Neural Network Based Secured Transmission of Medical Images with Burrow's - Wheeler Transform

M. Ramakrishnan[1], R. Sujatha[2]

[1] Professor and Head, Department of Computer Science, Madurai Kamarajar University, Madurai, India.
ramkrishod@gmail.com
[2]Assistant Professor, Department of Electronics and Communication Engineering, Velammal Engineering College,
Anna University, Chennai, India.
ece.sujatha@velammal.edu.in

ABSTRACT

Cryptography is basically essential for protecting sensitive information as the importance of security and the privacy of it has become crucial in this electronic world with the advent of online transaction and processing e-commerce. Nowadays security of digital images is a major area of concern, especially when we deal with medical images where it may be stored or sent through insecure communication channels. In this paper we propose to make use of neural networks which has fewer overheads and also requires fewer computations. The key used here is complex so that undesirable sources will not be able to access it. Thereby we generate the key using neural network. Using the encryption algorithm such as blowfish, we encrypt the image. The encrypted image is compressed with the help of burrow's-wheeler transform which is a lossless compression. And then this compressed secured information is successfully transmitted. In this paper we obtain the results by simulation using MATLAB.

Keywords — Cryptography, Neural network, Blowfish Algorithm, Burrow's-Wheeler Transform

1. INTRODUCTION

In the past few years, the security and integrity of data is the main concern. In the present scenario, almost all the data is transferred over computer networks due to which it is vulnerable to various kinds of attacks. To make the data secure from various attacks and for the integrity of data, we must generate key from neural network and then encrypt the data before it is transmitted or stored. If these confidential images about the patient fall into wrong hands then such breach of security could lead to wrong treatment. Protecting confidential images is an ethical and legal requirement. Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. To encrypt the data we make use of Blowfish algorithm. The blowfish algorithm is symmetric since the same secret key is used for both encryption and decryption of the medical images. The secret key effectively doubles the strength of the algorithm.

After encryption, we make use of Burrow's-wheeler transform which is used to reduce the size of the image. Then we decompress the image to obtain the mean square error and peak signal to noise ratio. This transformation is efficient because it is reversible and no need to store additional data. It also reduces the memory requirement and it is considered to be fast and efficient.

2. KEY GENERATION

2.1 Neural network:

Neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is usually implemented by using electronic components or is simulated in software on a digital computer. Neural network is a massively parallel distributed processor made up of simple processing units which has a natural propensity of storing exponential knowledge and making it available for use. It resembles brain in two aspects; one is that knowledge is acquired by the network from its environment through a network learning process, the other is the inter neuron connection strengths, known as synaptic weights are used to store the acquired knowledge. The basic elements of a neural network are: 1. A set of synapses or connecting links each of which is characterized by weight of its own, 2.Adder is used for summing the input signal weighted by their respective synapses, 3. An activation function for limiting the amplitude of output of neuron. Neural network also has external applied bias that has the effect of increasing or lowering the net input of the activation function. In our paper we make use of single layer feed-forward network. Here we have input layer of the source node that projects on to an output layer of neuron, but not vice-versa. Also we do not have any hidden layers here. Now from this neural network we are going to generate the key that will be used for blowfish encryption.

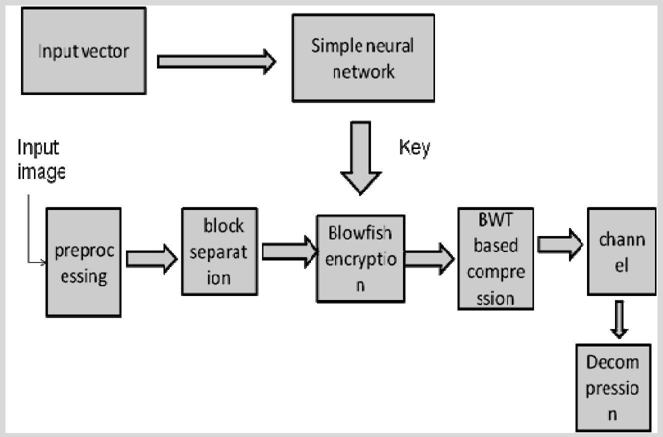

Figure 1: Overall Block Diagram

1.2 Generating the key:

First for obtaining the key, we generate a sample neural network. Generating a sample neural network involves initializing input vectors, weights, bias and output elements. P array has 18 values .So we go in for an iteration process, in order to generate 18 values. During the iteration process neural network is simulated. As a result keys get generated for blowfish encryption.

