VOL. 11, NO. 11, JUNE 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DYNAMIC VISUAL CRYPTOGRAPHY WITH ARNOLD'S ALGORITHM USING ANN FOR MEDICAL DATA PROTECTION

J. Joel Pavithran and T. Vino
Department of Master of Engineering, Embedded Systems, Sathyabama University, Chennai, Tamilnadu, India
E-Mail: joelpavithran@gmail.com

ABSTRACT

Cryptography is the intelligence of varying information into distinct unintelligibility in a way allowing a secret method of un-masculine. The fundamental idea of cryptography is the capability to send information between a party to in a way that prevents others from reading it. Artificial neural networks (ANNs) have been tested to solve many issues. The ANNs have many specialties such as secure, principle, less data specification, fast data processing, ease of performance. A Neural Network is a appliance that is perform to model the way in which the brain performs a work or function of entrust. It has the ability to implement complex ciphering with ease. Visual cryptography finds many functions in cryptographic plot such as key management, message privacy, authorization, verification, identification, and distraction. To implement encrypting, the input to the NN is a fixed of gray like images, and the output is a set of binary images (shares) that fulfills the adorable design. This approach is very much different from the traditional one, and can be enforced to confront with very complex access schemes. Visual cryptography is a secret allocating scheme which uses images allocated as interest such that, when the shares are overlap, a secret image is revealed. In visual cryptography, the share images are constructed to consist of meaningful cover images, thereby keep opportunities for combine visual cryptography and biometric security techniques. In this project we propose neural network based cryptography. First of all we create the neural network based key. This key value is used to calculate the weight for each pixel. This weight is multiplied to the image pixel to form cryptography. Then perform Arnold transform and Random Generator for encryption purpose. Reverse process of encryption original image is retrieved.

Keywords: cryptography, neural cryptography, visual cryptography, arnold's algorithm.

1. INTRODUCTION

There are two processes exist that are used for dispatching information in hidden way. These techniques are known as cryptography and neural network. Both techniques widely used for stability of network or data. Cryptography hidden message in cipher text form so that it is not dependent for illegal party to understand it. New system developed for preferred protection and with conviction. Now days particularly used we have a cryptography art- RSA very protected technique. It is more secure if we send data in secret form as to send it only in crusted form. Verification over in secure public system or with entrusted dependent increment more concerns in isolation and preservation. These models can solve difficult issues that cannot be organized by canonical methods due to the lack of acceptable information. NNs can replace the development of complicated algorithms by means of training by examples also known as managed information.

Visual cryptography (VC), first designed in 1994 by Naor and Shamir [1], is a obscure sharing arrangement, based on black and- white or binary images. Secret images are split into share images which, on their own, reveal no data of the authentic secret. Shares may be assigned to various parties so that only by conspire with an correct number of alternative parties, can the resulting connected shares open the secret image. Reformation of the privacy can be done by overlap the contribution images and, hence, the decoding procedure requires no certain hardware or software and can be easily done by the human eye. Visual cryptography is of precise interest for security applications based on biometrics [2]. For example, biometric data in the form of leading, fingerprint and signature images can be kept privacy by dividing into shares, which can be given for safety to a statistics of parties. The secret image can then retrieved when all parties discharge their share images which are then recommend Cryptography can be defined as the network of data into a mix code that can be break down and sent crosswise a public or private network. Cryptography is the form and study of hiding information. It is a demanding part of secure connection. Cryptography not only assures data from robbery or alternation but can be used as well for user identification.

Is a branch of cryptography committed to analyzing the function of stochastic algorithms, mainly neural network algorithms, for apply in encryption and cryptanalysis. Neural Networks are well known for their capacity to selectively analyze the explanation break of a given complication. This element finds a natural slot of application in the field of cryptanalysis.

At the same time, Neural Networks offer a new access to attack ciphering algorithms based on the standard that any purpose could be reproduced by a neural network, which is a powerful verified computational device that can be used to locate the inverse-function of any cryptographic algorithm. The ideas of common learning, self learning, and stochastic behavior of neural networks and like algorithms can be used for dissimilar aspects of cryptography, like public-key cryptography, solving the key sharing difficulty using neural network mutual organization, hashing or creation of pseudo-random numbers.

Cryptography: This is the study of techniques for make safe the privacy and /or accuracy of information .The two types of cryptology are cryptography, which is the study of the method of such performance and cryptanalysis, which deals with the break down such techniques ,to restore information, or produce information that will be approved as reliable.

Neural network: An artificial neural network repose of several convert units attached in a predetermined aspect to accomplish a aspire to arrangement recognition task.

