JPEG2000 COMPATIBLE NEURAL NETWORK BASED CIPHER

Qurban A Memon

UAE University, 15551, Al-Ain,
United Arab Emirates, qurban.memon@uaeu.ac.ae

ABSTRACT. In this paper, an efficient encryption technique is proposed, especially for JPEG2000 compatible images. The technique uses a multilayer neural network to generate a pseudo-random sequence for transforming wavelet subbands into cipher subbands. The neural network generator takes 64 bit key as a startup seed with additional 64 bit key for initial weights and biases. At each layer, output is calculated by several iterations to increase the complexity of the pseudorandom sequence generation. In order to examine effectiveness of this approach, various tests including correlation, histogram, key space etc. are conducted on test images, and the results demonstrate the robustness of the proposed approach.

Keywords: JPEG2000 compatible cipher; neural network based random sequence; block cipher; encryption

INTRODUCTION

In multimedia communication and data storage, security and protection of data is essential to fulfil vendor rights and client requirements. This may require encryption of image data as an alternative to other approaches. Recently, a great deal of concern has been raised regarding the security of the image transmitted or stored over public channels, and a lot of research works are being reported in this field. For example, the author (Lian, 2007) investigates neural network properties to propose low-cost authentication for images or videos. The author claims that the approach has the embedded ability to detect whether the data is modified maliciously. The author finally discusses open issues in this field like: which property of neural networks to be exploited for data protection; which neural network models are suitable for data protection; and learning ability of neural networks, etc. In another work (Munukur, Gnanam, 2009), the authors aim to use neural network in the receiver for the purpose of decryption. The authors use back propagation algorithm in the receiver to train it with a 12-bit cipher text as an input, and 8-bit plain text being the target output. The approach also introduces some impurity in the plain text at the transmitter to misguide any eavesdropper. However, this addition of impurity in the plaintext requires a pre-determined key. The authors (Lian, 2009) propose a neural network that is composed of a chaotic neuron layer and a linear neuron layer. The network is used to construct a block cipher that encrypts the plaintext into a cipher text using a key. The objective set in the work is to construct a chaotic neural network (CNN) based block cipher with good computing security. The block cipher involves two processes: diffusion process implemented by chaotic neuron layer and confusion process implemented by a linear neuron layer. These processes are iterated a number of times to improve the encryption strength.

The Chaos has also been investigated in combination with neural networks. The authors (Lian, 2011) exploit neural network structure to process many media contents in the parallel manner. The idea used is to construct an encryption/decryption scheme that uses chaos and neural networks. The scheme combines encryption and watermarking together. The encryption part uses random sequences generated from chaos system with the help of an encryption key. This key is then used to encrypt media contents with a neural network structure. However, there is apparent disadvantage in this scheme that more sub-keys need to be transmitted to the receiver. Similarly, the work in (Joshi, et al, 2012) aims at secure image transmission using randomness in encryption algorithm, thereby creating more confusion to obtain the original data. The security of the original cipher has been enhanced by addition of impurities to misguide the cryptanalyst. Since the encryption process is one way function, the artificial neural networks are claimed to be best suited for this purpose as they possess features like high security, no distortion and its ability to perform for nonlinear input-output characteristics, Thus, the need for key exchange is also eliminated, which is otherwise a perquisite for most of the algorithms used today. In another research (Bigdeli, et al, 2012), the authors propose an image encryption/decryption algorithm based on chaotic neural network. The employed network comprises two 3-neuron layers: chaotic neuron layer (CNL) and permutation neuron layer (PNL). The authors use a 160-bit-long authentication code to generate initial conditions and the parameters of both layers. In this approach, the overall process is repeated several times to make it more robust and complex. The proposed method uses two more keys where a slight mismatch in one of them results in a severely decrypted image. In another work, the same authors (Bigdeli, et al, 2012) propose an encryption method that is based on a new hybrid chaos-based encryption algorithm. The algorithm carries permutation–diffusion architecture, where chaotic control parameters are used for permutation. A logistic map is used to generate these chaotic control parameters for the permutation stage. Next, in the diffusion stage, another chaotic logistic map with different initial conditions and parameters is used to generate the initial conditions for a hyper-chaotic Hopfield neural network to generate a key stream for image homogenization of the shuffled image. For further reading, the reader may refer to (Memon, 2006 and 2014). As a summary, many research works have appeared in literature to address encryption of data before transmission. The concern that is still being investigated is the robustness in presence of malicious attack, as well as compatibility with current transmission standards.

