ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient and Secure Video Encryption and Decryption using Neural Network

Saraswati Singh
M.Tech. Scholar, CSE Department,
School of Engineering & IT,
MATS University, Raipur (C.G.), India

Nilmani Verma
Head, CSE Departments,
School of Engineering & IT,
MATS University, Raipur (C.G.), India

Vinay Kumar
Assistant Professor, ET&T Department,
Bhilai Institute of Technology,
Raipur (C.G.), India

Abstract: With the increase of multimedia data are transmitted in the various fields like commercial, video conferencing, medical image system and military communication etc., which generally include some sensitive data. Therefore, there is a great demand for secured data storage and transmission techniques. Information security has traditionally been ensured with data encryption and authentication techniques. Different encryption standards have been developed where secrecy of communication is maintained by secret key exchange. In this paper we proposed the video encryption algorithm for secure video transmission using permutation and doping function, thereby security of the original cipher has been enhanced by addition of impurities to misguide the cryptanalyst. Since the encryption process is one way function, the artificial neural networks are best suited for this purpose in decryption algorithm. The ANNs have many characteristics such as learning, generalization, less data requirement, accuracy, ease of implementation, and software and hardware availability, which make it very attractive for many applications. Also need of key exchange prior to data exchange has been eliminated. This paper presents video compression after encryption algorithms such that compressing encrypted video can still be efficiently performed. In addition, this paper focuses the quality of video to make it efficient using enhancement technique.

Keywords: Artificial neural networks, Back propagation algorithm, Encryption, Decryption, Cipher and Decipher, Normalization, Lossless compression, Enhancement.

I. INTRODUCTION

Today, cryptography is a cornerstone of the modern security technologies used to protect information on both open and closed networks. It uses mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [1]. The encryption algorithm transmits the video securely over the network so that no unauthorized user can able to decrypt the video. The challenge in multimedia applications is the transport services to media such as text, image and video with limited bandwidth and huge data size. With the huge demand for bandwidth due to the large data transmitted in multimedia applications, it becomes necessary to apply compression technique on transmitted data.

Through years, different encryption algorithms have been developed based on symmetric key encryption and asymmetric key encryption were highlighted and evaluated with respect to their security level and encryption speed. Most of the algorithms used are generic and there is need of key to decrypt the multimedia data [2]. Dual approach of video compression & encryption is carried out in two processes such as individual or independent compression and encryption (i.e. either compression followed by encryption or encryption followed by compression) & Joint Compression and Encryption. Data encryption standard (DES) [5] has been proposed for main encryption standard. DES are generally not to be suitable for video encryption because of the relative slow speed, complex and less secure using symmetric key. M. Abomhara, Omar Zakaria and Othman O. Khalifa [8] [3] have presented a comparative study of different video encryption algorithm. Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas and Aniket More [6] made a safely exchange confidential videos by an innovative encryption algorithm for videos compressed using H.264.

It shuffles the video frames along with the audio to maintain a balance between security and computational time and then AES is used to selectively encrypt the sensitive video codewords. Amit Pande, Joseph Zambreno & Prasant Mohapatra [7] proposed chaos-based for Joint Video Compression and Encryption (JVCE) to reduce the computational complexity of video compression, as well as provide encryption of multimedia content for web services. This approach is recently used which may be fast as compared to Compression Followed by Encryption (CE) and Encryption Followed by Compression (EC) but procedure is complicated. Some of papers are presented encryption/decryption technique using Neural Network because it plays a very important role in information security. Khalil Shihab [9] have used neural network for encryption/decryption of text data and Saraswati D. joshi, Dr. V. R. Udupi [10] have used novel neural network approach for encryption/decryption of digital image. Also need of key exchange prior to data exchange has been eliminated. There are trades offs when applying different encryption algorithms and its choice depends on the applications. However, many researchers have pointed out

the weaknesses of these methods such as either low security, or low speed, or poor quality or stream size increases.

This paper presents for video using one way cryptography based on Artificial Neural Network. Neural network and cryptography together can make a great help in field of networks security. The objective of this paper to make an efficient and secures video transmission and reception.

