Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BANN: A NOVEL INTEGRATION OF SECURITY WITH EFFICIENCY USING BLOWFISH AND ARTIFICIAL NEURAL NETWORKS ON CLOUD

[1] JOHN JEYA SINGH.T, [2] DR E.BABURAJ

[1] Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India.

[2] Professor and Head, Department of Computer Science & Engineering, SUN Engineering College, Nagercoil, Tamilnadu, India

E-mail: [1]johnjsingh_2001@yahoo.co.in , [2] alanchybabu@gmail.com

ABSTRACT

Multimedia data security and storage space allocation on cloud servers is a matter of concern for many CSPs and also has a vast scope for research. Media files generally are encrypted and stored on storage servers due to various security threats. Though recent advancements are in mass storage density of servers and high speed processors have provided a little relaxation to CSPs but still with their limited storage capacity and heavy usage of services by users globally, these storage servers usually pave way for high memory allocations for media files resulting in lack of server space. We argue that uncompressed media such as images take more storage space compared to compressed files and also consume more time for cipher operations, which results in poor performance and considerably high bandwidth usage for operations. We propose a combination of **B**lowfish encryption algorithm with **A**rtificial **N**eural **N**etworks (BANN) to provide an efficient way to store and process media files on servers. We have evaluated the performance of proposed work and compared it in terms of PSNR, compression ratio, mean square error, average difference, maximum difference and normalized absolute error and time efficiency during cipher operations. Through these experimental results we prove the efficiency of system which increases dramatically using BANN technique.

Keywords: *Cloud Computing, Cloud Storing, Cloud Retrieval, Neural Networks, Compression.*

1. INTRODUCTION

Day by day, use of multimedia, image and videos is expanding globally for various applications such as video conference, HDTV, medical imaging etc. [1] Digital images carry significant information (redundant information also included) which is very useful for visual perception for users [2]. Cloud systems provide infrastructure to store and retrieve user data with ease of accessibility. It facilitates remote access to the data with global accessibility but this increasing demand of data communication for imaging system requires enormous storage capacity to store information [3]. During transmission, huge size of image or multimedia data requires more bandwidth and power consumption which is a challenging task for researchers [4]. While the storage capacity of cloud systems is undoubtedly huge the storage cost involved in it increases burden for server administrators and its users.

To overcome these issues, various data compression approaches have been introduced. Cloud servers definitely get benefit of less storage consumption by compression schemes, rather than storing similar amount of files which are uncompressed. The methods for data compression are classified into two main categories: (i) Lossless compression method and (ii) Lossy compression method [5]. Efficiency in cloud storage capacity can be achieved with data compression techniques such as DCT, DWT and fractal coding schemes. T. M. Quan et al. [6] presented a new scheme for image processing using GPU based on DWT implementation. In this method a hybrid approach is introduced which boosts the performance. Moreover, Haar DWT is developed with the help of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mixed band memory layout to achieve multilevel transform by applying fusion of a single kernel. Based on discreet cosine transform (DCT), image compression method is presented [7]. This method is implemented for endoscopy image compression. In this approach YEF is used for color space representation which requires less number of addition and multiplication. This approach results in low complexity and higher speed for data processing but still it is a challenging task to provide better reconstruction quality of image.

Though compression helps in saving storage space but it alone doesn't guarantee any security to the data. Compressed data on server is accessible to any hacker or administrators of untrusted servers; this can harm privacy or the integrity of the data. To cater this, security is also need to be included after compression. Several researches have been done in the past in the field of image or multimedia data encryption. In order to ensure and secure multimedia storage, we apply symmetric cryptography scheme because encryption process changes data stream during transmission. According to this scheme, data is considered as binary sequence and can be encrypted by applying conventional cryptography approach such as AES or DES [8]. Generally, when there is no dynamic requirement i.e. real time streaming, data can be treated as binary sequence and conventional approaches can be applied for securing data but due to dynamic nature of communication, conventional approaches fail to provide efficient security and consumes more power and resources. Also encryption and decryption of uncompressed image takes more time relatively to time taken by compressed images. To overcome these issues, in this manuscript we propose a combined scheme for image compression and encryption using ANN and Blowfish algorithm.

Remainder of manuscript is arranged as follows: section 2 presents review of the literature, section 3 discusses about proposed system model which includes neural network implementation, image compression, blowfish encryption, decryption and cloud storage and retrieval. Section 4 discuss about experimental setup and results. Finally section 5 gives concluding remarks of proposed method.

