Image Encryption Using Chaotic Cryptosystems and Artificial Neural Network Cryptosystems: A Review

Minal Chauhan[1], Rashmin Prajapati[2]
Department of CE, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Baroda, Gujarat, India
minal19ch@gmail.com[1], rashmin.1012@gmail.com[2]

Abstract: Cryptography is the exchange of information among the users without leakage or loses of information to others. Today the protection of multimedia type of data is becoming very important. Much public key cryptography algorithms are available which are based on number theory but it has the own drawback of large complexity, computational power, and time consumption and so they do not work well with image data. Chaotic systems are sensitive to initial conditions and system parameters. Noise like behaviour of chaotic systems is the main reason of using these systems in cryptology. The objective is to overcome these drawbacks and to analyse that the neural network is the best way to generate secret key. My survey research aims mainly at chaotic based and ANN based cryptosystems for the encryption of image data also to general information about image cryptography. I am going to list the all methods and highlight their similarities, their strength, relative Performance.

Keywords: Chaotic maps, Image encryption, Chaotic cryptosystems, Artificial neural network, Symmetric encryption;

I. Introduction

Information security is an increasingly important problem in the present era of advanced information technology, because of which encryption is becoming very important to ensure security. Popular application of multimedia technology and increasing transmission ability of network gradually lead us to acquire information directly and clearly through images. Image encryption has applications in Government, military, financial institution, hospitals and private business.

The digital images, which are transmitted over the internet, must be protected from unauthorized access during storage and transmission for communication, copyright protection and authentication purposes. This can be accomplished using

A suitable methodology for image encryption involves the use of cryptographic techniques.

This paper is organized as follows In Section 1; general guide line about cryptography is presented. In Section 2, survey on already existing research papers is presented. Finally, concluded in section 3.

A. What is Cryptography?

Cryptography is the science to transform the contents of information in secure mode. Encryption is converting the image to be transferred to cipher image which is an unintelligible image or data which cannot be understood by any third person. Encryption is used to assure security. Encr

yption is done using a key which is proposed in the encryption algorithm. In order to transmit secret images to other people, a variety of encryption schemes have been proposed to enhance the security of these images. At the receiver Side, key is used to decrypt the image.

B. What is Image Encryption?

Image encryption is an intelligent hiding of information. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. This cipher text can be saved or transmitted over the network. At the receiver, the cipher text can be transformed back into the original plaintext by using a decryption algorithm.

C. Why Image Encryption?

Images are a form of multimedia data. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons.

Table 1: Comparison of Text and Image Data

Parameters	Text	Image
Size	Generally KB to few MB	Comparatively much greater then text
Length of PT and CT	Must be same	Not necessary
Time to process data	Less time	More time

However second requirement is not essential for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

D. What is Chaotic Systems?

A Chaotic sequence is non-converging and non-periodic sequence that exhibits noise-like behaviour through its sensitive dependence on its initial condition. A large number of uncorrelated, random-like, yet deterministic and reproducible signals can be generated by changing initial value. These sequences so generated by chaotic systems are called chaotic sequences. Chaotic sequences are real valued sequences. This real valued sequence can be converted into integer valued sequence. This generated sequence makes it much effective for pixel permutation that can be used for image encryption. One of the simplest and most widely studied nonlinear dynamic systems capable of exhibiting chaos is the logistic map.

E. What is ANN?

A neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated

in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use. It resembles the brain in two respects:

- Knowledge is acquired by the network from its environment through a learning process.
- Interneuron connection strengths, known as synaptic weights, are used to store the acquired knowledge.

II. Literature survey

There are many algorithms to encrypt image data which I have described in this section:

Modified AES Based Algorithm for Image encryption, 2007

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki [3] studied the Advanced Encryption Standard (AES), and in their image encryption technique they have added a key stream generator to AES to ensure improving the encryption performance.

Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization, 2007

K.Deergha Rao and Ch. Gangadhar [4] studied the Chaotic-Key Based Algorithm (CKBA) algorithm which is susceptible to chosen/known-plaintext attacks and ciphertext-only attacks and they have proposed new modified Chaotic-Key Based Algorithm (MCKBA) which enhance the security of CKBA and it is achieved by increasing key sizes of CKBA and a nonlinear operation (mod operation) on the added value of image pixel and key in addition to the operations of the CKBA. They have also shown the cryptanalysis of MCKBA and their result shows that the security of MCKBA for known / chosen plaintext attack is very high as compared to CKBA.

Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm, 2008

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [5] have presented image encryption technique using the Hill cipher. They have generated self-invertible matrix for Hill Cipher algorithm. Using the key matrix they encrypted gray scale images and colour images. Their algorithm works well for all types of gray scale and colour images. For the images with background of same gray level or same colour the problem occurs.

Digital Image Encryption Algorithm Based on Chaos and Improved DES, 2009

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [6] have done their research work on the chaotic encryption, DES encryption and on the combination of image encryption algorithm. In their technique the new encryption scheme uses the logistic chaotic sequencer for making the pseudo-random sequence, carried over the RGB with this sequence to the image chaotically, and then it they have applied double time encryptions with improved DES. Their results have shown higher starting value sensitivity, higher security then DES and the higher encryption speed.

A Chaos-Based Data Encryption Algorithm for Image/Video, 2010

Min Long and Li Tan [7] have studied a chaos-based data encryption algorithm for image or media data. They have generated the encryption and decryption keys by using Chebyshev map, which confuses the plain-text with random input keys. Then Logistic map were used to confuse the plain-text and then Nonlinear Chaotic Algorithm (NCA) were used to shuffle the position of the plain text. The initial conditions and parameters of chaotic system are obtained by confusion of the random input keys and plain-text. Their cryptanalysis shows the results of the key space analysis, key sensitivity tests, information entropy analysis, statistical analysis, and plaintext sensitivity analysis, and those analysis shows that the proposed encryption algorithm possesses high security.

Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), 2010-2011

Hiral Rathod, Mahendra Singh Sisodia and Sanjay Kumar Sharma [8] have researched on a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called Hyper Image Encryption Algorithm (HIEA). The proposed encryption algorithm works on the image of type .bmp or .jpeg. With the image of size minimum 256 the binary value of the image is obtained and then divided in the blocks. Each block is of size 256 bits. 256 bit key block is divided in 1+-6 sub blocks of 16 bits each. From transformation table 64 bits are taken and 4 blocks of 16 bits are created. Then the X-OR operation is applied in first 8 block of image and the key. Apply the X-OR between last 4 block of image and the transformation table. Apply the circular shift in last 4 blocks of the key and the image. Apply the X-OR between this output and key. Apply Circular Shift Operation on 4 blocks of transformation table and key. Apply logical XOR operation between transformation table and selected key. Combine the above outputs to produce 256 bit which is an input to next round.

Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it, 2011

Kuldeep Singh and Komalpreet Kaur [9] have compared the results of four chaotic maps Cross chaotic, Logistic, Ikeda and Henon map and the effects of noise were observed on image type of data. In their research they have used the image encryption algorithm to convert original image to encrypted image and they have applied noise on the encrypted image and then decrypt cipher image with noise back to original image. Their results have shown that cross chaotic map shows the best results than other three chaotic maps.

Image Encryption Based on the General Approach for Multiple Chaotic Systems, 2011

Qais H. Alsafasfeh and Aouda A. Arfoa [10] have proposed a new image encryption technique based on new chaotic system by combining the two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. From Experimental analysis they have shown that the image encryption algorithm has the advantages, over using only single

chaotic system for image data, of large key space and high-level security, high obscure level and high speed.

An Adaptive Neural Network Guided Secret Key based Encryption through Recursive Positional Modulo-2 Substitution for Online Wireless Communication (ANNRPMS), 2011

J. K. Mandal and Arindam Sarkar [11] have proposed a neural network guided secret key based technique for encryption (ANNRPMS). They have used recursive positional modulo-2 substitution. Both networks receive an indistinguishable input vector, produce an output bit and were trained based on the output bit. The dynamics of the two networks and their weight vectors were used, where the networks synchronize to an identical time dependent weight vectors. Based on this fact the length secret-key using a public channel was decided. The length of the key depends on the number of input and output neurons. The original plain text was encrypted using recursive positional modulo-2 substitution technique and secret key also generated through encryption process in a cascaded manner. This intermediate cipher text was again encrypted to form the final cipher text by chaining and cascaded x-oring of identical weight vector with the identical length intermediate cipher text block. If the size of the last block of intermediate cipher text is less than the size of the key then this block kept unchanged. Then at receiver end the receiver will use identical weight vector for getting the recursive positional modulo-2 substitution encrypted cipher text and secret key for decoding for performing deciphering process.