II. ARTIFICIAL NEURAL NETWORKS USING BACKPROPAGATION ALGORITHM

Artificial Neural networks (ANN) [9] are simplified models of the biological nervous system. An ANN, in general, is a highly interconnected, massively parallel distributed processing network with a large number of processing elements called neurons in an architecture inspired by the brain, which has a natural propensity for storing experimental knowledge and making it available for later use. Each neuron is connected to other neurons by means of directed communication links each with an associated weight. Each neuron has an internal state, called its activation or activity level, which is a function of the inputs it has received. Typically, a neuron sends its activation as a signal to several other neurons. There are several architectures in which the neurons can be connected. Commonly neural networks are adjusted or trained, so that specific input leads to specific target output.

The Backpropagation learning algorithm is one of the well known algorithms in Neural Network. The introduction of back propagation algorithm has overcome the drawback of previous Neural Network where single layer perceptron fail to solve a simple XOR problem**.** Hence multilayer feed forward (MLFF) networks with Back propagation learning and non linear node functions are used to overcome these limitations. Multilayer feed forward network [MLFF] is made up of multiple layers such as: input layer, output layer and intermediary layers called hidden layers. The output from a Backpropagation neural network is computed using a procedure known as the forward pass, where input layer propagates a particular input vector's components to each node in the middle layer. Middle layer nodes compute output values, which become inputs to the nodes of the output layer. And output layer nodes compute the network output for the particular input vector. The forward pass produces an output vector for a given input vector based on the current state of the network weights. Since the network weights are initialized to random values, it is unlikely that reasonable outputs will result before training. The weights are adjusted to reduce the error by propagating the output error backward through the network. This process is where the Backpropagation neural network gets its name and is known as the backward pass. The training set is repeatedly presented to the network and the weight values are adjusted until the overall error is below a predetermined tolerance.

III. PROPOSED METHOD

The proposed method has been used compression after encryption algorithm to transmit the video at faster rate with high level security. In decryption algorithm, it used Artificial Neural Network to decrypt the video frames which does not use any secret key hence there is no fear to hacking of secret information. In addition focus the video quality to make it better than the original video by using enhancement technique. Here we are using the Brightness preserving Bi-Histogram Equalization (BBHE) technique [11] because it gives better quality than other enhancement technique with less complexity [14]. As the size of video is very huge hence it focused on the compression technique [4] [13] so that efficient use of transmission channel can be done.

Semantic block diagram of proposed approach is given below in figure1. The proposed model is divided into four modules- Enhancement, Encryption, Decryption and Compression.

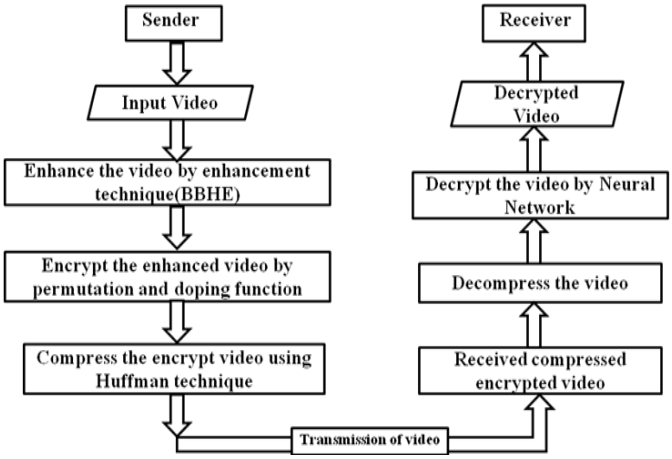


Figure 1: Architecture of Proposed Model.

A. Enhancement module:

The raw input video is fed to Enhancement module which uses brightness preserving bi-histogram equalization (BBHE) technique to improve the quality of video for human interpretation. BBHE method decomposes the original video frame/image into two sub-images, by using the image mean gray-level, and then applies the Histogram Equalization (HE) method on each of the sub-images then it composes, and this method is applied in whole video frames. It is mathematically shown that the BBHE method produces an output image with the value of brightness (the mean gray-level) located in the middle of the mean of the input image and the middle gray-level (i.e., L/2).

