iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 7 Issue: II Month of publication: February

DOI: http://doi.org/10.22214/ijraset.2019.2046

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue II, Feb 2019- Available at www.ijraset.com

Cryptography using Artificial Neural Network

Satish Singh[1], Shravan Singh[2], Gaurav Sancheti[3], Rohan Shinde[4], Jyoti Mali[5]
[1, 2, 3, 4, 5]Mumbai university, Atharva College Of Engineering, Malad Marve road, Malad (W) Mumbai 400095

Abstract: The main purpose of this work is to explore the problem the use of artificial neural network for retransmission large satellite image encoding. Central Accreditation uses fixed, arbitrary keys in the learning process such as classical symmetric and asymmetric coding. The network used is NxMxN neurons, hidden and exit levels. The network is being trained weight regulation, and bias is given a fixed value 0 to 1 after normalization. It is biased is determined. Bidability between the input layer and the hidden layer Layer acts as the first key (K1), whereas bias is partial the hidden layer and the outer layer represent the second key (K2).The course method uses K1, K2, or both, and is made through use small sized images to improve speed. Then the network is used to encode and solve images of ordinary satellites. Many tests prepared various satellite optical and SAR pictures and so on content between decoding (decryption quality) good quality images and decoding were at least 98% images that the network has not previously been trained to decode. The also found that the network does not affect geometry image distortion, such as translation, size and rotation.

I. INTRODUCTION

Cryptography is the study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity, and entity authentication. The first try for use of neural cryptography in January 2002 by the physicists Kanter and Kinzel. They introduced a new key exchange protocol between two parties A and B. Theirs method was based on the outcome of two neural networks are able to synchronize to mutual understanding [1]. Synchronized ¿ring (SF) has been observed among cultured cortical neurons, and it is believed that it serves aprominent role in information processing functions of both sensory and motor systems [2]. Synchronization of neural networks applied to cryptography and used for creation of a secure cryptographic

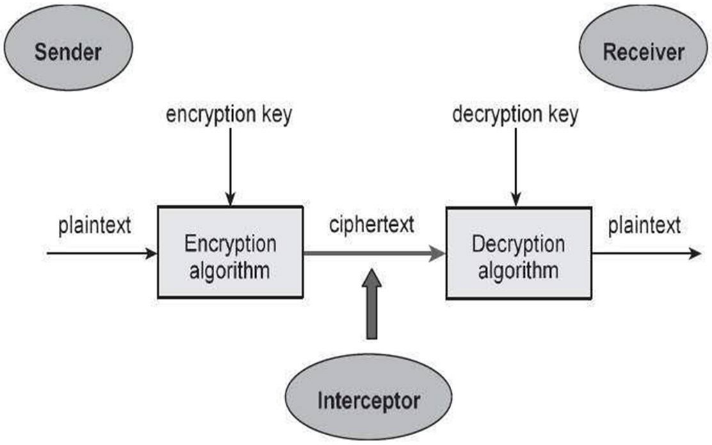

Fig1. Block Diagram

Secret-using a public channel [3-6]. In artificial neural networks (ANN), feed-forward Multilayer perceptions (MLPs) utilize the back-propagation (BP) training algorithm [7]. Backpropagation is one of the most commonly used supervised ANN models. A back propagation network uses the back-propagation learning algorithm to learn how to use the encryption and decryption [8]. In this paper, a simple Multi Layer Perception (MLP) network is used for satellite image encryption. This network consists of N elements as an input layer that feeds a hidden layer of M neurons, which then feeds an output layer the same number of neurons as the input layer. If the input image is for example 50x50 pixels, it will be segmented into L sub-images, each of your size 5x5 elements (N = 25), for instance. Each sub-image is fed to an input to the network. The input and the hidden layers represent the sender (encryption part), and the receiver consists of the hidden and output layers. The back-propagation algorithm is used for adjustment of the weight coefficients of the neuron network. The MLP network was tested using different images, some of which were video images and others were satellite images. The rest of the paper proceeds as follows. The following section contains the structure of the MLP network. Experiments and results are included in Section III. Finally, section IV contains conclusions and future work.

