The International Journal of Engineering and Science (IJES)
|| Volume || 8 || Issue || 12 || Series I || Pages || PP 67-70|| 2019 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Image encryption using chaotic neural network

Sushil Kumar
Computer Science and engineering, Maharaja Surajmal institute of technology, New Delhi, India

----------***ABSTRACT***----------
The present work proposes the implementation of Wavelet based Chaotic Neural Network (WCNN) for image encryption. The neural network used is chaotic in nature i.e. its weights and bias will be determined by chaotic sequence with the help of 1-D logistic map. Private key system is achieved with the help of initial conditions. WCNN provides two level security along with the data compression to be transmitted. The image is first encrypted and then decrypted using WCNN. Encryption is carried out using only approximate coefficients, which reduces the transmitted data to a large extent. CNN is also applied for comparison purpose. The proposed methodology is applied on standard and real images. Further the behavior of system is verified with different key values at the receiver end and the proposed encryption scheme is proved to be keysensitive.
KEYWORDS: -*CNN, WCNN, Chaotic Cryptography.*

Date of Submission: 10-12-2019 Date of Acceptance: 29-12-2019

I. INTRODUCTION

A computer network has created a revolution in the field of communication. Internet enables millions of people to communicate. Confidential communication is common practice in the social life. However, as information communicated on shared network, it is exposed in public domain and may lead to undesirable results. The communicated information must be secured from public access, illegal changes and accessible to authorized users. The digital images can be secured by using [1] cryptography, steganography and watermarking. An approach to achieve confidential or secure communication is called cryptography. It is a technique for converting intelligible message to unintelligible forms. Steganography is a technique of hiding secret information whereas watermarking hides the proprietary information.

The image data has redundancy, large size and high correlation between pixels. Therefore conventional encryption methods can't be easily applied to images. The image encryption requires real-time processing, format consistency, and image compression. The real-time image processing is a challenging task as these requirements must be accomplished along with secured communication.

II. LITERATURESURVEY

Mitra A et al. [1] used bit, pixel and block permutations for combinational image encryption. The permutation of bits significantly reduces the correlation and therefore perceptual information is decreased, whereas the permutation of pixels and blocks achieve better security in comparison to bit permutation.Kede Ma et.al [2] used reversible data hiding for image encryption by reserving room. The proposed technique extracts the data and image is recovered without error i.e. real reversibility is achieved. The reversible data hiding with distributed source encoding is suggested by Zhenxing Qian et. al[3]. The proposed method proves to be better than the techniques available in literature. Ran Tao et.al [4] suggested multi-order fraction Fourier Transform based image encryption. The results show that image decryption is sensitive to transform order. Jiantao Zhou et. al[5] designed a prediction error clustering and random permutation based image encryption-then-compression system. The proposed approach is comparable to other techniques in terms of compression efficiency. Xinpeng Zhang et. al [6] proposed a scalable coding for encrypted images and the original image is successfullyreconstructed.

III. SYSTEM MODEL

A. ChaoticCryptography

Confusion and diffusion are two properties of the operation of a secure cipher which are discussed by Claude Shannon. Chaotic systems are deterministic and highly dependent on initial conditions and parameters. This implies that behavior of chaotic systems is modeled by mathematical equations. G. Jakimoski and L. Kocarev [7] suggested and analyzed chaos based cryptography using exponential and logistic chaotic maps. The technique is successfully applied on Feistel network.

B. Chaotic Neural Netwrok (CNN) based ImageEncryption

The chaos-based image encryption may be carried out in three ways i.e. pixel scrambling, pixel replacement and combination of scrambling and replacement. The image encryption process which is secret key encryption scheme is based on neural network is chaotic in nature because the weight and biases of network are adjusted according to the bit sequence generated by using 1-D logistic map. Encryption is implemented on pixel values of gray scale image using 1-D logistic map based on chaotic neural network. Parameter μ and x(0) of 1-D map is a secret key for implementing thescheme.

The steps of encryption process are discussed as follows:

Step (1) Input the grayscale image as 1-D signal and the length of signal is M.
Step (2) Set the initial parameters μ and x(0) of the 1-D map which act as secret key for the encryption.
Step (3) Run the logistic map from 1 to M to generate chaotic bit sequence
Step (4) adjust weights and biases of Neural Netwrok.
Step(5) obtain the 1-Dencrypted signal.
Step (6) Convert the 1-D encrypted to grayscale image as the encrypted image.
The decryption process is similar to encryption. The input to the decryption algorithm is the encrypted image.

