ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 17-21

Hybrid Cryptography Using Artificial Neural Network

Satish Singh Yadav[1], Gaurav Sancheti[2], Rohan shinde[3] , Shravan Singh[4], Prof. Jyoti Mali[5]

[1](extc, Atharva College Of Engineering, India)
[2](extc, Atharva College Of Engineering, India)
[3](extc, Atharva College Of Engineering, India)
[4](extc, Atharva College Of Engineering, India)
[5](extc, Atharva College Of Engineering, India)

Abstract: *The main objective of this work is to explore the problem: the use of artificial neural networks for the retransmission of the encoding of images of large satellites. The central accreditation uses fixed and arbitrary keys in the learning process, such as classical symmetric and asymmetric coding. The network used is NxMxN neurons, hidden levels and output. The network is being trained to regulate the weight and the bias receives a fixed value from 0 to 1 after normalization. Is biased is determined. The supply capacity between the input layer and the hidden layer, the layer acts as the first key (K1), while the 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 done by using small-sized images to improve speed. Then, the network is used to encode and resolve images from normal satellites. Many tests prepared several satellite, optical and SAR images, and so on, the content between decoding (quality of decryption), good quality images and decoding were at least 98% of images that the network has not been previously trained to decode. They also found that the network does not affect the distortion of the geometric image, 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 attempt to use neural cryptography in January 2002 by physicists Kanter and Kinzel. They introduced a new key exchange protocol between the two parties, A and B. Their method was based on the result of two neural networks that can be synchronized with mutual understanding. The synchronized ring (SF) has been observed among cultured cortical neurons, and is believed to play a prominent role in information processing functions of sensory and motor systems. Synchronization of neural networks applied to cryptography and used for creation of a secure cryptographic secret-using a public channel. In artificial neural networks (ANN), feed-forward Multilayer perceptions (MLPs) utilize the training algorithm of backward propagation (BP). The backward propagation is one of the most used ANN supervised models. A backward propagation network uses the backward propagation learning algorithm to learn how to use encryption and decryption. In this document, a simple Multilayer Perception Network (MLP) is used for the encryption of satellite images. This network consists of N elements as an input layer that feeds a hidden layer of M neurons, which then feeds an output layer with the same number of neurons as the input layer. If the input image is, for example, 50x50 pixels, it will segment into L sub-images, for example, each of its elements of size 5x5 (N = 25). Each sub picture is fed to an entrance to the network. The entry and hidden layers represent the sender (encryption part), and the receiver consists of the hidden and output layers. The backward propagation algorithm is used to adjust the weight coefficients of the neural network. The MLP network was tested using different images, some of which were video images and other satellite images. The rest of the article continues as follows. The following section contains the structure of the MLP network. The experiments and the 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 output strip or input layer, bias 2. The key should be digital. if the keys characters and strings, just ASCII sub-programme 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 encoding algorithm is as follows:

The input image is segmented into windows L; sub-images of each size L1xL2 = N pixels. Then, each secondary image is regulated, since the nerve networks work better if the inversions and the keys are between 0 and 1) The normalized subsystems of N are entered: the network and the hidden layer product are calculated using equations 3 and 4, the input image NL is, therefore, the hidden product. The layer is a protocol production layer (...) of equation 1. Using the response of the resulting layer, which has a pixel size NL, the decoded image is transformed into mass extracted in a matrix of two faces. 9, 16 and 25 are the best structure to choose for coding purposes; there is no defined method or approach that determines the best structure . Network relationships: structure precision and coding Next section, using MATLAB attempts. It is important. Specify here that the size of the input vector is set to 25 elements and the network is trained only in 75 images of size 50x50 pixels, 256 levels of gray.

Introduction to the hidden layer K1 K2 V1 W1 ICCTA 2012, from October 13 to 15, Alexandria, Egypt

1) [| ()] = Δ = -N. iii n x y (7)

(7) Since the production coefficient () wp, qn represents the weight of a hidden neuron "p" before the producing neuron "q" before weight regulation, then (1) wp, qn + after the weight. I- Portable signals in the production layer of the neuron "q", given that

() q qq δ = m x - y (8)

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

Calculated in n + 1:

(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); Effect factor α (usually around 0.9).

