Video Encryption and Decryption with Authentication using Artificial Neural Networks

Renuka.B.Talewad
(M.Tech, *Digital Communication, Basaveshwara Engineering College, Karnataka, India)*

Abstract *:Multimedia data security is becoming important with the continuous increase of digital communications on internet. With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. . The encryption algorithms developed to secure text data are not suitable for multimedia application because of the large data size and real time constraint. 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. The secrecy of communication is maintained by secret key exchange. In effect the strength of the algorithm depends solely on the length of the key. The presented work aims at secure video transmission using randomness in encryption algorithm, thereby creating more confusion to obtain the original data. The 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 as they possess features like high security, no distortion and its ability to perform for non linear input-output characteristics, In the presented work the need for key exchange is also eliminated, which is otherwise a perquisite for most of the algorithms used today. The proposed work finds its application in medical imaging systems, military image database communication and confidential video conferencing, and similar such application. The results are obtained through the use of MATLAB 7.14.0*

Keywords: *Artificial Neural networks, Back propagation algorithm, video encryption and decryption, cipher and decipher.*

I. INTRODUCTION

Information security has traditionally been ensured with data encryption and authentication techniques. Different generic data encryption standards have been developed. Although these encryption standards provide a high level of data protection, they are not efficient in the encryption of multimedia contents due to the large volume of digital image/video data. In order to address this issue, different image/video encryption methodologies have been developed. In the past few years there have has been an explosion in the use of digital media. Industry is making significant investment to deliver digital audio, image and video information to the consumers. Hence security of multimedia data has become more and more important. Data encryption standard (DES)[5] has been the main encryption standard from 1977. However in the year 1998 it has been shown to be vulnerable to brute force attacks, differential cryptanalysis and linear cryptanalysis. Acknowledging the need for a new encryption standard, several ciphers have been proposed such as AES, 3DES, MARS, RSA, Serpent, two fish, blowfish, IDEA and GOST were used[10][15]. Because of voluminous data involved in image/video, other encryption methodologies such as affine transform, the chaotic system and the frequency domain algorithms have been developed.

Neural network plays a very important role in information security and lot of work has been going on in this direction. Whether it is image processing or otherwise, most of the algorithms used are generic, because of which the key exchange has become a prerequisite prior to exchange of the data [4]. Hence the strength of such encryption solely lies on the key length. In the presented work, encryption process uses random substitutions, and impurity addition (doping) creating more confusion and misguide the cryptanalyst to obtain the cipher. At the receiving end, it uses artificial neural networks to obtain the original video. The elimination of the key exchange and the usage of artificial neural network for high security are the major strengths of the presented work.

II. ARTIFICIAL NEURAL NETWORKS

Artificial Neural networks (ANN)[3] 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. By choosing the suitable model and appropriately training the network, it can be used as a mapping function. Commonly neural networks are adjusted or trained, so that specific input leads to specific target output as shown in Fig 1

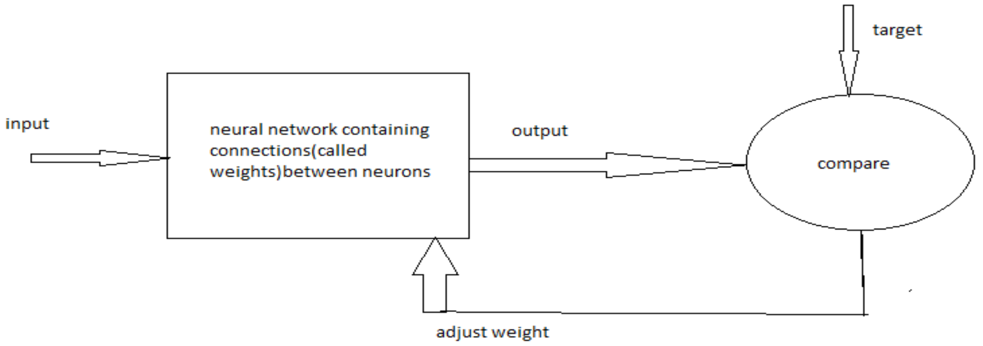

target
input
neural network containing connections(called weights)between neurons
output
compare
adjust weight

Fig 1. Neural network training

In the backpropagation neural networks [3], perceptron and other one layer networks are seriously limited in their capabilities. Hence multilayer Feedforward (MLFF) networks with Backpropagation learning and non linear node functions are used to overcome these limitations,. Multilayer feedforward network [MLFF] is made up of multiple layers. Thus, architectures of this class, besides possessing an input and an output layer also have one or more intermediary layers called hidden layers. Here the neurons of one layer are connected to the neurons of the next layer and so on till the output layer. The hidden layer aids in performing useful intermediary computations before directing the input to the output layer [3]. Backpropagation neural nets are those feed forward networks which use backpropagation learning method for their training. The training of a network by back propagation involves three stages: the feed forward of the input training pattern, the calculation and back propagation of the associated error, and the adjustment of the weights. Once the process converges, the final weights are stored in a file. After training, application of the network involves only the computations of the feed forward phase

III. SYSTEM DESIGN

Fig 2 depicts the schematic diagram of the presented work.