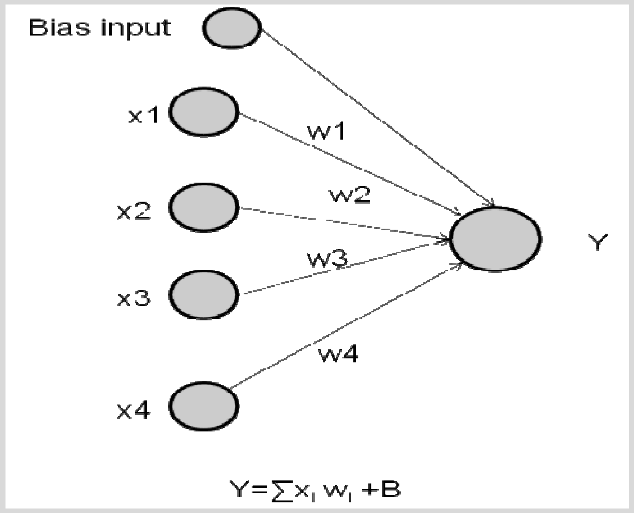

Figure 2: A simple feed-forward neural network

3. ENCRYPTION ALGORITHM

3.1 Blowfish Algorithm:

A symmetric 64-bit block cipher invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in over 80 products.

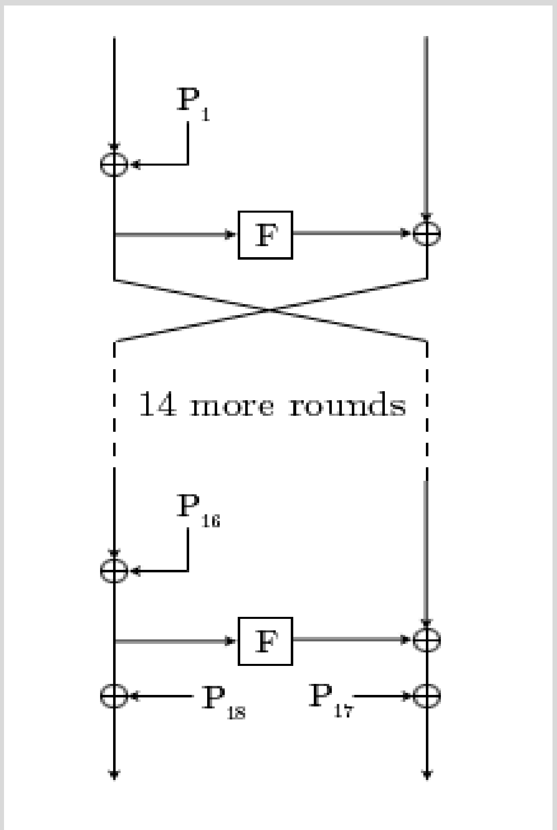

Figure 3: Flow of Encryption

Fig 3 shows the block diagram of an algorithm with the Feistel structure for encryption, with 16 rounds of confusion and diffusion.

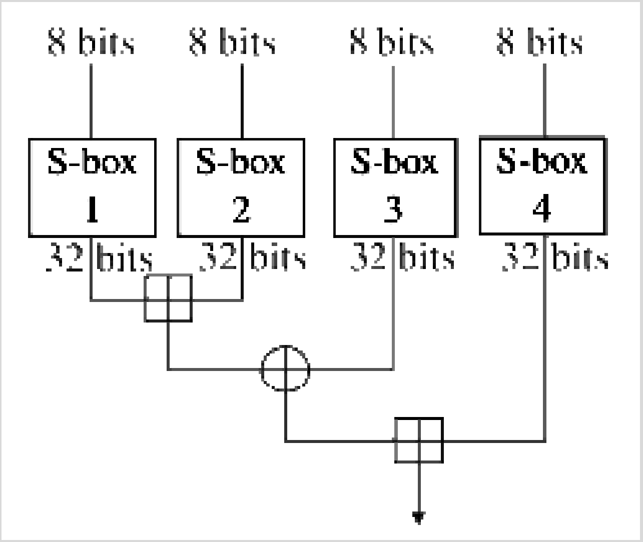

Figure 4: Feistel function

Fig 4 is considered as a primary source of algorithm security. It combines two simple function namely addition modulo 2 (XOR) and addition modulo 232.

```
Blowfish has 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18.
Finally, recombine xL and xR to get the ciphertext
```

4. COMPRESSION

In computer science and information theory, data compression or source coding is the process of encoding information using fewer bits (or other information-bearing units) than a unencoded representation would use, through use of specific encoding schemes.