(8) The weight () vi, p n between the hidden neurons and between them the i-input junction is similar to step (7) changes p z to i x, and all q tod p. But the error The signal p p for the The hidden neuron p is calculated with the following reason: | == -N.kp ppkwp kz 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)], new weights, keys (permanent), products and errors are stored as old values, while α has changed to 0.7a. If Δ (n +1) <= Δ (n), the new weights, keys (constant), product and error are updated with new values and α changes to 1.05a.

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

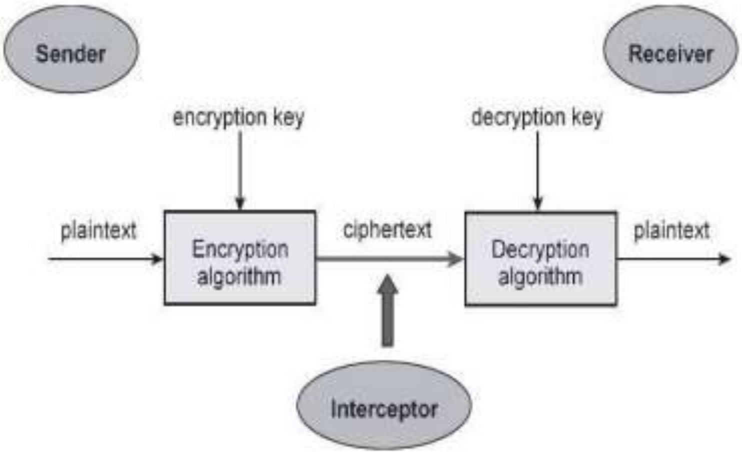
USING NEURAL NETWORK TO LEARN THE PUBLIC KEY:

An encrypted message has (N+N') bits. However, it will have only 2N valid states.Noother state is generated. To learn the Public key, the valid states are fed to asupervised neural network. We will expect that the initial message M will show up as the output. In other word, training set will be the following pairs:

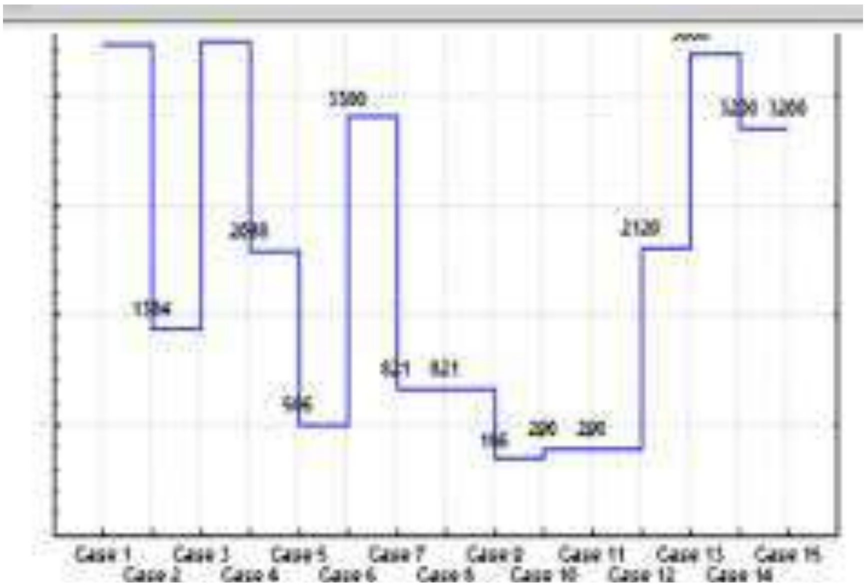
{(E0, M0), (E1, M1)…(E2N-1, M2N-1)}. The neural network used in the decryption process is a 3-layer feed-forward network implementing the back propagation algorithm. There are 16 neurons input layer, 24 neurons in the hidden layer and 12 neurons in the output layer.