B. Encryption module:

In encryption module, enhanced video is encrypted by using permutation-substitution method with impurity addition. There is no secret key on which a permutation is generated since the encryption process is one way function. There are following steps of encryption algorithm:

Step1: Get the pixel value of the image file. [0000001] [1]

Step2: Divide the pixel byte value into upper and lower nibble [0000 and 0001].

Step3: Exchange the nibbles and concatenate to form a byte [00010000].

Step4: Calculate the impurity by EX-ORing the original msnibble and lsnibble, [0001].

Step5: shift the bits of impurities by 5 bits to right. Now we get 9 bit number [000100000]

Step6: EX-OR the results of step3 and step5 [000110000] = 48.

Step7: Add impurity to the obtained result in step 6.Impurity Value chosen is 117, [48+117].

Step8: Continue step1 to step7 for all the pixels of the video frames.

Additional column required:

Step9: Additional one column is added and the value of 117 is added in that column. This is required for the normalization of the matrix because after addition of 117 in pixel value it exceed the range of 256.

Table I shows the transformation of the sample pixel values after encryption.

Table 1: Sample of Encryption Result

Original Pixel Value	Pixel Value after Encryption
1	165
45	423
67	329
165	559
199	401
255	372

C. Compression module:

Huffman code method is used for the compression of encrypted video frames; basically it is a lossless compression method. There are the following steps for this:

Step1: Compression of encrypted video is performed by Huffman coding.

Step2: Find the pixel value (i.e. intensity value) which is non-repeated.

Step3: Calculate the probability of each pixel value.

Step4: Probability of pixel values are arranged in decreasing order and lower probabilities are merged and this step is continued until only two probabilities are left and codes are assigned according to rule that the highest probable symbol will have a shorter length code.

Step5: Further Huffman encoding is performed i.e. mapping of the code words to the corresponding symbols will result in a compressed data. Thus a Huffman code tree is generated and Huffman codes are obtained from labelling of the code tree

Step6: At the receiving end, decompression of compress encrypted image/video is performed by Huffman decoding.

Step7: Generate a tree equivalent to the encoding tree.

Step8: Output the character encodes in the leaf and returns to the root, and continues until all the codes of corresponding symbols are known.

Step9: The original encrypted video is reconstructed i.e. decompression is done by using huffman decoding. Thus result find in compressed encrypted video.

D. Decryption module:

In decryption algorithm, decrypt the compressed encrypted video by Artificial Neural Network [12] which is best suited for one way encryption. Also there is no need of key to decrypt the video. Where it is provides high level security because it's able to perform for non linear input-output characteristics. MATLAB's neural network tool box is used for training and implementing. The system is designed for three layers-input, output and hidden layers.

The input and output have only one neuron while in hidden layer the neurons can vary. Large number of neurons is required to achieving high security. The structure of the network NxMxN has been used with different numbers of hidden neurons M = 4, 6,9,16 and 25 etc. to select the best structure for video encryption purpose; there is no certain method or approach to determine the best structure. One way encryption based on multi-layer neural network have presented, as shown in figure.2, which produces the hash value of the video data as input.

The neural network is trained for standard mapping value and the weights and biases are stored before applying input to it. Finally, the simulation results showed that after training the artificial neural networks.