II. IMAGE ENCRYPTION USING FIXED KEYS

This paper presents a new idea of cryptography - we can safely exchange between the use of data S and R. S. represents the sender (encryption) and R presents the site decryption. CPA weight and bias are presented public and private keys. The public key is given, weight after the sake of origin is pure and can be biased After normalizing the values, they have always gained value. Bidability between the input layer and the hidden layer called bias1 (K1) and bias, which is hidden between the layer and the outer layer are called bias2 (K2). Encoding the key is at least one bias (bias 1 or bias or two biases). The K1 or K2 keys or both during a fixed (refillable) period training. The key of the key is determined by: the number of hidden layers in the network configuration. The key is: The length depends on the number of neurons in the hidden layer for bias1 and neurons in the number of ouput strip or input layer, bias 2. The key should be digital. if the keys characters and strings, just ASCII subprogramme to apply. The keys are based on the training data. The main input of this note is to evaluate a new method that is applicable to the NOP for a symbolic number with encryption fixed, arbitrary keys through which the sender (S) and receiver (R) agree with the keys used in the NBP; training. Our technique can also use the NBP as a function asymmetric coding with which the weights represent: public key and bias represent a private key.This work involves the configuration of the NxMxN network neurons that represent input, hidden and output layers, accordingly: The backward-spreading algorithm is exploited purpose of learning. Garlic function is used to hide layer and linear function of output line. Sigmoid: The function is a distinctive function that includes neuron induction range (-∞, ∞) to the new range (0.1). The result: each hidden neuron is determined using the squashing function.Z = 1 / (1 + exp [- (x1v1 + x2v2 + ... + xnvn + b1)]) (1) Linear output produces values inside range (-1: +1). This linear activation function increases: dynamic product range and accelerates convergence levels. The In the second layer, the output of each neuron is clear: Y = m (z1w1 + z2w2 + ... + zMwM + b2) + c (2) where m is on the slope of the straight line, and C represents: Cut the y axis. If minimal and maximum values y are a1 and a2, respectively, then C's value (a1 + a2) / (a1-a2): Figure 1 shows the introductory picture transfer MLP Network (BP). The first and second equations are replaced by Alignment 3 and 4, respectively, equality 3 represents the coverage and 4 is decoded. Z (serum) = 1 / (1 + exp [- (x1v1 + x2v2 + --- + xnvn + K1)]) Y (decipher) = m (z1w1 + z2w2 + --- + zMwM + K2) + c (4) Therefore, we describe the proposed training, encryption and decoding algorithms. Learning algorithm: The training algorithm is based on: adaptive momentum training algorithm [9] and is defined as follows:

1) The key is regulated to obtain real values domain [0, 1] by the equation. Norm (K) = Ki / max (Ki), 1 <= i<= N or M (5) Where N is the number of inlay / outbreak neurons, and M is the number of neurons hidden in the strip.
2) Initialize weight with matrix V and W randomly with values from 0 to 1.
3) The embodiment embodied in subparagraphs L, each having N; elements of the pictures (pixels).
4) The input vector (,, ...,) k 1 2 N X = x xx is calculated each sub-picture and network transfer as an input layer. Vector X k is calculated by setting the lower image by dividing the value of each pixel to the maximum possible pixels value (eg 255) or using a simple relationship. () 1 / [1 exp ([] / 2)] k i k k X i = + - x-μ (6) Where μ k and σ k are mean and standard deviations respectively, X k and k are the input predictive index. Then the result of the hidden layer (, ...,) 1 2 M z zz calculated by equation (1). The structure of the neural network used for the 1st image encoding and formula.
5) Results of response layer (, ...,) 1 2 N y yy taking into account (, ...,) 1 2 M z zz and weighing After activating the matrix W, using the linear function Balance 2:
6) The difference between the desired result (original:sub-picture) and the actual result(,,, ...,) 1 2 N y yy step (n) is calculated using: on this occasion, Y (pen) z (password)