2. RELATED WORK

This section explores the recent related works in the field of image compression, cloud computing and data security. Ram et al. [9] recommended a new compression mechanism, utilizing lately designed redundant tree based wavelet transformation. Formerly intended for computations defined on graphs as well as cloud of points, their novel technique has been exposed to be highly successful as an image adaptive redundant and multiscale decomposition. Chief notion of their scheme is re-ordering of the image pixels that shape an extremely smooth 1D signal that can be spared by a standard wavelet. Their research has brought a new image adaptive transformation in the area of compression of allied frontal face images. In Shizhong Li [10] proposes a hardware-oriented lossless image compression algorithm, supporting block and line random access flexibly for adapting diverse hardware video codec architectures. Simulation results show that the proposed algorithm achieves competitive rate compression performance compared with reference algorithms. The proposed hardware architecture is verified supporting real-time processing for quad HD videos at the frequency of 166 MHz. Hussain et al. [11] developed DNN (Deep Neural Network) based technique for image compression. Main aim of this technique is to reduce the training time for compression which can be employed for real time application. In order to carry out this work, rectified linear units (ReLUs) is used which speeds up the working of DNN. Watkins et al. [12] developed DNN based image compression technique for a fault tolerant system. According to this process, Levenberg arguardt DNN is applied for image compression. Furthermore, it is used for channel error correction during real-time applications.

Kapil Mishra et al, [13] designed a lossy run length encoder that exploits the pixel redundancy and visual imperceptibility of human eye to fine details in the digital images. Along with compression image encryption using henon chaotic map is performed. After encryption the size and resolution of the image is changed that further enhances the security.

Security and less memory availability are two major concern when storing the data via cloud. While the issue of reduced memory could be addressed by compression algorithm, several paper have been published for securing the data stored in the cloud. Heba M et al. [14] proposed a mechanism on messy map encryption via diverse means of procedures. They worked on Fractional Fourier transform realm for image ciphering. As per the outcome assessments, the encryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

response type procedure is suitable for ciphering than in-block cipher type. This mechanism is simple, quick, and offers good security with noise resistance. In order to hide data or to encrypt, reversible data hiding is a useful technique which is applied during image authentication or archive management of data. Considering this, F. Huang et al. [15] developed a new scheme by shifting histogram where message bits are carried by 1 and -1 values and zero coefficients remain unchanged. Later, based on zero coefficients blocks are selected by applying 8x8 windows which is utilized for data hiding. But, as we have discussed before that reconstruction quality is a bottleneck for image compression and better reconstruction.

In [16] Ali Abdulgader et al. derived a mechanism that triumphs over the preset S-box restrictions and enhances the efficiency of AES algorithm when performed to encrypt images, mainly when the size of image is huge. Substitution is performed in the Mix Column Phase, with that of Chaotic Mapping and the Exclusive Disjunction procedure is performed to lessen operational complications. Sejun Song et al. [17] designed and developed an application based on Selective Encryption and Component Oriented De duplication (SEACOD) mechanism that attains both high speed and effectual data ciphering as well as cutback Mobile Cloud Computing services. Their mechanism not only eliminates duplicate objects in files and mails but also works on images utilizing object level elements based on their skeleton. It also efficiently trim downs the total encryption operation cost on the mobile appliance by adjusting compression and cipher techniques as per the festering data types. This research was intended to optimize operations on mobile devices. Wen-Chuan Wu et al, [18] this paper presents an efficient image protection method to secure the existence of important private images in the cloud by using steganography technique. Experimental results show that the proposed method is able to not only enhance image security but also increase the cloud storage capacity.

Narendra Khatri et al, [19] Proposed algorithm is based on image scrambling and Linear canonical Transform. The image scrambling accomplished using the chaotic function with iterations along the length of the image to be scrambled. The Linear canonical transform (LCT) is used to encrypt all the three components of color image i.e. Red, Green and Blue at the same time. Application of the LCT over these components makes to not affect each other. So the connections between Red, Green and Blue components is condensed in the encrypted components. The security of the colour image is increased using the proposed algorithm. Simulation results represents that the proposed algorithm is best suited for the colour image encryption as well it provide safety to various attacks.

Xiaozhu Xie et al, [20] they proposed a scheme of RDH-EI using reformed JPEG compression. First, the cover image is transformed to quantized DCT coefficients, of which the vast majority of ac coefficients at high frequency is zeros. Therefore, they proposed to embed the secret message into the zeros. Before embedding, quantized DCT coefficients were reformed and encrypted to generate the encrypted image. The recipient can extract data from the marked image with the embedding key. JPEG image can only be recovered with the encryption key. The experimental results demonstrated that the proposed scheme still recovers a JPEG image with both keys, it maintains good quality, which is more than required in some applications.

Chun Ting Huang et al. [21] carried out an intense study on topical multimedia storage security techniques involving cloud systems. Subsequent to the outline of cloud's persistence mechanisms as well as security issues involved in it, they concentrate on core research area of it such as integrity, privacy and updating of data in the cipher text arena. They explained various vital designs and developments presented in the recent researches and indicated probable expansions and future enhancements. Their research purpose is to recommend an up to date information to the fresh scholars who want to go into this exhilarating domain. In Long Bao, [22] propose a lossless (k; n) secret image sharing scheme (SMIE-SIS) that have the certain advantages. This method was fully able to recover the original image without any distortion and was able to verify and detect a fake share. It was able to generate completely different secret shares that are unpredictable and non-repetitive with low computation cost.

