International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 01 Issue 09
October 2015

New Cryptography Based Compression Method using Blowfish and Neural Network

Rupinder Kaur ; Er.Rajat Tiwari

[1] *Student M.Tech Department of ECE;* [2]*Assistant professor , Department of ECE*

Chandigarh University Gharuan, Mohali, Punjab, INDIA 140413

email: roop.badwal@gmail.com ; email: er.rajattiwari@gmail.com

Abstract- *One of many major challenges associated with resource sharing with data communication network is actually their safety measures. That is premised with the belief that as soon as there's connection among personal computers sharing some resources, the problem associated with data security becomes important. The actual large progress within the networking technologies qualified prospects perhaps the most common culture intended for interchanging in the electronic digital photos really drastically. Hence it is a lot more prone associated with duplicating associated with electronic digital image and also redistributed by cyber-terrorist. Which means photos must be protected although transmitting it, vulnerable data such as credit cards, consumer banking purchases and also social safety numbers need to be protected. So to solve this problem, proposed work will be implemented on the usage of blowfish algorithm with neural network for image encryption as well as image compression in MATLAB environment*

Index Terms- *Image Encryption, Compression, Neural Network, Blowfish.*

I. INTRODUCTION

Cryptography is actually participating in a major purpose throughout data protection throughout applications managing inside a network environment. The idea enables individuals to ply their trade in an electronic form without having problems associated with deceit and also lies besides guaranteeing this sincerity in the information and also authenticity in the sender [3].

They have be a little more important to our day-to-day lifestyle simply because 1000s of folks have interaction in an electronic form every day; through e-mail, e-commerce, ATM equipment, cell phones, and so forth. This particular geometric increase associated with data carried in an electronic form has produced elevated reliability with cryptography and also authentication by consumers [4]. Although secured connection has been around since then, the key supervision issue has averted that coming from popular software. The actual development associated with public-key cryptography has allowed large-scale circle associated with network of users that may communicate safely with one another even when that they never communicated before.

A. Image Encryption

Image encryption plans have been progressively contemplated to take care of the demand for continuous secure image transmission over the Internet and through wireless systems. Encryption is the procedure of changing the data for its security [1]. With the tremendous development of PC systems and the most recent advances in computerized innovations, an immense measure of advanced information is being traded over different sorts of systems. It is frequently genuine that a substantial piece of this data is either classified or private. The security of images has turn out to be more imperative because of the quick advancement of the web on the planet today. The security of images has pulled in more consideration as of late, and a wide range of image encryption techniques have been proposed to upgrade the security of these images. Image encryption procedures attempt to change over a image to another that is difficult to get it. Then again, image decrypts the first image from the encoded one. Encryption is the procedure of encoding plain instant message into cipher text message though turn around procedure of changing cipher content to plain content is called as decryption [2].

B. Compression

Image compression is a process that intend to compact representation of an image by reducing the image storage or transmission requirements. The goal of image compression is to reduce the image file size without affecting the quality of an image. The term data compression refers to the process of reducing the amount of data requirement to represent a given quantity of information. In this definition, data and information is not the same thing; data means by which information is conveyed [5]. Because various amounts of data can be used to represent the same amount of information and representations that contain repeated or irrelevant information are said to contain redundant data. Let *b* and *b'* denote the number of bits in two representations of the same information,

International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 01 Issue 09
October 2015

the relative data redundancy *R* of the representation with *b* bits is

R = 1-1/C

In this paper cryptography uses to enhance the security in compression technique using Blowfish algorithm. It takes too less time to encrypt the file with Cryptography Mechanism [6].

III.PROPOSED METHOD

In this research there is combination of Blowfish encryption Algorithm to provide the Security of our data from unauthorized users and with the advantage of fast mechanism to encrypt the File in addition with neural network compression [7]. This Mechanism is more secure, robust and fast than AES and RSA mechanism. So there is implementation of this mechanism with compression to achieve better results from previous Research.

IV. METHODOLOGY

Below figure describes the steps to achieve proposed results using blowfish and neural network.