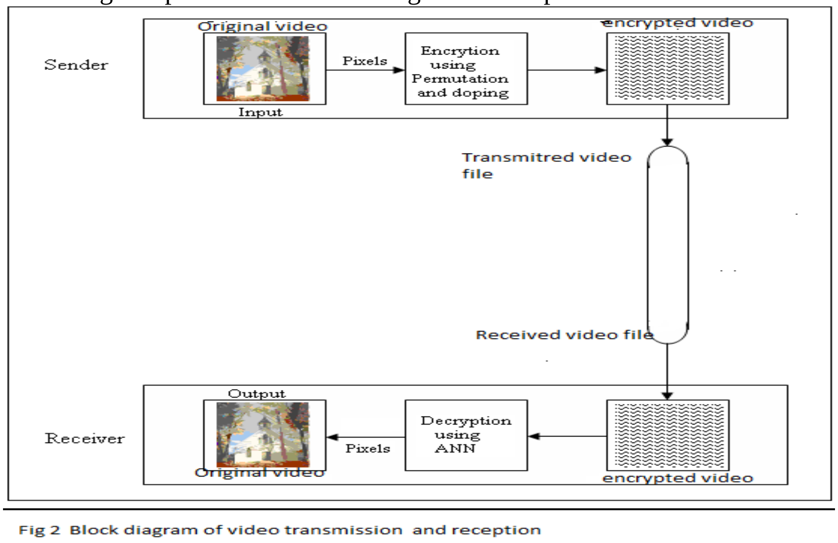


Fig 2 . Block diagram of video transmission and reception

System designed can be split into two modules-encryption and decryption. Whenever the sender wishes to send video, he feeds the video file to be sent to the encryption module. The video file is encrypted in the encryption module. At the receiving end the user in the remote system decrypts the video data by feeding the received data to the decryption module using artificial neural networks.

A. *Encryption Module*

The image to be encrypted is read pixel by pixel and transformation is done on these pixels using permutation, substitution and impurity addition. Two levels of encryption are used to obtain high level of image encryption.

Step1: Get the pixel value of the video file.[01000011] [67]
Step2: Divide the pixel byte value into upper and lower nibble [0100 and 0011].
Step3: Exchange the nibbles and concatenate to form a byte [00110100].
Step4: Calculate the impurity by EX-ORing the original msnibble and lsnibble ,[0111].

Step5: shift the bits of impurities by 5 bits to right. Now we get 9 bit number[011100000]

Step6: EX-OR the results of step3 andstep5[011010100]=212.
Step7: Add impurity to the obtained result in step 6.Impurity Value chosen is 117,[212+117].

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

Addition of two columns:
Step9: Additional two columns are added and the value of 117 is added to the first new column and 627 is added to the second new column. This is required for the normalization of the matrix.

Second level encryption:
Step10: Add another level of impurity to the resultant matrix obtained in step9 such that impurity changes with respect to the position of the pixel.

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

SAMPLE FIRST LEVEL ENCRYPTION RESULTS

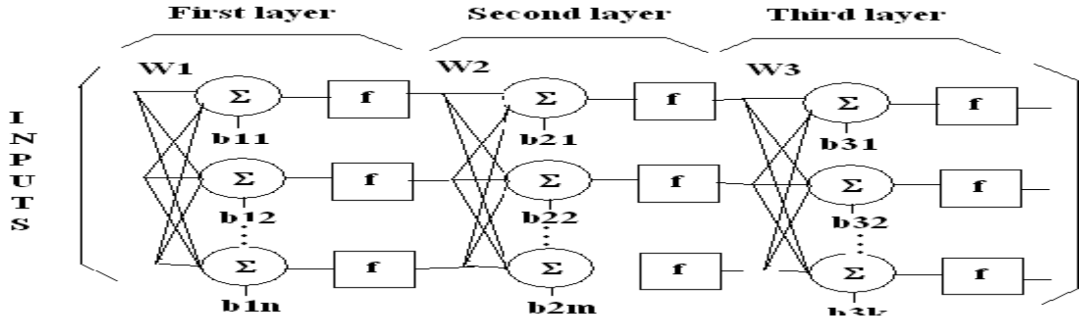
Original Pixel Value	Pixel Value after 1st level Encryption
1	165
6	277
45	473
67	329

Table II shows the transformation of the sample pixel values after second level of encryption.