Shi et al [23] addressed the issue of cloud storage and developed a data compression scheme for compressing the photo album. This approach is based on the feature analysis model unlike pixel analysis techniques for estimation of correlation between two distinct images. Moreover, the technique uses content-based feature matching

Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which has significant nature. This technique can perform for different scenarios where image scale, rotation and illuminations are varying in a specified time period. For cost minimization, images are arranged in a pseudo sequence based on the image correlation analysis. In this work a three stage prediction model is developed which helps to reduce various image deformation resulting in better prediction. Finally, block based motion compensation method is used for improving the compression performance. In Yushu Zhang [24], proposed an efficient secure service framework for big image data with the help of the hybrid cloud. Based on his work, the sensitive data are securely stored in the private cloud while the insensitive data are encrypted-then subsampled and stored in the public cloud from each image.

Several work have been carried out over the years, highlighting the need of efficient compression algorithm, and securing the data in the cloud. Several efficient method that provides secured access in cloud suffered from complexity issues and the need for optimized algorithm still exist. To address the issues related to these methods, this paper presents a novel technique that elaborates a new approach for image compression as well as encryption and decryption which is related to security. Section 3 discuss the proposed method in detail.

3 SYSTEM MODEL

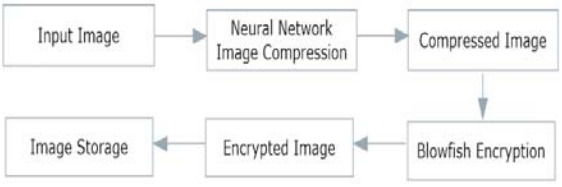

Figure 1: System Diagram of Proposed Storage Approach

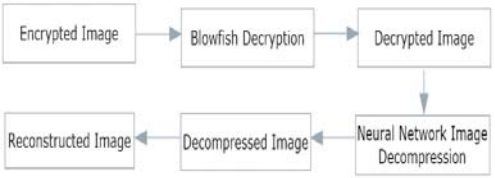

Figure 2: System Diagram of Proposed Reconstruction Approach

Figure 1 and 2 depict the overall system approach for data storage and data retrieval. In this paper, the proposed method can be discussed in detail under three subsections. The subsection 1 describes the new method neural network modelling with the steps for compression and decompression. The novelty of subsection 2 lies in the usage of blowfish algorithm for encryption and decryption. Subsection 3 describes the usage of cloud storage and data retrieval.

3.1 Neural Network Modeling

This section describes the Neural Network Construction Algorithm, Training Process and neural network for image compression.

Let $\mathcal{N}$ be a neural network model which is having an input layer, h hidden layer and output layer. Key issue related to neural network is training of the neural network; therefore, we cast this as an unconstrained problem. Initial objective is to minimize the error of objective function which is defined as follows:

$$E^{(n)}(w,v) = \frac{1}{2}\sum_{i=1}^{k}\left\|\left(\sum_{j=1}^{d} g(x^i w^j)v^j\right) - t^i\right\|^2 \quad (1)$$

k Indicates fixed no. of given samples $x^i \in \mathbb{R}^m$
Target value is denoted as t^i which is $t^i \in \mathbb{R}^m$
For image compression scheme target values are considered equal to the input vector sample i.e. $t^i = x^i$ for all values of x and dimensionality is also considered as $r = c$, where r indicates the no. of rows and c indicates no. of columns. Hidden layer units generates weight in form of vectors which is denoted as v^i

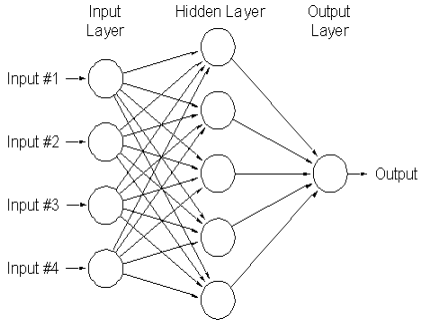

Figure 3: An illustration of feed forward neural network having n input layers, h hidden layers and n output layers