In this research, neural network structures are examined in combination with wavelet transform for image encryption and decryption. The motivation behind use of wavelets is that current image transmission and storage is mostly preferred using JPEG2000, which is a new standard for image transmission and coding. This is motivated by the fact that the JPEG2000 is better at compressing images (up to 20 per cent plus), and that it can allow an image to be retained without any distortion or loss (Nguyen, and Marpe, 2014). The paper is structured as follows. In the next section, proposed approach is presented that describes key parts of the solution. Section 3 analyzes the performance of the approach with regard to key space, histogram, correlation coefficient and 0/1 balancedness test. In section 4, conclusions are presented.

PROPOSED APPROACH

In this section, we present the approach. Consider plain image $p(x, y)$ of size NxN. The first step in JPEG2000 is to apply n-level wavelet transform to the image. For purpose of simplicity, assume that n=2. This means that wavelet transform will produce 4 frequency subbands of the image, where each is of quarter-size. Thus, this variable n can also play a role to create an ambiguity about how many subbands have to undergo encryption stage. In this paper, the approach is not to apply encryption on these subbands directly; rather these subbands undergo bit plane decomposition to generate eight (8) binary images for each subband. Depending upon need, a set of these binary images is transformed into encrypted bit plane images. If desired, these subbands can undergo next step of the JPEG2000 encoder, or otherwise inverse wavelet transform can be applied to generate encrypted image. The set of binary images for encryption is another variable to introduce ambiguity. The proposed approach is shown in Figure 1, where CT stands for chaotic transformation involving a pseudo-random based sequence generated by 8-4-2-1 chaotic neural network. This is simply an XOR operation between random sequence and the subband image pixels. In the following paragraph, this is further discussed.

An 8-4-2-1 neural network, as shown in Figure 2, is used to generate pseudo-random sequence. The objective behind this architecture is to introduce non-linearity in the generating a sequence, besides a 64-bit input key i.e., A= [A_1, A_2, A_3, ……, A_{64}] is applied at the input layer such that 8-bits enter at each node of the layer. The output of this layer may be written as:

$$B = f^{n0}(Aw_o + A_o, K_0) \tag{1}$$

where w_0 is the matrix of size 8x8 *i.e.*, w_0=[$w_{0,0}$, $w_{0,1}$ $w_{0,2}$ $w_{0,3}$ $w_{0,4}$ $w_{0,5}$ $w_{0,6}$ $w_{0,7;}$ $w_{1,0,........;}$ $w_{7,7]}$, A is the input vector, the bias is A_0 = [a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7], K_0 is the control parameter [k_0, k_1, $k_{2,\ ......,}$ k_7] and $n0$ is random number generated by key generator in the range 1≤ $n0$ ≤10. The function f is the transfer function based on piecewise linear chaotic map (PWLCM) (S. El Assad, et al, 2008) and is given by:

$$x(n) = f\big(x(n-1)\big) = \begin{cases} \dfrac{x(n-1)}{k} & if\ x(n-1) \in\ [0, k[\\ \dfrac{x(n-1)-k}{0.5-k} & if\ x(n-1) \in [k, 0.5[\\ f\big(1-x(n-1)\big) & if\ x(n-1) \in\ [0.5, 1] \end{cases}$$

where k ε [0, 0.5[and x(n) ε [0, 1]. x(0) and k are used as secret keys. For a dynamical system to generate highest lyapunov exponent, k is typically chosen to be 0.5.