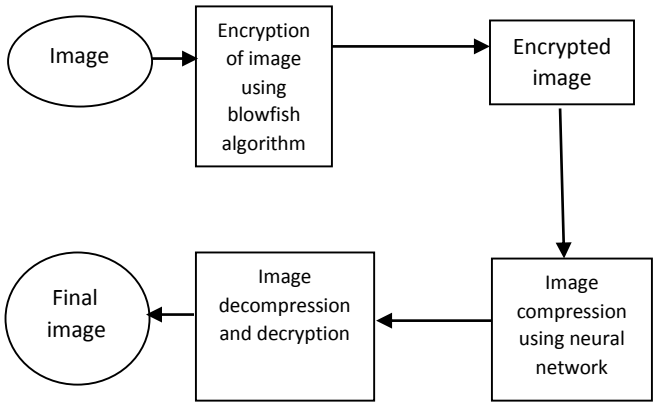

Figure.1 Methodology of proposed work

B. Input Image

At First window is browsed and image file is picked up and therefore loaded in the database where compression and encryption two different mechanism takes place in single way [8,9].

Figure 2. Input image

C. Encryption using Blowfish

Then implementation of basic encryption algorithm takes place which would encrypt the image file.

Figure1. Encrypted Image

Above figure describes the encrypted image using Blowfish algorithm.

D. Training using Neural Network

The Back Propagation neural network is artificial neural network based on error back propagation algorithm [10]. The Back Propagation (BP) neural network model consists of an input layer, more or less hidden layers as well as an output layer. Each connection connecting neurons has a distinctive weighting value.

In training the network, the nodes in the BP neural network obtain input information from exterior sources, and then go by to hidden layer which is an interior information processing layer and is answerable for the information conversion, and then the nodes in the output layer supply the required output information.

After that, the back-propagation of error is transported by distinct the actual output with wanted output. Each weight is revised and back propagated layer by layer from output layer to hidden layer and input layer.

This process will be continued until the output error of network is reduced to an acceptable level or the predetermined time of learning is achieved. The processing results of information are exported by output layers to the outside [11].

The process of BPNN training has been described below:

```
[training_rows_total,cols]=size(new_image);
training_rows=round(training_rows_total*70/100);
```

International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 01 Issue 09
October 2015

```
training_data(1:training_rows,:)=new_image(1:training_rows
,:);
for i=1:training_rows
Target(i)=i;
end
net=newff(training_data',Target,10);
net.trainParam.epochs=50;
net=train(net,training_data',Target);
```

This leads to initialization of the neural network and the compression process is performed.

E. Compression

Figure 3. Compressed Image

Above figure describes the compressed image using Blowfish algorithm and neural network.

F. Decompression

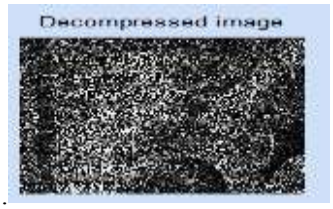

Figure 4. De- Compressed Image

Above figure describes the de-compressed image using Blowfish algorithm and neural network.

G. Decryption

Figure 5. Decrypted Image

Above figure describes the decrypted image using Blowfish algorithm and neural network.

V. RESULTS AND IMPLEMENTATION

The Research is carried on different size of image files with purposed algorithm which include Blowfish and neural network [12].

*A. Performance parameter and calculation: 1) PSNR :*The results are taken in matlab programming. The PSNR and MSE values are calculated using equation (1) and (2) The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

2) MSE

The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where M and N are the number of rows and columns in the input images, respectively.

3) CR

Image compression ratio is the division of uncompressed size file to compressed file size.

$$\text{CR} = \frac{\text{Uncomprssed image size}}{\text{Compressed image size}}$$

Table I
Comparison with AES-SS work

Images	METHOD	PSNR	CR

International Journal of Research
Available at http://internationaljournalofresearch.org/
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 01 Issue 09
October 2015

LEENA	**AES-SS**	**27.90**	**0.415**
	BF-NN	**27.7**	**0.647**
BOAT	**AES-SS**	**25.29**	**0.437**
	BF-NN	**27.92**	**0.632**
BABOON	**AES-SS**	**18.73**	**0.439**
	BF-NN	**27.81**	**0.523**
BARBARA	**AES-SS**	**21.69**	**0.445**
	BF-NN	**28.0**	**0.590**
GODHILL	**AES-SS**	**25.80**	**0.429**
	BF-NN	**28.0**	**0.541**
MAN	**AES-SS**	**25.29**	**0.437**
	BF-NN	**27.97**	**0.589**
PEPPERS	**AES-SS**	**26.02**	**0.427**
	BF-NN	**27.92**	**0.562**

Above table and below figure describes the evaluated values of PSNR, MSE, CR and Bits per Pixel for proposed algorithm for compression process, de-compression process and Decryption process.