Output is defined as

$$Output: \sum_{j=1}^{k} g(x^i w^j)v^j, i = 1,2,\ldots k \quad (2)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

w^i is the weight of incoming data to hidden units, input vectors are increasing monotonically which are represented by a sigmoidal function

$$\sigma(a) = \frac{1}{1+e^{-a}}$$

By using equation (3) the derivatives of the input can be written in the form of function, which is given as

$$\sigma'(a) = \sigma(a)(1-\sigma(a)) \quad (4)$$

Error in the neural network for image compression technique is computed as

$$e_i^j = S_i^j - t_i^j, \forall_i = 1,2,\dots,k \quad (5)$$

Where n-dimensional vector is computed as

$$S^j = \sum_{i=1}^{k} \sigma(x^i w^j) v^j \quad (6)$$

Components of neural network gradient function are computed by applying chain rule which is defined as follows:

$$\frac{\partial F^k(w,v)}{\partial w_q^p} = \sum_{i=1}^{k}\sum_{j=1}^{k}[e_i^j \times v_i^j \times \sigma(x^i w^j) \times (1-\sigma(x^i w^j)) \times x_q^i]$$

$$\frac{\partial F^k(w,v)}{\partial v_q^p} = \sum_{i=1}^{k}[e_i^j \times v_i^j \times \sigma(x^i w^j) \times (1-\sigma(x^i w^j)) \times x_q^i]$$

Where p= 1,2,3,..k and $q = 1,2,\dots n$

In this process, neural network training algorithm terminates at the stationary point function of the given function$F^k(w,v)$.

Let us consider $(\bar{w},\bar{v})$ is a point during training process which shows$(\bar{w},\bar{v}) \in S^{nxnx}$, is considered a point where$\nabla F^k(\bar{w},\bar{v}) = 0$, it is assumed that the network fails to provide a satisfactory reconstructed image, this network contains k hidden units.

In order to reduce the error we consider an error function which is given as $F^{k+1}(w,v)$ which corresponds to the given neural network with $k+1$ hidden layers. In order to compute this random vector is generated based on the n-dimensional zeros vector, random vector is denoted as $w^{k+1} \in S^n$ and n-dimensional zeros vector isv^{k+1}. According to neural network method, it can be evaluated that$F^{k+1}(\bar{w},w^{k+1},\bar{v},v^{k+1}) = F^k(\bar{w},\bar{v})$. Here our main aim is to trim down the error by finding and showing the input vector such as$F^{k+1}(\bar{w},w^{k+1},\bar{v},v^{k+1}) < F^k(\bar{w},\bar{v})$. In order to reduce the complexity, w^{k+1} is considered as a constant and new quadratic function for n variables is assigned as

$$g(v) = F^{k+1}(\bar{w},w^{k+1},\bar{v},v) = \frac{1}{2}\sum_{i=1}^{k}\|\Delta^i + \delta^i v - t^i\|^2 \quad (8)$$

In equation (8), Δ^i denotes the gradient measurement and can be written as

$$\Delta^i = \sum_{j=1}^{k} \sigma(x^i \bar{w}^j) v^j \quad (9)$$

$$\delta^i = \sigma(x^i w^{k+1})$$

By following equation (8) and (9), gradients can be computed as

$$\Delta g(v) = \sum_{i=1}^{k} \delta^i (\Delta^i + \delta^i v - t^i) \quad (10)$$

$$\nabla^2 g(v) = \left(\sum_{i=1}^{k} (\delta^i)^2\right) I$$

In equation (10), I denotes the identity matrix with n rows and n columns, with the help of this identity matrix, gradient function at zero can be written as

$$\Delta g(0) = \sum_{i=1}^{k} \delta^i \beta^i \quad (11)$$

$$= \sum_{i=1}^{k} \sigma(x^i w^{k+1}) \bar{e}^i \quad (7)$$

$\bar{e}^i$ is the variation between the output value of the network and its actual target value, which is given as $\beta^i = \Delta^i - t^i$

Function is in quadratic form which is considered for all the input vectors, in other words it can be written as

$$g(\beta v) = g(0) + \beta(\nabla g(0))^T v + \frac{1}{2}\beta^2 v^T \nabla^2 g(0) v \quad (12)$$

Above expression defines the neural network construction for image compression.

3.1.1 Neural Network Construction Algorithm

The neural network construction for image compression.

1. Assign initial number of hidden units k to 1
2. Initialize random weights for the given vector
3. Estimate the error minimization position
   a. Denote solution by $(\bar{w},\bar{v})$
4. If solution achieved as pre-specified accuracy then stop
5. Increase hidden layer by adding one unit and select the random weights such as $w^{k+1} \in S^n$ and set vector such as$v^{k+1} = \beta v$, v and β can be computed as discussed before. For the neural network, to minimize the error set $k = k+1$ and initiate the starting point as $(\bar{w},w^{k+1},\bar{v},v^{k+1})$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. Until the solution achieved, repeat from step 3

3.1.2 Neural Network Training Process

Image data is encoded using training process. This encoded data helps to construct hidden and output weights and forms a matrix. According to training process, it is assumed that input image I consists of r rows and c columns. First of all, image data is converted into vector form which is used for training purpose. In this vector, all pixel values are stored for training purpose. In next stage, mean square error (MSE) parameter is computed to obtain the best training performance by reducing MSE. Image is encoded using weight matrix.