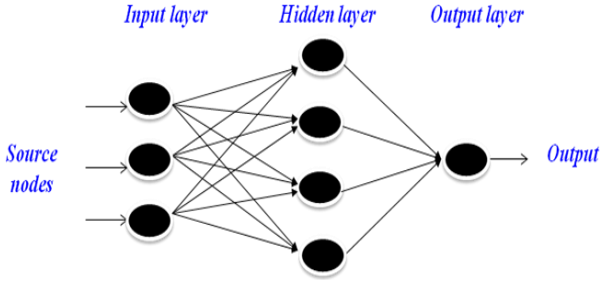
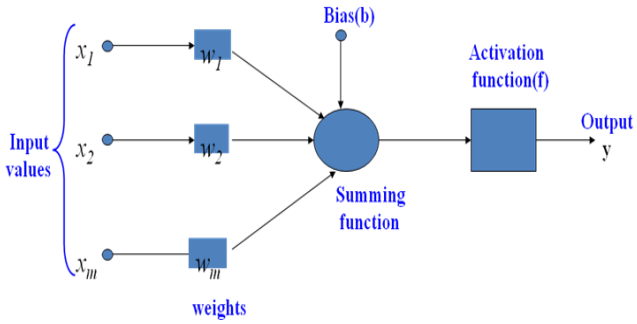


Figure 2: 3-Layer Feed Forward Network using Backpropagation



w_i - weight matrix of the i^{th} layer, f - activation function, b_{ij} - biasis of j^{th} neuron in i^{th} layer

Figure 3: Neurons diagram

IV. RESULTS AND DISCUSSION

MATLAB R2012a have used as a simulation environment. 'Uigetfile' function is use for loading and showing the input video sequence. The loaded video sequence is converted into frames using 'move (k).cdata' function. Here figure.4 (a-d) show the result of the frames (15-18) is separated from the input video.

Figure.5 (a-d) shows the result of enhanced frames, which is better than the original video frames. The video quality is measured by parameters such as Image Brightness Mean (IBM) and Image Contrast Standard Deviation (ICSD) for each original frame with their enhanced frames (figure 9 & 10).

Figure.6(a-d) shows the result of the encrypted video without key using one way function. Hence there is no fear to hacking of secret information.

Figure.7(a-d) shows the result of the compressed encrypted video without loss of video quality.

Finally figure. 8(a-d) shows the result of decrypted frames thus the video frames are recovered in better quality.

A. Video quality analysis by parameters:

The quality of video file is measured by parameters which are Image Brightness Mean (IBM) and Image Contrast Standard Deviation (ICSD).Where image brightness mean should be either minimum or close to original video frame and image contrast standard deviation should be high for better result. Figure.9 shows the graph between IBM and number of frames for input frames and enhanced frames and

figure.10 shows the graph between ICSD and number of video frames of input frames and enhanced frames. Thus the proposed method shows better result in terms of contrast of the enhanced video then original video and having better in preserving the brightness of the enhanced video then original video.

V. CONCLUSION

Presented work discusses an efficient and secure video encryption and decryption. Proposed method uses the Neural Network to decrypt the video frames which does not use any secret key hence there is no fear to hacking of secret information. A feed forward multilayer perceptron utilize Backpropagation algorithm that have been found to be suitable for one way video encryption. The accuracy of the system has been found very high. Result shows that the proposed algorithm not only successfully encrypt and decrypt the video but also give the video in better quality. It provides flexible, accurate and natural looking video frames. However, this method ensures that every aspect of security is maintained without sacrificing the quality of video for real-time applications.

VI. REFERENCES

[1] William Stallings," network security essentials, applications and standards", 4th edition Pearson Education India, 2007 - 432 pages.

[2] Francia G.A, "applied image processing to multimedia information security", IEEE International Conference on Image Analysis and Signal Processing, pp. 104-107, 11-12 April 2009.

[3] B. Furht, D. Socek, and A. M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques," Multimedia Security Handbook, CRC Press, 2005.

[4] Shiguo lian, Multimedia Content Encryption: Algorithms and Application, CRC Press, 2008.

[5] Wayne G. Barker, "Introduction to the analysis of the Data Encryption Standard (DES)", Aegean Park Press, 1991.

[6] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas and Aniket More, "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study", International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, pp.1-5, March 2013.

[7] Amit Pande, Joseph Zambreno & Prasant Mohapatra, "Joint Video Compression and Encryption using Arithmetic Coding and Chaos", IEEE Intl. Conf. on Internet Multimedia Systems Architecture and Application, 2010.