VN WN 1 x2 xNx1hMz 1 hour 2h N y

Introduction to Hidden Layer K1 K2 V1 W1 ICCTA 2012, October 13-15, Alexandria, Egypt

1) [| ()] =Δ = -N. iii n x y (7)

(7) Since the coefficient of production () wp, q n represents weight a hidden neuron "p" before the production neuron "q" before weight regulation, then (1) wp, q n + after weight The adjustment can be calculated as follows: I- Portable δ q signals in the production layer of neuron "q"given that,

() q qq δ = m x - y (8)

II- Updated weight (1) wp, q n +

Calculated at n + 1:

how:

(1) (1) wp, q n + = wp, q n + Δwp, q n + (9-a)

(1) [(]] Δwp, q n + = ηδ q z p + α Δ wp, q n

, (9b)

where η is the learning coefficient (usually 0.01 to 1.0); α effect factor (usually about 0.9).

(8) Weight () vi, p n between hidden neurons and between then the i-input junction is similar to the step (7) change p z to i x, and δ q tod p. But the mistake The signal p p for the hidden neuron p is calculated using on the occasion of: | == -N.kp ppkwp k z zz1, δ (1) [δ] (10) (9) Let Δ (n) and Δ (n +1) indicate old and new errors accordingly: If d (n + 1)> 1.04 [Δ (n)], the new one weights, keys (permanent), products and errors are stored as old values, while α has changed to 0.7a. If Δ (n +1) <= Δ (n), new weights, keys (constant), product and error are updated with new values and α changes to 1.05a.

(10) The four steps above (step 6-9) are repeated until the end the actual error Δ (n) is less than the predetermined value; The circus (aca) is equal to some values.

A. *The Encoding Algorithm Is As Follows*

1) The input image is segmented in L windows; sub-images of each size L1xL2 = N pixels. Then, each sub-picture is regulated as it is nervous networks work better if investments and keys lie 0 to 1 [11].
2) N's normalized subsystems are input: network and hidden layer product calculated using the equations 3 and 4 the input image NL is therefore the hidden product the layer is a ML size vector where M is The number of hidden neurons.
3) N inputs are 8-bit digital numbers and: The hidden layer's results are M real values transfer as a password. To get it right? image encoding, hidden layer results generate quantitative. This is the action is done by rounding each neuron after multiplication 255 products.
4) The encoded image is generated by conversion the result of a layer covered by a layer of one size in a two-sided matrix.

B. *The Document Decoding Algorithm Is As Follows*

1) the elements of the coded image M are entered: the output layer of the decoding unit and so on protocol production layer („ ...,) 1 2 Y yyy calculated from Equation 1.Using the result layer response, which is in size NL pixels, the decoded image is transformed into extracted mass in two-sided matrix.The NxMxN network structure has been used with different numbers of hidden neurons M = 4,6,9,16 and 25 are the best structure to choose for coding purposes; There is no definite method or approach determine the best structure [10]. Network Relationships: structure and coding accuracy Next section, using MATLAB attempts. It's important Please specify here that the input vector size is fixed to 25 elements and network trained only on 75 images size 50x50 pixels, 256 gray levels.

III. EXPERIMENT AND RESULTS

Six sources of satellite imagery have been used for training and use test the proposed encoding / decoding algorithms. All images have 256 gray levels. Source1 images captured photo shop for various human figures (women, men and children) and digitized by 50x50 pixels 256 gray level. Source2 images are 48 images of 6 planes models; each has 8 images in different directions and all The images are 50x50 pixels in size. Source3 images were: collected public magazines, stories and cartoons, and all digitalized at 512x512 and 50x50 pixels. Source 4 images downloaded from Internet 1 . Source5 images Iconsos were electro-optical satellite imagery satellite 2 Size 512x512 pixels. Source6 images Synthetic images of radio porridge (SAR) 3