Similarly, the output of each layer becomes input to the next layer, apart from becoming input to that neuron itself. Continuing in the same fashion, the output of remaining layers is calculated as follows:

$$C = f^{n1}(Bw_1 + B_o, K_1) \tag{2}$$
$$D = f^{n2}(Cw_2 + C_o, K_2) \tag{3}$$
$$O = f^{n3}(Dw_3 + D_o, K_3) \tag{4}$$

where the matrices w_1, w_2, w_3 have sizes equivalent to 4x8, 2x4 and 1x2; B_0, C_0, D_0 with sizes 4x1, 2x1, and 1x1; $K_{1,}$ $K_{2,}$ K_3 with sizes 4x1, 2x1, and 1x1, respectively. During iterations at each layer, the control parameters are also adjusted using respective layer outputs in such a way that respective range lies in [0.4, 0.6], for example K_0=0.2xB+0.4 to get chaotic behavior. Like n_0, the values of n_1, n_2, and n_3 are obtained through key generated. Once the value of output is obtained between 0 and 1, then this value is normalized in the range 0-255. In order to enforce randomness, this normalized value is then compared with a threshold of 127 to take 0 or 1 in the sequence.

Key Generator: Many chaotic key generators exist but the one used in this research involves 1-D cubic map (Djellit Ilhem and Kara Amel, 2006). It takes 64-bit random key, calculates initial conditions based on its 16-bit component and returns values of the map using iterations. The states of the cubic map are written as (Gao, T., and Chen, Z, 2008):

$$y(n+1) = \lambda y(n)\big(1 - y(n).y(n)\big) \tag{5}$$

where λ is typically set at 2.59 as a control parameter, and state of equation is satisfied by 0 ≤ y(n) ≤1.

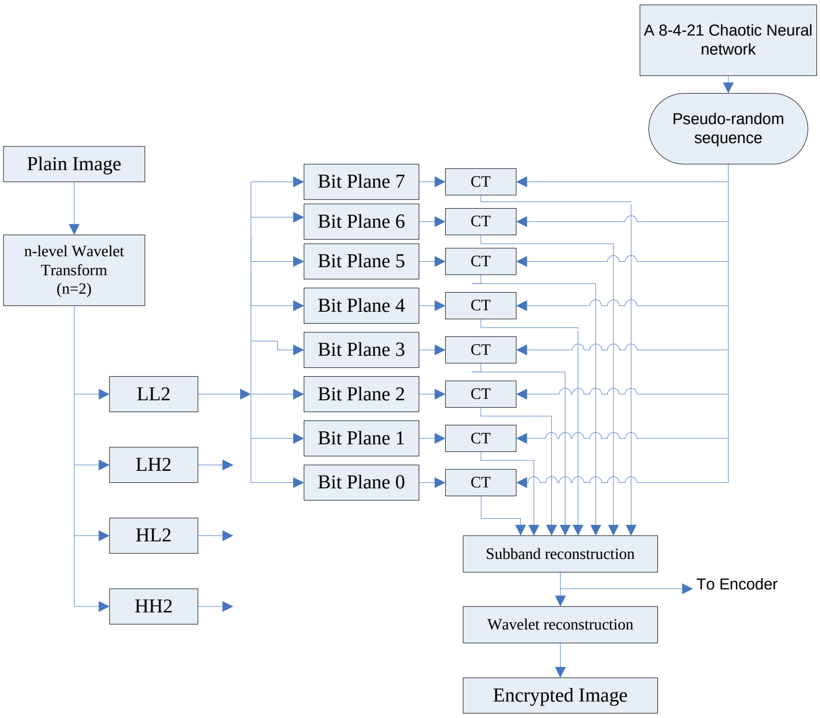

Figure 1. Proposed Approach

PERFORMANCE ANALYSIS

In this section, different measurement and tests are described that demonstrate the effectiveness of the proposed approach:*Key space*: The key space of the proposed scheme can be derived from two parts: neural network key generator, and *n*-level wavelet signal decomposition. There are two keys used: one is the 64-bit seed to neural network and another is the 64-bit to calculate initial conditions. The number of bits needed for a typical *n*-level transform does not exceed 3, and that how many of the bit planes have been encrypted is also the same. Thus, the key space for this encryption is above 128.