Another concept related to compression is that of Data deduplication. In computing, data deduplication is a specialized data compression technique for eliminating coarse-grained redundant data, typically to improve storage utilization.

Lossless compression algorithms usually exploit statistical redundancy in such a way as to represent the sender's data more concisely without error. Lossless compression is possible because most real-world data has statistical redundancy.

4.1 Burrows Wheeler Transform

The Burrows–Wheeler transform (BWT, also called block-sorting compression) rearranges a character string into runs of similar characters. This is useful for compression, since it tends to be easy to compress a string that has runs of repeated characters by techniques such as move-to-front transform and run-length encoding. More importantly, the transformation is reversible, without needing to store any additional data. The BWT is thus a "free" method of improving the efficiency of text compression algorithms, costing only some extra computation.

The Burrows–Wheeler transform is an algorithm used in data compression techniques such as bzip2. It was invented by Michael Burrows and David Wheeler in 1994 while working at DEC Systems Research Center in Palo Alto, California. It is based on a previously unpublished transformation discovered by Wheeler in 1983.

When a character string is transformed by the BWT, none of its characters change value. The transformation permutes the order of the characters. If the original string had several substrings that occurred often, then the transformed string will have several places where a single character is repeated multiple times in a row. The transform is done by sorting all rotations of text in lexicographic order , then taking the last column. In our paper the encrypted image is subjected to BWT compression. Initially the image is resized, then converted into string s. The strings undergo cyclic shifts to form a matrix. This matrix is then arranged in lexicographic order. After this process we obtain the compressed image. The reverse process is used to obtain the decompressed image.

The decompression is done to obtain parameters namely mean square error and peak signal to noise ratio.

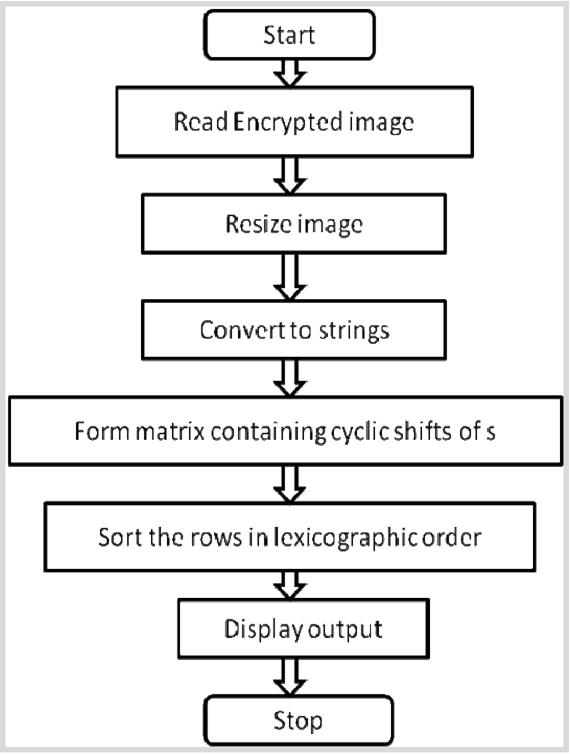
Start
Read Encrypted image
Resize image
Convert to strings
Form matrix containing cyclic shifts of s
Sort the rows in lexicographic order
Display output
Stop