III. Experiment and Results

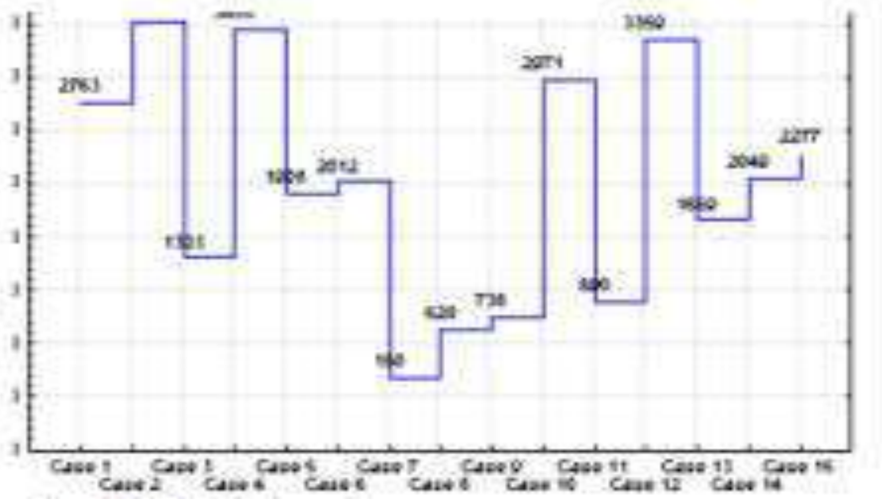
Six sources of satellite imagery have been used for training and use test the proposed encoding / decoding algorithms. All images have 256 gray levels. Source1 images captured photo shop for various human figures (women, men and children) and digitized by 50x50 pixels 256 gray level. Source2 images are 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 Icons 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. (10)



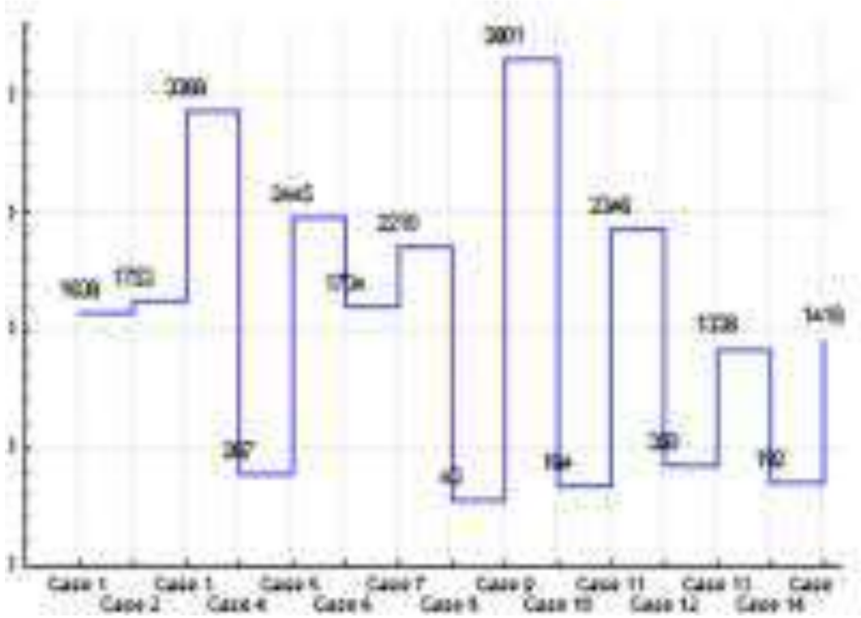
Source3: Set4 contains 14 synthetic diaphragms Radar images (SAR) from Source6. Set5 consists of 12 images of electro-satellite images from Source5. Set6 used for training and contains 50x50 images Source1, Source2 and Source3. Attempts were made on the following computer: H / W and S / W Configuration 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 ok is adapted to the original and the decoded images are calculated using a simple report. Where Xl represents the sub-legal entries of the sizes L and Yl corresponding to the decrypted image. Several numbers of hidden neurons (4, 6 and 25) were used. Fixed input and output nodes for the impact analysis and the number of hidden neurons. Detected as a number the growth of hidden neurons. The received network (25x25x25) is convenient larger satellite images with K1, K2 or two K1 and K2 keys. The satellite images of Set4 and Set5 have been tested using the BP nerve network with fixed keys, K1, K2 or both. Attempts have brought at least 98% of goodness. From for convenience. Set4 when decoding the image quality Attempts have brought at least 98% of the goodness for convenience. Set4 when decoding the image quality.The course was conducted in fixed K1 with 99, 99, 98, 99, 98, 99, 99, 99, 98, 98, 99, 99, 99 and 99 respectively. Figure 2 Decoding quality for K1 (set4).The quality of decoded images of Set5 during the course 99, 99, 99, 99, 99, 99, 99, 98, 99, 99, 99, 99, 99, 99 and 99.