A. Recurrent Neural Networks (RNN)

Is a network which neurons send observation signals to each other, such as the Hopfield network, Elman and Jordan's network? This enables the design of dynamic behaviors with the obstacle of more memory decrease if compared to straight from the networks?

B. Multilayer neural networks (MLP*)*

MLPs repose of several layers of computational units, consistent in a feed-forward way. MLPs use a variety of information techniques, the most prominent being back-propagation, where the output values are related with the correct answer to figure out the value of some pretend error-function. The error is then sustain back through the network.

C. Neural cryptography

Is a branch of cryptography committed to evaluate the operation of stochastic algorithms, specially neural network algorithms, for use in encryption. Neural Networks are well known for their strength to selectively research the solution space of a given problem. This aspect finds a natural slot of operation in the patch of cryptanalysis.

2. RELATED WORKS

Neural Cryptography with erroneous transmitted information with error prediction

In this paper, the security of neural cryptography was shown to be improved by submit three algorithms, the DTMP algorithm with error forecasting, the SCSFB algorithm, and a hybrid result of both DTMP and SCSFB. The new algorithm SCSFB is a hybrid of the DTMP algorithm and the organization with advice scheme. It is based on the plan that the input vector becomes moderately secret. Therefore, the attacker cannot apply the knowledge rule straight without predicting the secret part of the input patterns. The SCSFB was shown to recover the DTMP security. In addition, the algorithm is effective in its ability to confuse the attacker by not generous any window to conviction the transmitted bits during a certain predefined period [1].

Enhancement key of Cryptography and steganography using RSA and neural network

This research paper presented the work that has been implemented to enhance the Steganography technique. Using DCT for 32*32 blocks and RGB image pixel embedding offers improved results. It is close that operating the pixels to a deeper level increases the quantity of the image to secret certain messages. The Neural Network has been found useful enough to find pixels to extract the data bits with least affecting the original pattern of the image [2].

Recurrent Neural Networks to Design Symmetric Ciphers

In this article, a symmetric cipher design based on the application of regular neural networks in cryptography was distinguished. The proposed design has several advantages due to use of RRNN for symmetric ciphers. The security of the proposed cipher is based on the assumption that the weight distribution of the hidden layers is unpredictable without knowledge of the original key [3].

Cryptography based on neural network

Eva Volna proposed multi-layer neural networks in cryptography. The multilayer neural networks modified by back-propagation. The planned model converted the input message intro ASCII code then gets the sequence of bit for each code which divided into 6 bit blocks are used as input for the encryption procedure. The cipher key is the neural network arrangement limited input layer, hidden layer, output layer, and efficient weights. Experimental results show that the system is secure [4].

Implementation of neural - cryptographic method using FPGA

Karam M. presented a stream cipher system based on pseudo Random Number Generator (PRNG) through using artificial Neural Networks (ANN). The PRNG model has a high statistical randomness property for key sequence using ANN. The proposed neural pseudo random number alternator repose of two stages; the first stage is alternating a long series of arrangement from perfect equation and initial value. So these patterns acquire the randomness and unpredictable properties. The total number of equations and initial values depend on the number of bits that represented the initial value, the second stage is an artificial neural network (ANN) that gets the outputs of the before stage and locate it as input to the NN [5].

Cryptography based on delayed chaotic neural networks

Wen wu Yu proposed an encryption techniques based on the chaotic hopfield neural networks with time unreliable delay. The chaotic neural network is used for introduce binary sequences for protect the plaintext. The binary value of the binary classification chooses the chaotic logistic map any way, that used for generated the binary sequences. The plaintext is masked by switching of the chaotic neural network maps and permutation of bring out binary sequences. Simulation results show that the complex chaotic cryptography is more constructive in the

secure connection of large multi-media files over public data communication network [6].

A triple-key chaotic neural network for cryptography in image processing

Shweta B. presented a triple key chaotic neural network for image cryptography. The triple parameters are used to execute the various operations on image so as to move quickly the data in particular way which look like random but actually it is in particular sequence. The triple key contains a hexadecimal key that extraction and manipulations to achieve the intermediate key which combined with initial and control parameters to generate chaotic sequence [8].

Existing scheme: In existing scheme, nonparametric spatial smoothing filters such as enhanced Frost, enhanced Lee, Gamma, and Kuan filters can use large convolution templates to get satisfactory results; they also simultaneously blur the shape boundary and decrease the accuracy of feature extraction. Edge detection algorithms face a similar issue, where a small convolution window preserves noise, whereas a larger window blurs slick features.