3.1.3 Compression of Image

Let us consider an image, which we are interested to store in compressed form. Image contain $r \times c$ matrix where r indicates the no. of rows and c indicates the n. of column of the image. Later image is divided into sub blocks with the size of$m \times m$. Each block is considered as a single pattern which is utilized for the neural network training procedure. While input image is compressed with neural network having h units of hidden nodes, in this process we store non-linear transformed value which are$\alpha(x^i, w^j), j = 1,2,3 \ldots, h$. In this way, reconstructed image is obtained by applying liner transformation, as$\sum_{j=1}^{h} \alpha(x^i w^j) v^j$. $\sum_{j=1}^{h} \alpha(x^i w^j) v^j$ varies from 0 to 1, this nature of linear transformation allows us to quantize the input using 8 bits , this results in lower deterioration and quality preservation of image.

In order to perform the quantization, q bits are considered. Required bits for compression and storage are expressed as

$$S_{NN} = \left(\frac{512 \times 512}{m \times m} \times b \times h\right) + \left(m \times m \times h \times r(b)\right) \quad (1)$$

These steps are followed to compress the input image:

1. Input image is converted in to a matrix form (I)which is denoted as $X_{r,c}$ where r is row vector and c is column vector
2. In next step, pixel values and neighboring pixel repetition values are counted which are combined in a pair
3. The sequence of this pair is given as input to neural network
4. By considering this, weights are computed for each pixel value
5. Hidden layer is created as

$$H_j = \sum_{i=1}^{n} x_{ij} x_i \quad (13)$$

H gives the compressed image file

For decompression steps are:

1. Get compressed file as layers $H_{i=j}$
2. Perform weight computation as

$$w_{ij} = \sum_{j=1}^{k} H_j H_j^T$$

3. In next stage, output layer is created with the help of weight

$$O_i = \sum_{j=1}^{k} w_{ij} H_j$$

4. Output layer is converted into sequence as a row vector
5. Row sequence vector is represented as a pair where each pair denotes pixel value and repetition of neighboring pixel value.
6. Pixel pairs are converted in to a matrix form
7. This matrix is displayed in the form of image.

3.2 Blowfish Algorithm

Blowfish uses same secret key for encryption and decryption due to its symmetric nature. During encryption and decryption message is divided into fixed block length. This algorithm provides alternate approach for DES or IDEA algorithm. In this, variable length key is varied from 32 bits to 448 bits. This algorithm is Festal Network in which encryption function is performed 16 times. Block size contains 32 bits and length of key can be up to 448 bits [25].

This is performed into two parts: (a) key expansion (b) data encryption part. According to key expansion, various sub keys are generated by converting key bits. In data encryption section, encryption function is performed 16 times by using Festal network. In each repetition key, data substitution and key based permutation are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

included. Addition operations use four indexed array data and other operations are performed by implementing XORs. During execution, blowfish uses huge number of sub keys. Before encrypting the data, keys are computed.

In $P-array$, 18 sub keys are stored with the size of 32 bit each
Four $s-boxes$ are used with 256 entries

Blowfish algorithm has shown significant improvements in efficiency compared to other symmetric algorithms which are demonstrated in following results section.

3.3 Cloud Storage and Retrieval

Once the encryption process is done they can be stored in the cloud. Cloud provides the services as required by the clients. The services provider of the cloud, provides the required resources to store the large amount of data at low price. The updated data are stored in the cloud and then retrieved whenever necessary by the clients. The storage and retrieval time is also less. The image can be retrieved from the cloud and then decrypted. The decryption requires the private key to be known by them.

4 EXPERIMENTAL SETUP AND RESULTS

To conduct the experiment, we use two different set of software i.e. for image compression we use MATLAB 2013b, neural network toolbox and image processing toolbox and for overall execution of code in cloud simulation environment we use CLOUDSIM 2.0 API running on Eclipse Indigo platform which is installed on top of JDK 1.6.0_11 in windows 7 (64 bit) OS. As MATLAB tool has limitations to run code on cloud platform, we call MATLAB subroutines from CLOUDSIM VMs. For execution we use single VM as XEN server with 512MB RAM and 1GB bandwidth.

In our experimental model we are using 6 parameters of quality matrices and a histogram analysis is evaluated to verify the quality of reconstructed image. These parameters are: (1) PSNR (Peak Signal to Noise Ratio) (2) MSE (Mean Squared Error) (3) Average Difference (4) Maximum Difference (5) Normalized Absolute Error, and (6) Average training performance. These parameters can be computed by using below given equations. Proposed model is implemented on cloud so to show the performance of cloud simulation we consider encryption and decryption time for performance evaluation.