[8] M. Abomhara, Omar Zakaria, Othman O. Khalifa, "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp. 103-110, February 2010.

[9] Khalil Shihab, "a Backpropagation neural network for computer network security", Journal of Computer Science vol. - 2 (9), pp.710-715, 2006.

[10] Saraswati D. joshi, Dr. V. R. Udupi and Dr. D. R. joshi, "A novel neural network approach for digital image data encryption/decryption", IEEE International Conference on Power, Signals, Controls and Computation (EPSCICON),pp.1-4, 3-6 Jan. 2012.

[11] Yeong-Taeg Kim, "Contrast enhancement using brightness preserving bi-histogram equalization", IEEE Trans. Consumer Electronics, vol. 43, no. 1, pp. 1-8, Feb. 1997.

[12] Liew Pol Yee De Silva L.C,"application of multilayer perceptron network as a one way Hash function", IEEE International Joint Conference on Neural Networks,vol.2, pp.1459-1462, May 2002.

[13] Jagadish h. pujar and Lohit m. kadlaskar, "A new lossless method of image compression and decompression using huffman coding techniques", Journal of Theoretical and Applied Information Technology, Vol.15, No.1, pp. 18-23, 2010.

[14] Vinay Kumar and Himani Bansal, "Performance Evaluation of Contrast enhancement Techniques for Digital Images" International Journal of Computer Science and Technology, pp-23-27, Vol.-2, Issue-1, March 2011.

VII. RESULTANT FIGURES :

Figure: 4(a), 4(b), 4(c) & 4(d)

Figure: 5(a), 5(b), 5(c) & 5(d)

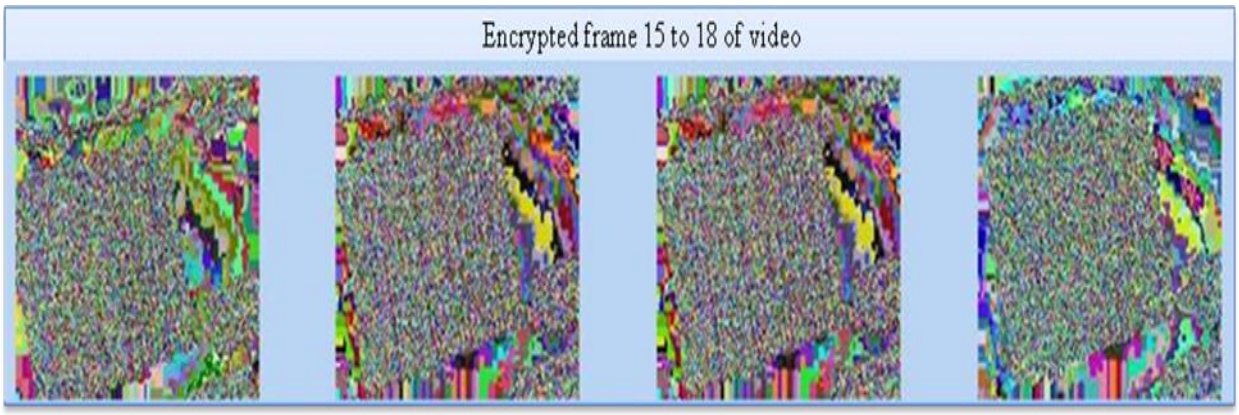


Figure: 6(a), 6(b), 6(c) & 6(d)