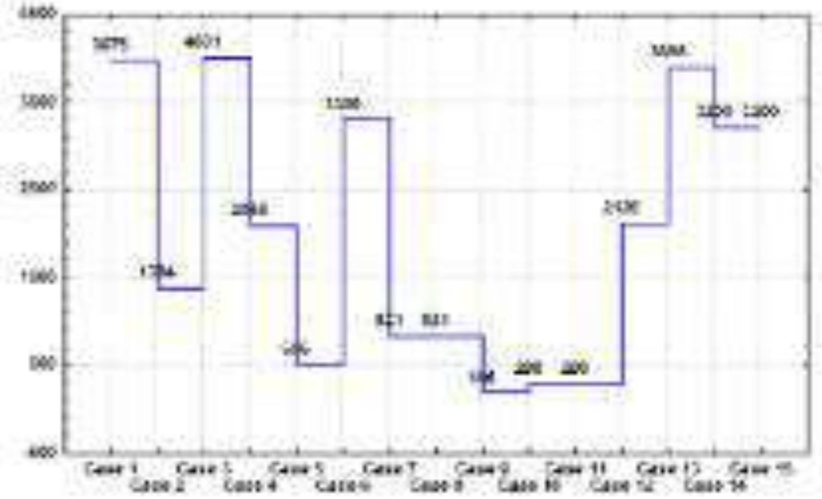
Original signal before encryption



XORed signal

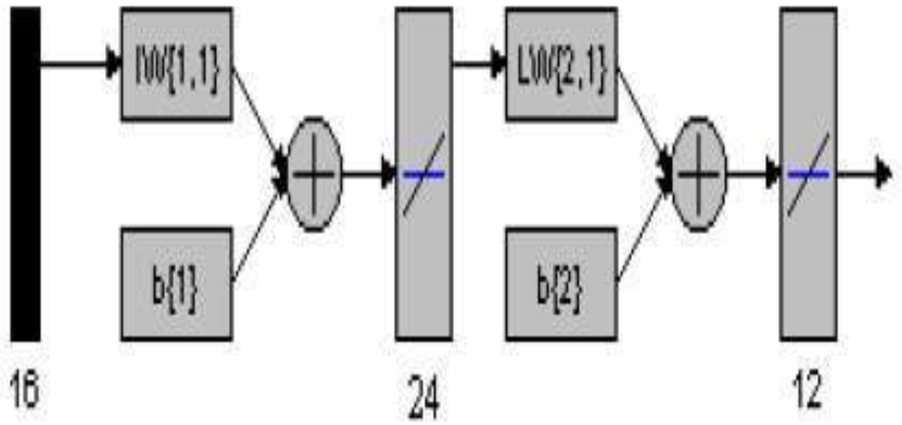


Permuted signal



Decrypted signal

DECRYPTION PROCESS USING ANN



IV. Conclusion and Future Work

The progress of multiple layers of backward propagation (BP) has been found in cryptographic applications that use fixed classical cryptography. The length structure of the neural network. The algorithms worked well on the image that the network has not been trained. The geometric image was not influenced, as the translation, the scale, a network has proven to be suitable for images, such as satellite images, with at least 98%. The reconstructed goodness of the adaptation is better than mine, and each one took about 1.6 minutes of importance to mention the satellite images here. For future work, the efficiency of the proposed algorithms will be the randomness measures and is 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