1) PSNR (Peak Signal to Noise Ratio)

$$PSNR_{dB} = 20.\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad (14)$$

(2) MSE (Mean Squared Error)

$$MSE = \frac{1}{MN}\sum_{M}\sum_{N}[Re\tilde{I}_{img}(m) - Out(x \quad (15)$$

(3) Average difference

$$AverageDifference = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)) \quad (16)$$

(4) Maximum difference

$$MaxDifference = MAX|x(i,j) - y(i,j)| \quad (17)$$

(5) Normalized absolute error

$$NormAbsError = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|(x(i,j) - y(i, \quad (18)$$

`For experimental study we have considered standard benchmark images with size of 512x512 and 256x256 pixels.

Table 1: Compression Result of Lena Image

 Lena Image (512x512)	 Compressed Lena Image	 Reconstructed Lena Image

In above Table 1, we show the results of image compression and reconstruction. We have considered “Lena” Image.

Proposed approach for image compression and encryption is compared with other state–of-art Compression techniques [26]. These schemes are compared using different images and their sizes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Performance Results of Proposed Scheme for Different Test Image

Image	MSE	PSNR	Average Difference	Normalized Absolute Error	Maximum Difference	Compression Ratio	Encryption Time	Decryption Time
Lena (512*512)	362.856	22.533dB	0.162646	0.084604	141	25%	192ms	13ms
Barbara (512*512)	367.23	21.89dB	0.1860	0.01298	203	25%	18ms	12ms
Cameraman (256*256)	259.3375	42.1739dB	0.021093	0.018521	71	25%	175ms	17ms
Rice (256*256)	241.029	43.938dB	0.016089	0.011327	106	25%	19ms	16ms

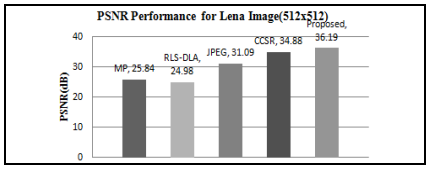

Figure 4: PSNR Performance for Lena Image

Above given Figure 4 shows comparative performance of Lena images in terms of PSNR. Using proposed approach of compression, maximum PSNR achieved in cameraman image is 31.17 dB whereas for the same image CCSR [26] 30.4 dB which shows 7.7% improvement in the reconstruction quality of image. In Barbara image PSNR performance is 31.12 whereas using [26] 31.8dB is achieved.

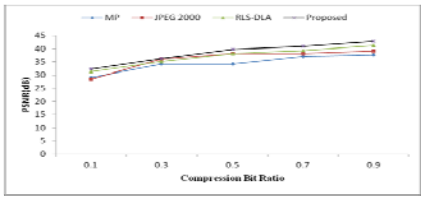

Figure 5: Comparative Analysis

Another study is carried out by varying compression bit ratios on Lena image and based on these variations PSNR values are achieved. Fig. 5 shows performance comparison by considering all schemes. From this, it can be concluded that proposed approach provides maximum PSNR of 42.85 dB which provides better reconstruction. For better understanding of this comparative study, varied compression bit rate achieved PSNR is given in table 3.

Table 3: Performance Results of Proposed Scheme for Different Test Image

Compression Bit Rate	**0.1**	**0.3**	**0.5**	**0.7**	**0.9**
MP	29	34.12	34.12	37.14	37.78
JPEG 2000	28.38	36.15	38.12	38.12	39.12
RLS-DLA	31.25	35.22	38.11	39.22	41.2

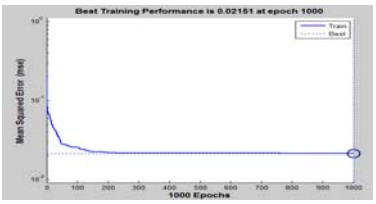

Figure 6: Average Training Performance

Figure 6 shows average training performance of neural network. For this analysis, maximum 1000 number of epochs are considered where neural network achieves best training performance as 0.021 however, experimental study includes training for four images and can be extended up to 16 images.

Similarly, in order to evaluate reconstructed image quality, we perform histogram analysis on input and reconstructed Lena image. For original image and reconstructed image, histogram analysis is presented Figure 7 and 8 respectively.

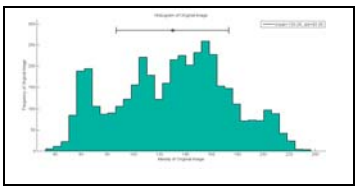

Figure 7: Histogram Analysis of Original Lena Image

Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

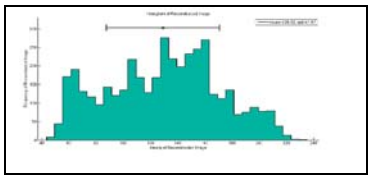

Figure 8: Histogram Analysis of Reconstructed Lena Image

Histogram of any image can be verified by evaluating mean and standard deviation of any image, in our simulation study mean and standard deviation for original image are 130.28 and 43.35 respectively, for reconstructed image mean and standard deviation are 129.35 and 41.67 respectively. This analysis shows the information preserving nature of proposed BANN approach. We evaluate encryption and decryption performance and compare it with other existing algorithms such as AES, DES and 3DES.