Image Encryption Based on Diffusion and Multiple Chaotic Maps, 2011

G.A.Sathishkumar, Dr.K.Bhoopathy bagan and Dr.N.Sriraam [12] researchers have explained a new algorithm for the image encryption/decryption scheme, to provide a secured image encryption technique using multiple chaotic based circular mapping. The procedure overview: first, a pair of sub keys is given by using chaotic logistic maps. Second, the image is encrypted using logistic map sub key and in its transformation leads to diffusion process. Third, sub keys are generated by four different chaotic maps. Based on the initial conditions, each map may produce various random numbers from various orbits of the maps. Among those random numbers, a particular number and from a particular orbit are selected as a key for the encryption algorithm. Based on the key, a binary sequence is generated to control the encryption algorithm. The input image of 2-D is transformed into a 1- D array by using two different scanning pattern (raster and Zigzag) and then divided into various sub blocks. Then the position permutation and value permutation is applied to each binary matrix based on multiple chaos maps. Finally the receiver uses the same sub keys to decrypt the encrypted images.

Cryptography Based on Neural Network, 2012

Eva Volna, Martin Kotyrba, Vaclav Kocian and Michal Janosek [13] have done their research on using neural network in cryptography for designing a neural network that would be practically used in the area of cryptography. They have used the neural network to design the topology, to design the method of training algorithm and to design the training set for training. They have generated messages (plain text) that were encrypted via the first adapted neural network. Then we have received some cipher text, which represented some input into the decryption process carried out via the second adapted neural network. Each obtained cipher text was compared with the original message after its pre processing. Their results shows that the neural network works reliably and absolutely no errors are found in the outputs during encryption and the neural network also works reliably during the decryption process, which is the reverse of the encryption process.

III. Conclusions

In this paper, I have survey the different encryption techniques and algorithms for image data. Most of the traditional encryption algorithms are designed for textual data may not be suitable for multimedia data.

Now based on the different issues associated image encryption I have conducted the comparison between the ranges of approaches concluded in the form of table.

Table 2: Comparison of Conventional, Chaotic Based and ANN Based Cryptosystems

Approach	Technique	Advantage	Disadvantage
Image encryption	Symmetric key encryption	Algorithm for the image encryption/ decryption scheme, to provide a secured image encryption technique	Large computational power, complexity and time consumption during generation of key, for sensitive digital images and videos naive encryption doesn't work properly
Chaotic based Cryptology	Multiple chaotic maps	Loss-less, good peak signal to noise ratio (PSNR)	The major weakness is fewness of system parameters
ANN based cryptosystems	Sequential, BPN etc	It appears to be exceedingly difficult to break without knowledge of the method-logy behind it	effective secret-key system, with the key being the weights and architecture of the network

Although not mentioned in this paper, there have been number of approaches in Image encryption in the context of neural networks, chaotic systems, using genetic algorithms and many more. The goal of these techniques which have been described is related to provide higher security and speed and so the cryptosystem should be chosen appropriately.

REFERENCES

[1] William Stallings, "Cryptography and Network Security: Principles and Practices", second edition.

[2] Aloha Sinha, Kehar Singh, "A Technique for Image Encryption using Digital Signature", Optics Communications, Vol.2 No.8 (2203), 229-234.

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27 2007.

[4] K.Deergha Rao, Ch. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization", IEEE, 15th International. Conference on Digital Signal Processing (DSP), 2007.

[5] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jen, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[6] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES", IEEE International Conference on Systems, Man and Cybernetics, 2009.

[7] Min Long, Li Tan, "A chaos-Based Data Encryption Algorithm for Image/Video", IEEE, Second International Conference on Multimedia and Information Technology, 2010.

[8] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)" International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, No.3 (2010/2011).

[9] Kuldeep Singh, Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications (0975 - 8887) Vol.23, No.6, June 2011.

[10] Qais H. Alsafasfeh, Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

[11] J. K. Mandal, Arindam Sarkar, "An Adaptive Neural Network Guided Secret Key based Encryption through Recursive Positional Modulo-2 Substitution for Online Wireless Communication (ANNRPMS)", IEEE, International Conference on Recent Trends in Information Technology (ICRTIT), June 2011.

[12] G.A.Sathishkumar, Dr.K.Bhoopathy bagan and Dr.N.Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[13] Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, "Cryptography Based on Neural Network", 26th European Conference on Modelling and Simulation, 2012.

[14] Sesha Pallavi Indrakanti, P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Vol.28, No.8, 2011.