3. METHODOLOGY OF THE WORK

In this project we propose neural network based cryptography. First of all we generate the neural network based key. This key value is used to calculate the weight for each pixel. This weight is multiplied to the image pixel to form cryptography. Then implement Arnold transform and Random Generator for encryption point. Reverse process of encryption original image is retrieved.

Neural network method i.e., using back-propagation feed forward neural networks for abstraction of encoded bits. Using neural networks gives finest results. There are three layer exist one is input and subsequent is hidden layer and further is output layer. In Feed forward workings only in forward direction but in back-propagation feed forward neural networks also works in back direction i.e. back propagates and acquisition errors and update weights consequently. In input layer vectors that are pre-processed are accessible and at output layer calculation of error observed. If error is judgment at output layer then it comes on input layer by backward process. This process is lifelong till the last pattern. This form an emphasis process. At end of every-iteration test patterns are existing to neural network, and the prediction act of network is evaluated.

ARNOLD TRANSFORM

Arnold Transform is commonly known as cat face transforms and is only suitable for N × N images digital images. It is defined as mod N (x, y) and (x', y') {0, 1, 2, ...N - 1} where (x, y) are the same of original image, and (x, y') are the coordinates of image pixels of the transformed image. Arnold Transform is normally known as cat face transform and is mainly apt for digital images of size N × N. It is defined as

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & \\ 1 & 1 \\ 2 & \end{pmatrix} \begin{pmatrix} X \\ y \end{pmatrix}$$

mod N, (x, y) and (x' , y') ε {0, 1, 2, ...N - 1}, where (x, y) are the coordinates of original image and (x', y') are the correlative of image pixels of the transformed image. Transform changes the location of pixels and if done many times, scrambled image is access. N is the height or width of the square image to be handled. Arnold Transform is interrupted in nature. The decryption of image confide in on transformation periods. Period changes in agreement with size of image. Iteration number is used as the encryption key. When Arnold Transformation is functional, the image be able to do iteration, iteration quantity is used as a secret key for obtaining the secret image.

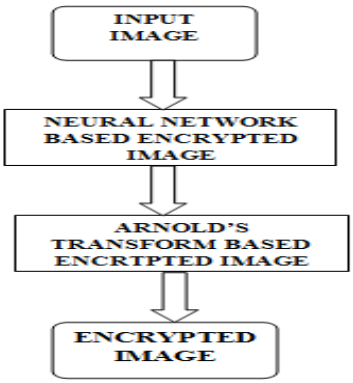

Figure-1. Block diagram of encryption.

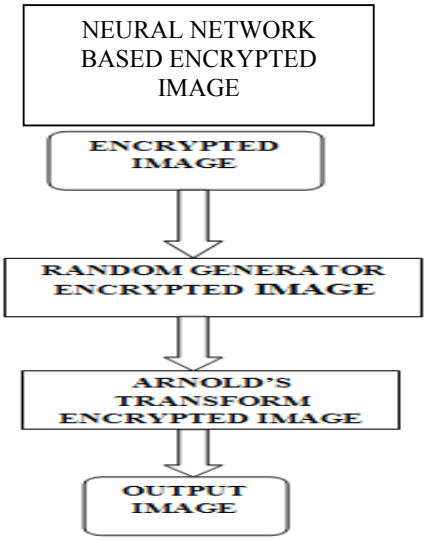

Figure-2. Block diagram of decryption.

4. SIMULATION RESULTS

Encryption

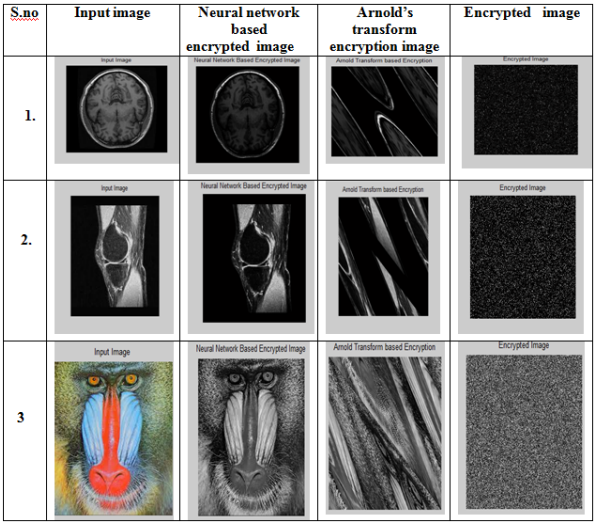

Figure-3. Encryption of input image.