From the above 6 sources, the images were divided into more than 6 devices. Set1 contains 108 images Source1, Source2 and Source3. Set2 consists of 60 images Four of the different sources and figures (women, men, etc.) children) from Source1. Set3 had a 4-dimensional image From 512x512 to Source3: Set4 contains 14 synthetic diaphragms Radar images (SAR) from Source6. Set5 consists of 12 images of electro-satellite images from Source5. set6 used for training and contains 50x50 images Source1, Source2 and Source3. Attempts were made on the following computer: H / W and S / W Configuration Intel (R) Core (TM) i3 Processor M330 @ 2.13 GHz, 4 GB of RAM and 64-bit operating system. The algorithm has been implemented on Matlab 6.0.0.88 Release 12. To perform an encoding evaluation: algorithm, the goodness of φk adapts to the original and the decoded images are calculated using simple report. where Xl represents the sub-legal inputs of the sizes L and Yl corresponding decrypted image. Several numbers of hidden neurons (4, 6 and 25) Fixed nodes of input and output were used for impact analysis the number of hidden neurons. Detected as a number the growth of hidden neurons, improved improvement, as indicated in Table 1. The received network (25x25x25) is convenient larger satellite images with K1 keys,K2 or two K1 e K2. Satellite images of Set4 and Set5 have been tested using the nerve BP network with fixed keys, K1, K2 or both. Attempts have brought at least 98% of the goodness 2 Http://www.mapmart.com/Products/SatelliteImagery/IKONOS.aspx 3 From http://www.jpl.nasa.gov/radar/sircxsar/ for convenience. Set4 when decoding the image quality The course was conducted in K1 fixed with 99, 99, 98, 99, 98, 99, 99, 99, 98, 98, 99, 99, 99 and 99 respectively Table 2, Figure 2 and Figure 3. Figure 2 Decoding quality for K1 (set4) The quality of decoded images of Set5 during the course 99, 99, 99, 99, 99, 99, 99, 99, 99, 98, 99, 99, 99, 99, 99, 99 and 99 as presented in Table 3, 4 and 5.

IV. CONCLUSION AND FUTURE WORK

Multilayer progress perc back-propagation (BP) has been found cryptographic applications that use fixe classic cryptography. The length structure of the neural network. Th the algorithms worked well on the image the network has not been trained. The it was not influenced by geometric image, as translation, scale, an network has proved suitable for images, such as satellite images, w at least 98%. The reconstructed goodness of adaptation better than that of me and each took about 1.6 minutes important to mention here that the satellite images. For future work, efficiency the proposed algorithms will be ev randomness measures, and the pr compared to the traditional image.

REFERENCE

[1] N. Prabakaran, P.Loganathan and P.Viv with multiple transfer function International Journal of Soft Computin Magazines, 2008
[2] ErolGelenbe, Stelios Timotheou, "R Synchronized interactions ", Neural Com © 2008 Massachusetts Institute of Tech
[3] I. Kanter, W.Kinzel, "The Theory of Cryptography ", Quantum Computers an
[4] R. M.Jogdand1 and SahanaS.Bisalapur KEY GENERATION NEURAL ", In Intelligence & Applications (IJAIA), V
[5] Roland E. Suri, Terrence J. Sejnowski, long asymmetric asymmetric lea (2002) DOI 10.1007 / s00422-002-0355-
[6] David Norton and Dan Ventura, "Prepare Machines that use hebbian learning Conference on the Sherat neural networks Vancouver, BC, Canada July 16-21, 20
[7] JoarderKamruzzamanMonash, "Artif and production ", the Idea group publishers
[8] Khalil Shihab, "A cryptographic scheme Proceedings of the 10th WSEAS COMMUNICATIONS, Vouliagmeni.
[9] Enrique Castillo, Bertha Guijarro-Berd Amparo Alonso-Betanzos, "A Very First Networks based on Sensitivity Analysis Research 7 (2006) 1159-1182
[10] TaskinKavzoglu, "Determination of Optimum Networks ", in Acts of 25 A Remote Sensing Membership Show 10 September 1999.
[11] S. Anna Durai and E. "Anna Saro, Propagation of the neural network using World Academy of Science, Engineering