C. Wavelet based Chaotic Neural Network (WCNN) image encryption

The CNN based encryption algorithm is modified to obtain two level security by incorporating the discrete wavelet transform.DWTisfirstappliedtopixelvaluesofgrayscale encryption at the transmission side. At the receiving end IDWT is applied to reconstruct theimage.

Step (1) Read the grayscale image as 1-D signal i.e., pixel values of image.
Step (2) Apply discrete wavelet transform.
Step (3) Find the length of signal obtained after DWT and set equal to M.
Step (4) Set the initial parameters μ and x(0) of the 1-D map which acts as secret key for the encryption.
Step (5) Run the logistic map from 1 to M to generate chaotic bit sequence.
Step (6) adjust weights and biases of Neural Netwrok.
Step (7) Obtain the 1-Dencrypted signal.
Step (8) Convert the 1-D encrypted to grayscale image as the encrypted image.
The decryption process is similar to encryption. The input to the decryption algorithm is the encrypted image.

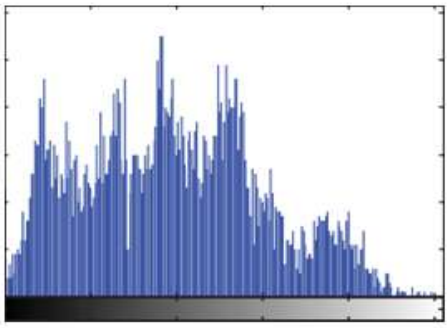
The decryption process is explained as follows:

1. Takeoutputof encryptionprocessas input and set its length is set equal toM.
2. Apply step of encryptionprocess.
3. Apply IDWT to reconstruct theimage.
4. In the decryption, image can also be reconstructed without applying IDWT to reduce the size of image by half.

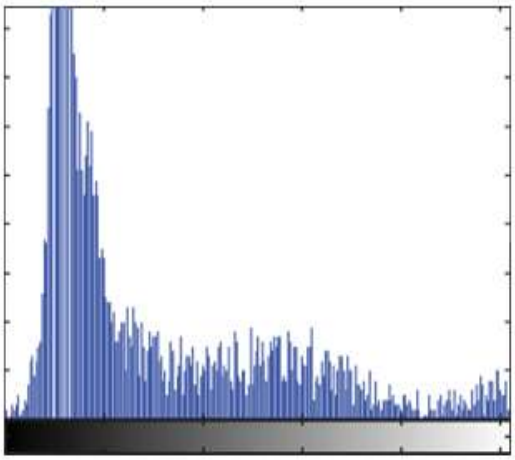
IV. RESULT AND DISCUSSION

A. CNN ImageEncryption

The encryption scheme is further extended to image encryption on two types of images i.e. standard and real time image. The input images are gray scale images of size 73×72 and 68×68 respectively. The images are encrypted using two combinations of key i.e. μ=0.75 and x(0)=3.9 and μ=0.72 and x(0)=3.7 and are used to analyze the difference incipher images encrypted with different keys. The correlation coefficient and histogram of both standard as well as real time image are also analyzed to study the difference in the results using combination of keys.



A. Standard Image and Histogtam



B. Real Time Image and Histogram

The correlation coefficients between plain and cipher images lie in the range -0.0204 to 0.0015. It is observed that correlation coefficients are extremely low and are near to zero, which indicates that encrypted images have no relation with the original images. The correlation coefficient between the encrypted images using different key combination is -0.0287 and 0.0093. The negative correlation coefficients clearly show that encryption scheme is key sensitive. Histograms of the images show that the proposed encryption algorithm provides acceptable confusion and diffusionproperties.

Further encrypted images are decrypted by using different keys and same key is used for encryption. The results of decryption are shown in Table1.