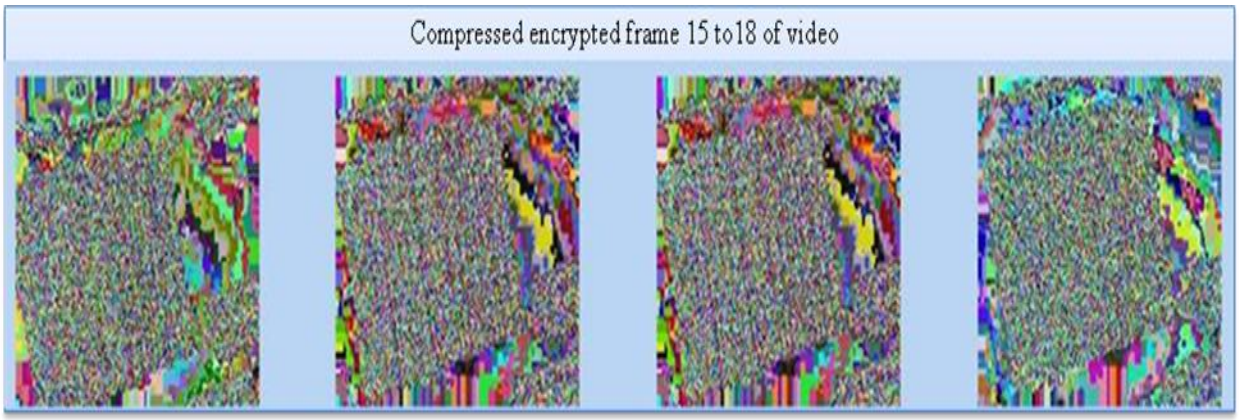


Figure: 7(a), 7(b), 7(c) & 7(d)

Figure: 8(a), 8(b), 8(c) & 8(d)

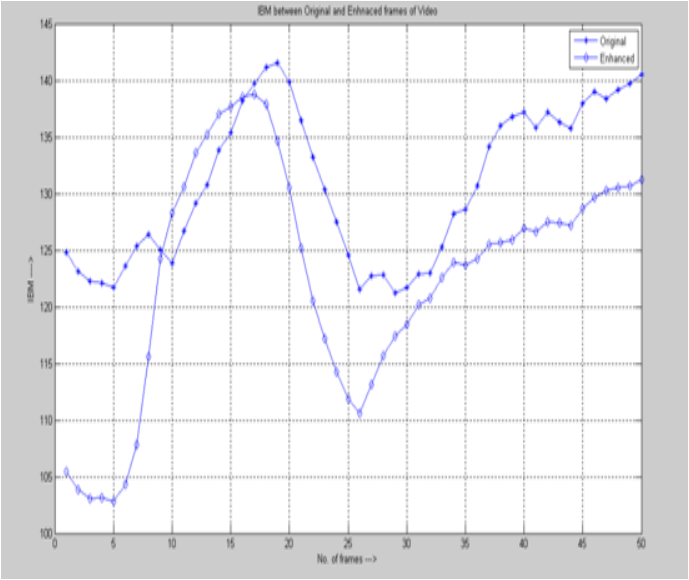


Figure 9: Image Brightness mean (IBM)

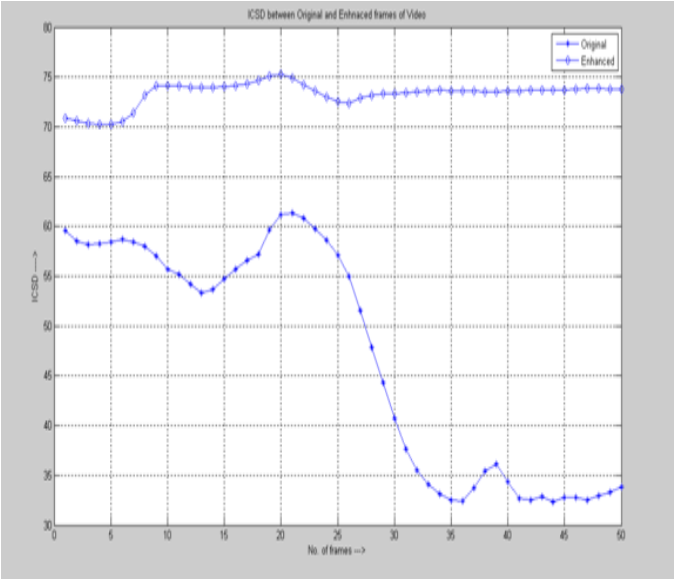


Figure 10: Image Contrast standard deviation