 2012
Tulay Yildirim proposed the automatic decryption using ANN without knowing what the decoder is.The decryption is processed through Multilayer perceptron and Radial Basis function network was tested using GUI interface.The cryptograph process occurs by applying the inverse of the same encoding method is used,for decoding on the transmitting side.The simulation result shows that RBF was better than MLP with shorter processing time and less error rate.

G.A Triple Key Chaotic Neural Network For Cryptography In Image Processing,2012
Shweta B,presented a triple key chaotic neural network for image cryptography. The triple parameters are used to perform the various operations on image so as to

scramble the data in particular way which look like random but actually it is in particular sequence. This key contains hexadecimal key used to extract and manipulate to achieve the intermediate key which combined with initial and control parameters to generate chaotic sequence. Experimental results shows that algorithm successfully perform the cryptography and can be applied on different colour image size.

H.Neural Cryptography For Secret Key Exchange And Encryption With Aes,2013
Ajit singh presented synchronization neural key exchange algorithm for cryptography. The model has multi-layer feed-forward neural network which have two tree parity machine(TPM) that synchronized with a random initial weight act as a common secret key for the encryption and decryption process. The weight can be updated according to learning rule only if output values of the two machines are equal. The experimental results show that the model are efficiency and secure through increasing the common key size.

Review Results

The above listed papers used neural networks for image encryption and decryption process based on different methods for providing security. But in those methods, key is transmitted along with the encrypted images, this shows that it will subjected to insecurity of images during transmission.

Proposed System

Cryptography of images by neural network, in which encryption is done by randomness process and decryption is carried out by comparing Levenberg-Marquardt algorithm and resilient back propagation algorithm which exhibits greater optimization and provide reduced number of hidden layers.

Conclusion

Insecureness is the major threat in the internet wireless communication systems. Transmission of images is to be securely processed in terms of robust, flexible, accurate, transmission and reception.

References

[1] William Stallings, Cryptography and Network Security: Principles and Practice|| , (5th Edition), Prentice Hall, 2010.

[2] “An Introduction to Neural network" by Ben Krose and Patrick van der Smagt Eighth editionNovember 1996.

[3] Wolfgang Kinzel, IdoKanter, “Neural Cryptography”, Proceedings TH2002 Supplement, Vol. 4, 147 – 153, 2003.

[4] Wenwu Yu, Jinde Cao, “Cryptography based on delayed chaotic neural networks”, Physics Letters A, Vol. 356, (4) Elsevier, 333–338, 2006.

[5] D.Gladis,P.Thangavel, “Noise removal using Hopfield neural network in message transmission”,II UKSIM European symposium on computer modeling and simulation,IEEE,2008.

[6] Ilker Dalkiran, Kenan Danis, “Artificial neural network based chaotic generator for cryptology”, Turk J Elec Eng& Comp Sci, Vol.18, No.2, 255- 240, 2010.

[7] R. M. Jogdand, Sahana S. Bisalapur, “Design of an efficient neural key generation”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.2, No.1, 60- 69, 2011.

[8] Tulay Yildirim, “Artificial decryption based on artificial neural network”,Intelligent system design,Trends in innovative company,2012.

[9] Shweta B. Suryawanshi, Devesh D. Nawgaje,”A triple-key Chaotic neural network for cryptography in image processing”, International Journal of Engineering Sciences & Emerging Technologies, Vol. 2, Issue.1,46-50,2012.

[10] Ajit Singh, Aartinandal, “Neural Cryptography for Secret Key Exchange and Encryption with AES”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue.5, 376- 381, 2013.