Pixel position	Original pixel value	Pixel value after 1st level of encryption	Pixel value after 2nd level of encryption
(1,1)	12	437	537
(4,68)	12	437	708
(10,34)	12	437	1050
(15,29)	12	437	1335
(19,8)	12	437	1563

B. *Decryption Module*

At the receiver end decryption is achieved using an artificial neural network [3]. The neural network is trained for standard mapping value and the weights and biases are stored before applying input to it. MATLAB's neural network tool box is used for training and implementing.



Wi-weight matrix of the ith laye
F-activation function
Bij-biasis of jth neuron in ith layer

Fig 3. Block diagram of 3 layer back propagation net

The system is designed for three layers-input, output and hidden layers. The input and output have only one neuron and hidden layer has 695 neurons. Large number of neurons is required to achieving high security. The decryption is achieved in three steps [4][5][12]. During the first step, the impurity which was varying with respect to position of pixel is removed. In the second step, the additional columns from the matrix which were added during the encryption is deleted [6]. During the third step, the received video data and weights which were stored after the training are used to stimulate the network. The output of this stage is the recovered video.

IV RESULTS AND DISCUSSION

The result of the frame of video encryption and decryption module are shown in Fig4 and Fig5

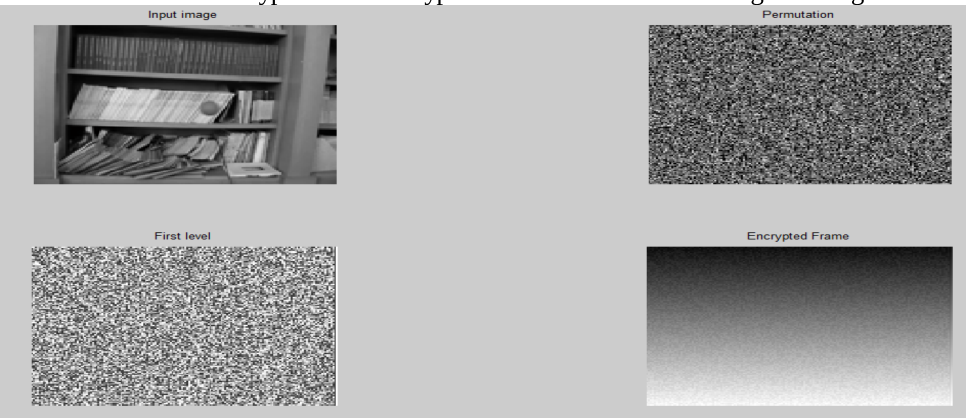


Fig 4. Output of the encryption module

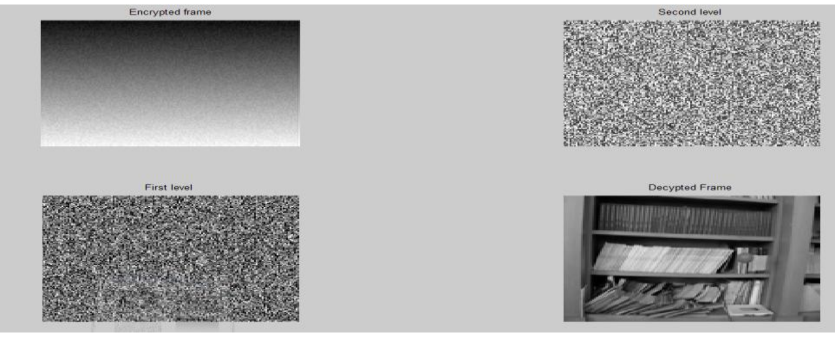


Fig 5. Output of decryption module

A. The need for two level of encryption

As already mentioned there are two level of encryption in the encryption module. It is required, because, for some of the images, a sample of which is shown in Fig 6, 1st level of encryption does not suffice. From the fig it is very clear that although the intensity of pixel has changed drastically, the picture is still in understandable form.