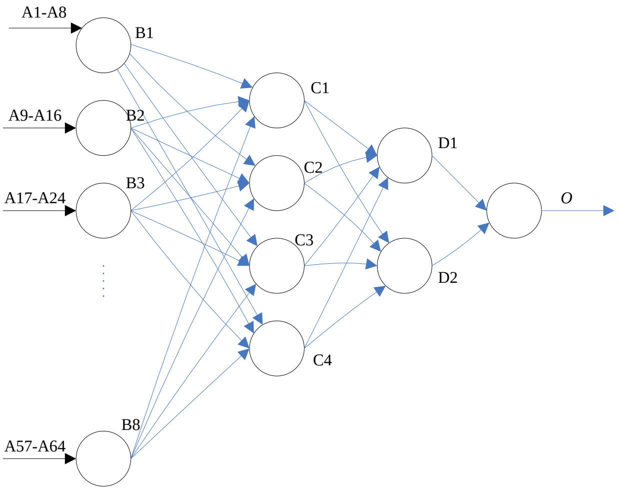

Figure 2. Generation of N-bit pseudorandom sequence for Chaos

0/1 Balancedness Test: In (Golomb, 1982), Golomb stated that the noise like sequence should look like an equality distribution, which means that the generated chaotic sequence should have equal number of 1's and 0's. In order to judge the proposed approach, a number of tests were run on the generator to produce the sequences of different length. These lengths were estimated to be 65536 (based on wavelet subband of size 256x256), 16384 (based on wavelet subband of size 128x128), 4096 (based on wavelet subband of size 64x64), and 1024 (based on wavelet subband of size 32x32). The results are shown in Table 1 and Figure 3, where it is clear that the numbers are quite close to 50%.

Table 1. Equality distribution within the chaotic sequence

Sequence length	Count of 1's	Percentage
1024	515	50.29
4096	2055	50.17
16384	8206	50.08
65536	32775	50.01

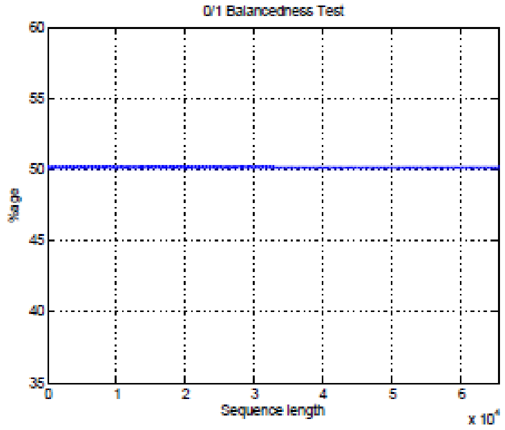

Figure 3. Percentage distribution of 1's in the sequence

Histogram Analysis: Generally, histogram of an image depicts pixel distribution density against intensity level. In order to test suitability of the proposed approach, 512x512 "Camera-man" image was deployed. The results are shown in Figure 4, where it can be clearly seen that histogram of the encrypted image is fairly uniform with statistical properties to those of the white noise. To investigate it further, standard deviations were also calculated and were found out to be 14.315 and 14.168 respectively, which is lower than in (Bigdeli, N., et al, 2012).

Correlation coefficient: This is a statistical parameter to measure quality of a good encryption. Theoretically, the autocorrelation function from the generated sequence should be a noise like impulse at the origin. For purposes of experimental analysis, this function was plotted using equations 1-5, and is shown in Figure 5, where good autocorrelation function can be seen clearly. The maximum value outside origin was observed to be 0.00215. In Table 2 is shown the correlation coefficient r_{xy} of batch of (x_i, y_i, for i=1, 2, 3….N) pairs of gray values of two adjacent pixels in various encrypted images. The correlation coefficient was calculated using the following equation (S. El Assad, et al, 2008):

$$r_{xy} = \frac{cov(x,y)}{\sqrt{d(x)}\,\sqrt{d(y)}}\ ;\ d(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N} xi\right)^2 \qquad (6)$$

where *cov* (*x*, *y*) stands for covariance between two pixels *x* and *y*. It is clear that pixels have been completely decorrelated due to encryption.