B. Performance parameters and comparison

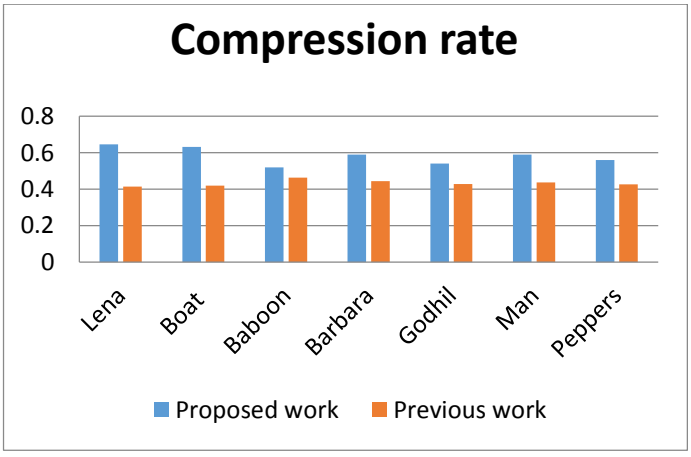

Figure 5. Comparison of compression ratio

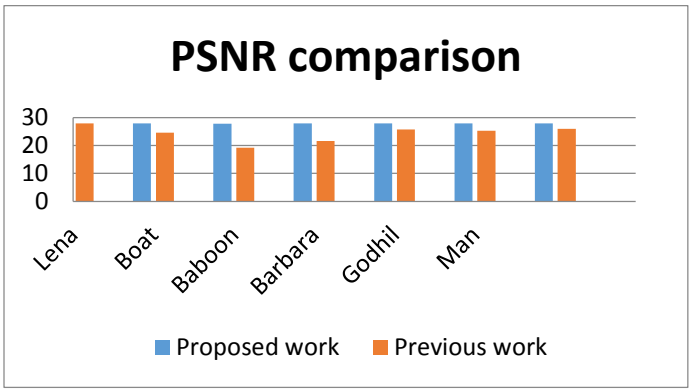

Figure 6. Comparison of PSNR values

VI CONCLUSION AND FUTURE SCOPE

In many practical scenarios such as cloud computing, the parties who process the encrypted data are often untrusted, and hence have no access to the secret key. This has led to the challenging problem of how to achieve superior efficiency of processing the encrypted data with zero knowledge of the secret. As one of the most common operations on multimedia data, multimedia compression over encrypted domain has received increasing attention since the last decade
In this paper, we have presented an image compression and encryption method based on blowfish and neural network machine learning algorithm. The whole simulation has been taken place in MATLAB 7.10 with good performance results.

ACKNOWLEDGEMENT

The authors would like to thank the Assistance Prof. Rajat Tiwari for their helpful comments and suggestions.

REFERENCES

1. Xianghong and L. Yang. "An Image Compressing Algorithm Based on Classified Blocks with BP Neural Networks," Proc. of the international conference on computer science and software engineering, IEEE Computer Society, Wuhan, Hubei, vol. 4, Dec 2008, pp.819-822, ISBN: 978-0-7695-3336-0, DOI: 10.1109/CSSE.2008.1357.
2. Fatima B. Ibrahim. "Image Compression using Multilayer Feed Forward Artificial Neural Network and DCT," Journal of Applied Sciences Research,

vol.6, no.10, 2010, pp. 1554-1560, INSInet Publication.

3. O. N. A.AL-Allaf. "Improving the Performance of Backpropagation Neural Network Algorithm for Image Compression/Decompression System," Journal of Computer Science, DOI: 10.3844/jcssp.2010.1347.1354, vol.6, Issue.11, 2010, pp. 1347-1354,
4. M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
5. D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf. Commun., Control, Comput., 2005, pp. 1–10.
6. D. Schonberg, S. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.
7. A.A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. 10th Workshop MMSP, Oct. 2008, pp. 760–764.
8. W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
9. D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.
10. A. A. Kumar and A. Makur, "Lossy compression of encrypted image by compressive sensing technique," in Proc. IEEE Region 10th Conf., Jan. 2009, pp. 1–6.
11. X. Zhang, Y. Ren, G. Feng, and Z. Qian, "Compressing encrypted image using compressive sensing," in Proc. 7th IEEE Int. Conf. IIH-MSP, Oct. 2011, pp. 222–2225.
12. X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Image Process., vol. 21, no. 6, pp. 3108–3114, Jun. 2012.