Table 1. Correlation coefficients of decrypted images using CNN

	x(0)=.72 μ=3.7	**x(0)=.75 μ=3.7**	**x(0)=.74 μ=3.9**	**x(0)=.75 μ=3.9**
Standard image	-0.0123	0.0177	5.19E-04	1
Real time image	-0.0277	-0.0222	-0.0204	1

B. WCNN based imageencryption

The modified encryption scheme is applied for image encryption on two types of gray scale images i.e. standard and real time image of size 73×72 and 68×68 respectively. The images are encrypted to analyze the difference in cipher images using two combinations of key i.e. μ=0.75 and x(0)=3.9 and μ=0.72 and x(0)=3.7. The standard and real time images are also recovered using the approximate coefficient to reduce the size of images after decryption. Histogram and correlation coefficients are also studied to evaluate the WCNN based imageencryption.

encrypted images lie in the range -0.0216 to -0.0082. The negative values of correlation coefficient (cc) show that similar show that similar images encrypted with different keys have no relation to each other. Similarly, the correlation coefficient of encrypted and original image lies in the range 0.0100 to 0.0246. The value of cc near to zero clearly indicates that encrypted images have no relation with the original images. Histograms of the images show that encryption of images is successfullyachieved.

Table 2. Correlation coefficient of decrypted images

	Decrypted images using CNN			
	x(0)=.72 μ=3.7	x(0)=.75 μ=3.7	x(0)=.74 μ=3.9	x(0)=.75 μ=3.9
Standard image	-0.0123	0.0177	5.19E-04	1
Real time image	-0.0277	-0.0222	-0.0204	1
	Decrypted images using WCNN			
	x(0)=.72 μ=3.7	x(0)=.75 μ=3.7	x(0)=.74 μ=3.9	x(0)=.75 μ=3.9
Standard image	-0.0109	-0.0059	-0.0155	0.9946
Real time image	-0.0043	0.0089	0.0259	0.9841

It is also observed that almost similar image to original image is recovered by decrypting the encrypted image using the same key as used for encryption. The similarity is verified with the help of cc and histogram. For differentcombination of keys the values of cc between original image and decrypted image lieintherange-0.01to0.02whereaswiththesamekeyccis 0.99 for standard and 0.89 for real time image. From the obtainedccitisobservedthatdifferentkeysyieldsdissimilar. images and similar images are obtained with same keys. Histogram of images and table 2 also verifies the similar observations. Therefore it is verified from the results that it is not possible to decrypt the image unless exact key combination and values are known. i.e., system is highly sensitive to initialconditions.

V. CONCLUSION

In the present work, two encryption schemes are implemented for image encryption i.e. CNN and WCNN. The proposed WCNN technique provides two level security using DWT and CNN. The case of CNN data transmitted remains the same as that of original image, whereas in WCNN approximate coefficients are required for encryption/decryption of the image. Therefore approximation coefficients are transmitted only and thus the size of the cipher image transmitted is reduced significantly. The correlation coefficient of plain image and cipher image shows that there is good confusion and diffusion property in both the algorithms. It is also observed that algorithms are key sensitive and thus secured. The correlation coefficient and histogram of both schemes clearly shows that WCNN is a better choice for image encryption.

REFERENCE

[1]. Mitra A., YV Subba Rao, and S. R. M. Prasanna. "A new image encryption approach using combinational permutation techniques." International Journal of Computer Science, vol. 1, pp. 127-131,2006.

[2]. Zhenxing Qian and Xinpeng Zhang, ‘‘Reversible Data Hiding in Encrypted Images With Distributed Source Encoding,’’ IEEE Transactions On Circuits And Systems For Video Technology, vol. 26, NO. 4, April2016.

[3]. Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li, “reversible data hiding in encrypted images by reserving room before encryption,” IEEE Transactions On Information Forensics And Security, vol. 8, no. 3, March2013.

[4]. Ran Tao, Xiang-Yi Meng, and Yue Wang, ‘‘Image Encryption WithMultiorders of Fractional Fourier Transforms,’’ IEEE Transactions On Information Forensics And Security, vol. 5, no. 4, December2010.

[5]. Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, ‘‘Designing an Efficient Image Encryption-Then- Compression System via Prediction Error Clustering and Random Permutation,’’ IEEE Transactions On Information Forensics And Security, vol. 9, no. 1, January 2014.

[6]. Xinpeng Zhang, Guorui Feng, Yanli Ren and Zhenxing Qian, “Scalable Coding of Encrypted Images,” IEEE transation on Image Processing, vol 21, no. 6, June2012

[7]. G. Jakimoski and L. Kocarev, “Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps”, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 48, pp. 163-169,2001.

Sushil Kumar "Image encryption using chaotic neural network" The International Journal of Engineering and Science (IJES), 8.12 (2019): 67-70.