In the above Figure-3, represents the various steps of encrypting the input image by using the key generation of neural network and Arnold's algorithm.

Decryption

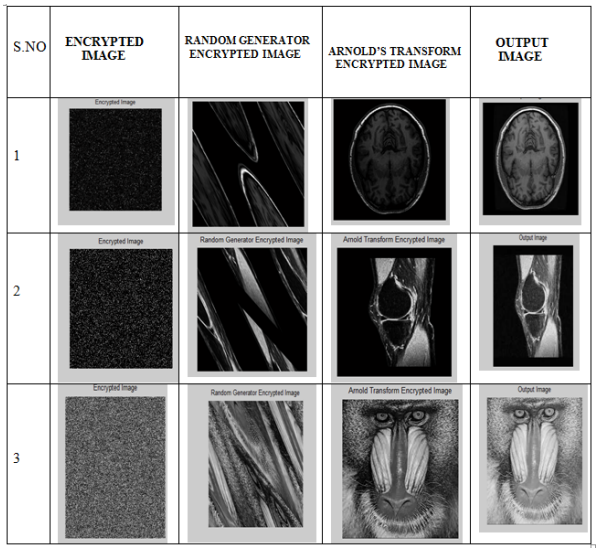

Figure-4. Decryption of encrypted image.

In the above Figure-4, represents the various steps of decrypting the encrypted image by using random generator and Arnold's algorithm to get the output image.

5. CONCLUSIONS AND FUTURE WORK

This paper has some recent analysis about the function of neural network in the range of cryptography. The layout NN-based cryptosystem is a better idea of construction very complicated cryptosystem, where the crypto analyst or the hard track not just need the choro graphy of the NN and the key to crack the system, but also need to know the number of modifying iterations and the final weights for the encryption and decryption systems. Applying higher numbers of plain-text/ cipher-text to the NN-based cryptosystem so as to make the inaccuracy rate as minimum as available. Our proposed method offers better PSNR, MSE values, so results better image quality and better way of hiding messages. It has been also concluded that if we can using visual cryptography by encrypting the data up to some level before merging it to the medical image and data. The Neural Network has been found effective enough to find pixels to extract the data bits with least touching the original size of the image.

REFERENCES

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

[2] T. P. Wasnik, Vishal S. Patil, Sushant A. Patinge, Sachin R. Dave, Gaurav J. Sayasikamal. 2013. Cryptography as an instrument to network security‖. International Journal of Application or Innovation in Engineering and Management (IJAIEM). 2(3): 2-80.

[3] Wolfgang Kinzel, IdoKanter. 2003. Neural Cryptography, Proceedings TH2002 Supplement. 4: 147-153.

[4] Einat Klein, Rachel Mislovaty, IdoKanter, Andreas Ruttor, Wolfgang Kinzel. 2004. Synchronization of neural networks by mutual learning and its application to cryptography. In: proceeding of: Advances in Neural Information Processing Systems 17, Neural Information Processing Systems NIPS.

[5] N. Prabakaran, P. Vivekanandan. 2010. A New Security on Neural Cryptography with Queries‖, Int. J. of Advanced Networking and Applications. 2(1): 437-444.

[6] C.-M. Kim, S. Rim, and W.-H. Kye. 2001. Sequential synchronization of chaotic systems with an application to communication. Phys. Rev. Lett. 88(1): 014103-1-014103-4.

[7] A. I. Galushkin. 2007. Neural Network Theory. New York: Springer-Verlag.

[8] Singla D. 2013. Data Security using LSB and DCT Steganography in images. IEEE International Conference ISSN-2332-1545 Vol. 8.

[9] Usha B.A, Srinath N.K. 2013. Data Embedding Technique in Image Steganography using neural network, IJARCCE. 2(5).

[10] Goel and Rana. A. Comparison of Steganography Techniques. International Journal of Computers and Distributed Systems. ISSN: 2278-5183, pp. 20-31.

[11] I. Woungang, A. Sadeghian, S. Wu, S. Misra, M. Arvandi. 2006. Wireless Web Security Using a Neural Network-Based Cipher. Chapter II in "Web Services Security and E-Business. G. Radhammani and G. S.V. Radha Krishna Rao (Eds.), Idea Group Publishing Inc., USA, ISBN: 1-59904-168-5, pp. 32-56.

[12] A. Allam and H.Abbas. 2009. Improved Security of Neural Cryptography Using Don't-Trust-My-Partner and Error Prediction. International Joint Conference on Neural Networks. pp. 121-127.