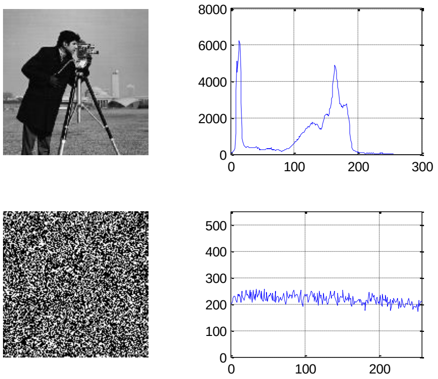

Figure 4. Histogram Analysis of proposed approach

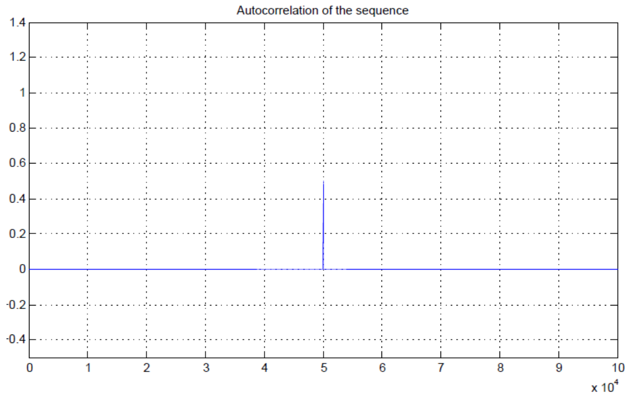

Figure 5. Correlation Function of the Sequence

Table 2. Correlation Coefficients of the original and encrypted images

Scheme	Image	Horizontal	Vertical	Diagonal
	Original Lena	0.9855	0.9881	0.9667
Proposed approach	Barbara	0.0009	-0.0011	0.00087
	Yacht	-0.000875	0.00071	-0.00084
	Lena	-0.00085	0.00084	0.00114

CONCLUSIONS

A JPEG2000 compatible block cipher was proposed in this paper with random key generated through 8-4-2-1 neural network, where hidden layers compute the output using repeated calculations in a cyclic manner to make it robust with increased complexity. During performance analysis, it was demonstrated that key space is more than 128. It should be clarified here that the key space can be extended up to 256 bits by adjusting neural network infrastructure. Furthermore, it was also demonstrated using 0/1balanceness, histogram and correlation analyses that the proposed encryption has robust performance.

REFERENCES

Bigdeli, N., Farid, Y., & Afshar, K (2012)., A Novel Image Encryption/Decryption Scheme based on Chaotic Neural Network, *Engineering Applications of Artificial Intelligence*, 25, 753-765

Bigdeli, N., Farid, Y., & Afshar, K.(2012), A Robust Hybrid Method for Image Encryption based on Hopfield Neural Network, *Computers and Electrical Engineering*, 38, 356-369.

Ilhem, D. & Amel, K. (2006), One-dimensional and two-dimensional dynamics of cubic maps. *Discrete Dynamics in Nature and Society*, Article ID: 15840, doi:10.1155/DDNS/2006/15840

Gao, T., & Chen, Z (2008). Image encryption based on a new total shuffling algorithm. *Chaos, Solitan, and Fractals*, 38(1), 213-220.

Lian, S. (2007), Image Authentication Based on Neural Network. Cornell University, CoRR abs/0707.4524.

Lian, S. (2009). A Block Chiper based on Chaotic Neural Networks. *Neurocomputing*, 72, 1296-1301.

Lian S., & Chen, X.(2011). Traceable Content Protection based on Chaos and Neural Networks. *Applied Soft Computing*, 11, 4293-4301

Joshi, S., Udupi, V., & Joshi, D.(2012). A Novel Neural Network Approach for Digital Image Data Encryption/Decryption. *Proceedings of IEEE International Conference on Power, Signals, Controls and Computation*, 1-4.

Memon, Q. (2014). On Integration of Error Concealment and Authentication in JPEG2000 Coded Images. *Advances in Image and Video Processing*, 2 (3), 26-42.

Memon, Q.(2006). A new approach to video Security over Networks. *International journal of Computer Applications in Technology*, 25 (1), 72-83.

Munukur, R., & Gnanam, V. (2009). Neural Network Based Decryption for Random Encryption Algorithms, *3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, 603-605.

Nguyen, T., & Marpe, D.(2014). Objective Performance Evaluation of the HEVC Main Still Picture Profile. *IEEE Transactions on Circuits and Systems for Video Technology*, 1-8., doi: 10.1109/TCSVT.2014.2358000

El Assad, S., Noura, H., & Taralova, I. (2008). Design and analyses of efficient chaotic generators for crypto systems, *Advances in Electrical and Electronics Engineering*, IAENG Special Edition of the World Congress on Engineering and Computer Science, 3–12.

Golomb, S. (1982). *Shift Register Sequences*, Revised Edition. Laguna Hills, CA: Aegean Park.