In Figure 9 and 10, performance in terms of time efficiency during encryption and decryption is depicted. A comparative performance is given by considering.

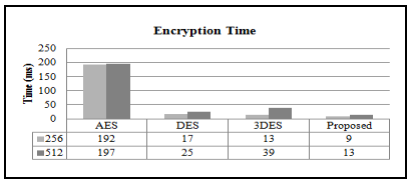

Figure 9: Comparative Analyses For Encryption Time

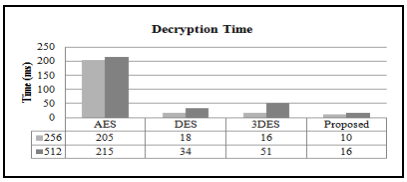

Figure 10: Comparative Analyses For Decryption Time

AES, DES and 3DES algorithm, it can be seen from Figure 9 and 10 that Blowfish requires less time in operations when compared to other schemes. In order to show the robustness of this work varied image sizes are considered and performance is evaluated on it.

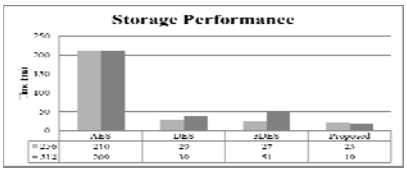

Figure 11: Comparative Analyses For Cloud Storage Time

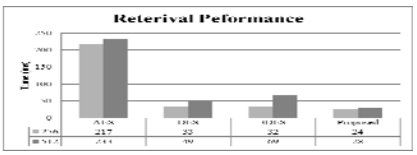

Figure 12: Comparative Analyses For Cloud Retrieval Time

Here we have checked performance against the existing system. Storage and retrieval performance is evaluated for different file size of images where 256 and 512 are considered as image size. We found out that the time taken for our system is less than that of the existing system. The time taken to compute the result increases with the increase in the image size. That is, in case the image size is big, the time taken to encrypt it is more compared to the smaller images Storage and retrieval time is computed and compared for both file size scenarios as depicted in Figure 11 and 12.

The overall contribution of the paper lies in proposing an efficient compression scheme which benefits the access time of the data in the cloud. Owing to the issues related to the security of the data, which is said vulnerable to threats, the paper also proposed an efficient encryption and decryption algorithm for the data. The results of the proposed work is achieves better PSNR and less cloud access time which is a significant contribution of the proposed work.

5 CONCLUSION

In this work, a joint scheme for compressing the data and providing security to it is addressed. To deliver an efficient compression of the data, Neural Network based compression technique is used and the security of the data is provided by Blowfish algorithm. In order to have an easy access to the data, the storage of the data is done in cloud and the proposed method also challenges the storage and retrieval time of data in cloud. Based on the performance evaluation carried out by computing statistical parameters such as PSNR, MSE, compression ratio the proposed technique out performs all the state of art algorithms. Simulation result show that proposed approach achieves better quality reconstructed image and consumes less time to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

encrypt and decrypt. Another advantage of the proposed method lies in consumption of minimum time for storing and retrieval of data in cloud.

Though the algorithm works well for JPEG format images, the efficiency of the algorithm need to be tested for other different types of images and HD quality images. In the future, we would like to focus our efforts on other different multimedia applications such as text, audio and video with suitable algorithms.

REFRENCES:

[1] I. Debbabi, W. Kammoun and R. Bouallegue, "A taxonomy of multimedia videoconferencing system Technologies and issues", *World Congress on Computer Applications and Information Systems (WCCAIS)*, Hammamet, 2014, pp 1-7.

[2] A. Heindel; E. Wige and A. Kaup, "Low Complexity Enhancement Layer Compression for Scalable Lossless Video Coding based on HEVC" , *IEEE Transactions on Circuits and Systems for Video Technology* , No 99, Apr 2016, pp 1-12.

[3] M. Hilbert and P. López, "The world's technological capacity to store, communicate, and compute information", *Science*, Vol 332, No 6025, 2011, pp 60–65.

[4] Hanaa ZainEldin, Mostafa A. Elhosseini, and Hesham A. Ali, "Image compression algorithms in wireless multimedia sensor networks: A survey", *Ain Shams Engineering Journal*, Vol 6, Issue 2, Jun 2015, pp 481-490.

[5] W. C. Chu, "On lossless and lossy compression of step size matrices in JPEG coding", *International Conference on Computing, Networking and Communications (ICNC)*, San Diego, 2013, pp 103-107.

[6] T. M. Quan and W. K. Jeong ,"A fast discrete wavelet transform using hybrid parallelism on GPUs", *IEEE Transactions on Parallel and Distributed Systems* , Vol 27, Issue 11, Nov 2016, pp 3088-3100.