Figure 5: Burrow's Wheeler Transform

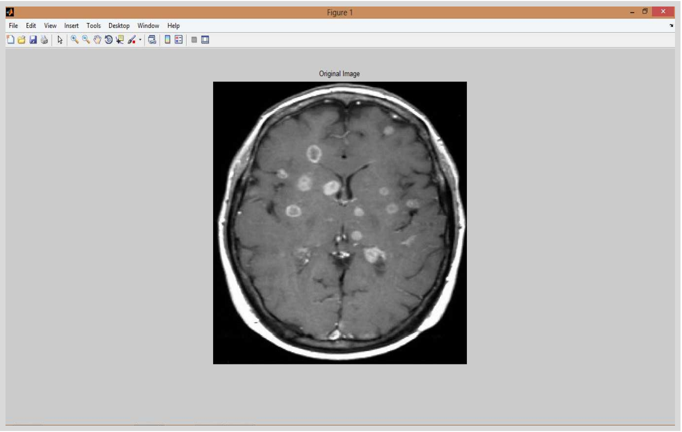

Figure 6: Original image

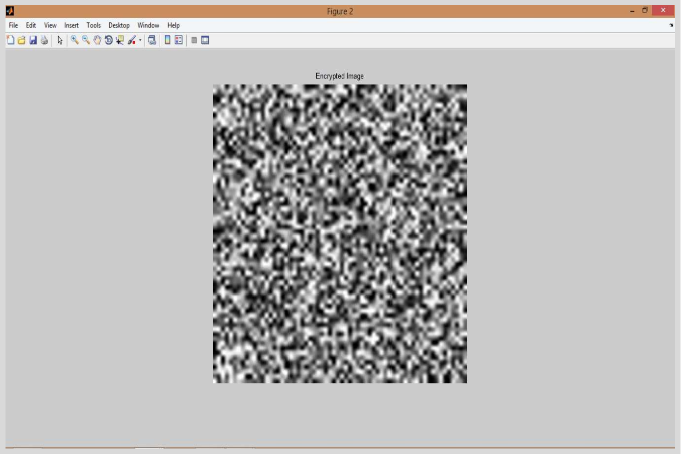

Figure 7: Encrypted image

5. CONCLUSIONS

In this paper we have proposed a new scheme of encrypting the medical images by the use of blowfish algorithm by generation of key from the neural networks. The blowfish algorithm is a form of symmetric key cryptography. By the usage of neural networks we achieve greater measure of parallelism which reduces computational speed and increases the complexity. By increasing the complexity we thus achieve greater security for the images. The encrypted image is then compressed by the use of a lossless compression technique to save the bandwidth of the transmission channel.

ACKNOWLEDGMENT

The authors would like to thank our supervisor Dr. M. Ramakrishnan for his input during this work, and the anonymous reviewers whose comments helped us to improve the work.

REFERENCES

[1] Pia Singh, and Karamjeet Singh, "Image Encryption and Decryption using Blowfish Algorithm in Mat lab.", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[2] Irfan Landge, Burhanuddin Contractor, Aamna Patel, and Rozina Choudhary, "Image encryption and decryption using blowfish algorithm", World Journal of Science and Technology, Volume 2, Issue 3, April-2012.

[3] N. Prabakaran , P. Saravanan and P. Vivekanandan, "A New Technique on Neural Cryptography", International Journal of Soft Computing, Medwell Journals, Volume 3, Issue 5, 2008.

[4] Singhal, Nidhi and Raina, J P S, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, Aug - 2011.

[5] Nadeem and Aamer, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[6] Bruce Schneier, "The Blowfish Encryption Algorithm Retrieved", October 25, 2008, http:// www. schneier.com/ blowfish.html.

[7] W. Lee, T. Chen and C. Chieh Lee, “Improvement of an encryption scheme for binary images”, Pakistan Journal of Information and Technology.

[8] H. Cheng and X.B. Li, “Partial encryption of compressed image and videos”, IEEE Trans. Signal Process. 48 (8) (2000).

[9] M. Ali BaniYounes and A. Jantan, “Image encryption using block-based transformation algorithm,in IAENG”, International Journal of Computer Science.

[10] Atul, Kahate, “Cryptography and Network Security”, (Second Edition 2008).

[11] Li. Shujun, X. Zheng, “Cryptanalysis of a chaotic image encryption method”, Inst. of Image Process. Xi'anvJiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002.

[12] P. Dang and P. M. Chau, “Image Encryption for Secure Internet Multimedia Applications”, IEEE Transactions on Consumer Electronics, voI.46,no.3,pp.395-403, Aug.2000.

[13] Ketu File, “Symmetric vs Asymmetric Encryption”, a division of Midwest Research Corporation, white papers.

[14] Tingyuan Nie and Teng Zhang, “A Study of DES and Blowfish Encryption Algorithm”, IEEE, 2009.

[15] Ozturk and I.Sogukpinar, “Analysis and comparison of image encryption algorithm”, Journal of transactions on engineering, computing and technology December, vol. 3, 2004.