[7] A. Mostafa, T. Khan and K. Wahid, "An improved YEF-DCT based compression algorithm for video capsule endoscopy",*36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Chicago, 2014, pp 2452-2455.

[8] Douglas R. Stinson, "Cryptography, Theory and Practice", *Chapman and Hall/CRC*, 3rd edition, 2006.

[9] I. Ram, I. Cohen and M. Elad, "Facial Image Compression using Patch Ordering Based Adaptive Wavelet Transform", *IEEE Signal Processing Letters*, Vol 21, No 10, Oct 2014, pp 1270-1274.

[10]] Shizhong Li, Haibing Yin, Xiangzhong Fang, and Huijuan Lu ,"Lossless image compression algorithm and hardware architecture for bandwidth reduction of external memory ",*IET Image Processing*, Vol 11, Issue 6, June 2017,pp 379 - 388.

[11] F. Hussain and J. Jeong, "Efficient deep neural network for digital image compression employing rectified linear neurons", *Journal of Sensors*, 2016, pp 1-7.

[12] Yijing Z. Watkins, and Mohammad R. Sayeh, "Image Data Compression and Noisy Channel Error Correction Using Deep Neural Network", *Procedia Computer Science*, Vol 95, 2016, pp 145-152.

[13] Kapil Mishra and Ravi Saharan, " Image Encryption Utilizing Lossy Image compression" ,*International Conference on Computer, Communications and Electronics (Comptelix)*,1-2 July 2017,Jaipur, India, IEEE, pp 494-500.

[14] Heba M. Elhoseny, Hossam H. Ahmed, Alaa M. Abbas, Hassan B Kazemian, Osama S. Faragallah, and Sayed M. El-Rabaie."Chaotic encryptions of Images in the Fractional Fourier Transform domain using different modes of operation". *Springer*. Vol 9, Issue 3, Mar 2015, pp 611–622.

[15] F. Huang, X. Qu, H. J. Kim, and J. Huang, "Reversible Data Hiding in JPEG Images" , *IEEE Transactions on Circuits and Systems for Video Technology* , Vol PP, No 99, 26 Aug 2015, pp.1-1.

[16] Abdulgader, MahamodIismail, Nasharuddin Zainal and Tarik Idbeaa, "Enhancement of AES Algorithm based on Chaotic Maps and Shift Operation for Image Encryption", *Journal of Theoretical and Applied Information Technology*, Vol 71,No 1 ,Jan 2015, pp 1-12.

[17] Sejun Song Baek Young Choi and Daehee Kim, "Selective encryption and component oriented deduplication for mobile cloud data computing", *International Conference on Computing, Networking and Communications (ICNC)*, Hawaii, USA, 2016, pp 1-5.

[18] Wen Chuan Wu and Shang Chian Yang, "Enhancing Image Security and Privacy in Cloud System Using Steganography ", *IEEE International Conference on Consumer Electronics*, Taiwan, 12-14 June 2017, pp 321-322.

[19] Narendra Khatri and Harish Sharma., "A Novel Colour Image Encryption Algorithm based on Linear Canonical Transform ", *International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017),* Navi Mumbai, India, 27-28 Jan. 2017, IEEE, pp 1101-1108.

[20] Xiaozhu Xie and Chin-Chen Chang. "Reversible Data Hiding in Encrypted Images Using Reformed JPEG Compression ", *5th International Workshop on*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Biometrics and Forensics (IWBF), Coventry, 4-5 April 2017, IEEE, pp 1-5.

[21] Chun Ting Huang, Zhongyuan Qin, and. Jay Kuo; "Multimedia Storage Security in Cloud Computing: An Overview", *Multimedia Signal Processing (MMSP)13th International Workshop*, Hangzhou, 17-19 Oct. 2011, IEEE, pp 1-6.

[22] Long Bao, Shuang Yi and Yicong Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k,n) Secret Image Sharing", *IEEE Transactions on Image Processing*, Vol 26, Issue: 12, Dec 2017 ,pp 5618 - 5631.

[23] Z. Shi, X. Sun and F. Wu, "Photo Album Compression for Cloud Storage Using Local Features", *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol 4, Issue 1, March 2014,pp 17-28.

[24] Yushu Zhang, Hui Huang, Yong Xiang, and Leo Yu Zhang, "Harnessing the Hybrid Cloud for Secure Big Image Data Service", *IEEE Internet of Things Journal*. Vol 4, Issue 5, Oct. 2017, pp 1380 - 1388.

[25] A. Alabaichi, F. Ahmad and R. Mahmod "Security analysis of blowfish algorithm", *Informatics and Applications (ICIA) Second International Conference*, Lodz, 2013, pp 12-18.

[26] M. Xu, S. Li, J. Lu and W. Zhu, "Compressibility Constrained Sparse Representation With Learnt Dictionary for Low Bit Rate Image Compression", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol 24, No 10, Oct 2014, pp. 1743-1757.