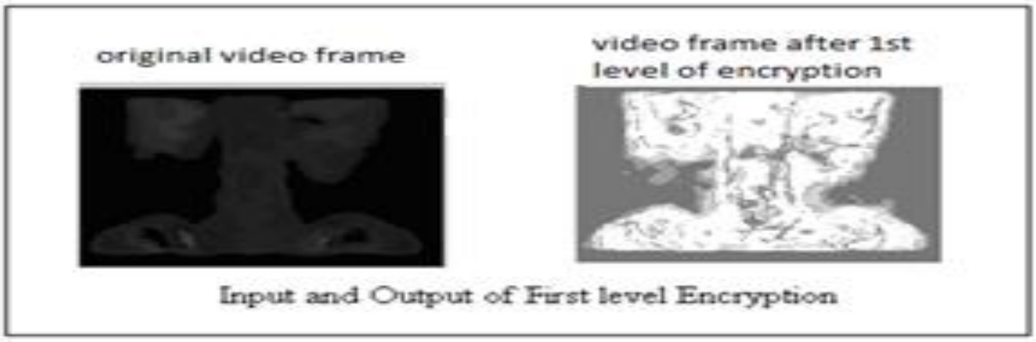

original video frame
video frame after 1st level of encryption
Input and Output of First level Encryption

Fig 6 input and output of 1st level encryption

The reason behind this is that, although the pixel value changes after 1st level of encryption all the pixels with same original value will have the same encrypted value, because of which intensity changes but image can be still visible.

To overcome this problem 2nd level of encryption is used. During the 2nd level encryption the impurity changes with respect to the pixel position (shown in table 2), it means pixel with same original value will have two different values after the second level of encryption depending on the pixel position. The output after 2nd level of encryption is as shown in Fig 7

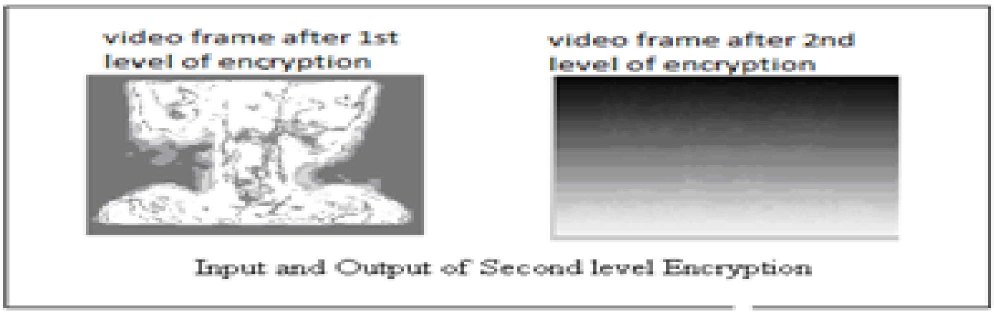

video frame after 1st level of encryption
video frame after 2nd level of encryption
Input and Output of Second level Encryption

Fig 7 input and output of 2nd level encryption

B. Need for normalization

As mentioned earlier ANN is used for decrypting the video. ANNs require training before they are used for any application. The results of training were not converging for the given input data set having 256 values. This problem was solved by the normalization of the input data. Normalization is the process of transforming the data set to the values ranging from -1 to 1.

C. ***Requirement of Additional Two Columns during Encryption :***

The image matrix was treated as a series of vectors (one row as one vector input) while simulating the network. Thus it became mandatory to have minimum and maximum pixel values in each row for achieving accurate normalization of the vector.

IV. PERFORMANCE ANALYSIS

A. Network Performance:

The training of the ANN is done using the function available in MATLAB’s neural network tool box [6][7]. It updates weight and biase values. It uses the heuristic method based on the standard numerical optimization method. The accuracy of the network has been found very high.

Table III provides the network performance analysis

TABLE III
NETWORK PERFORMANCE WITH VARIATIONS IN PERFORMANCE GOALS

Sl.No	Performance goal set	No of epochs	Time required in seconds	% error
1	0.1	1	06.10	92
2	0.01	4	10.94	41
3	0.001	4	34.41	7
4	0.0001	5	52.01	1
5	0.00001	7	59.00	0
6	0.000001	11	104.63	0

B. Application Performance

The presented work has been tested with many samples of avi files .Accuracy has been found to be very high. Table IV shows encryption and decryption time for the video.The decryption process was much slower than the encryption process. It is because of the fact that the simulation of the network during decryption process is done for each of the row separately.

TABLE IV ENCRYPTION AND DECRYPTION TIME

Sl.No	Video frame size in pixels	Encryption time in Seconds	Decryption time in seconds
1	256x256x1	0.002254	0.804936
2	256x256x3	0.016754	2.377046

V. Conclusion

The presented work discusses a novel neural network approach for video encryption and decryption. In order to make the decryption difficult for eavesdropper, a random algorithm has been used for encryption. Using neural network at the receiver end has made random encryption possible at the senders end. Also need of key exchange prior to data exchange has been eliminated. The accuracy of the system has been found very high. The presented work thus provides flexible, accurate and secure video transmission and reception.

REFERENCES

[1] unukur,R.K/;gnanam V,"neural network based decryption for random encryption algorithm ".
[2] Liew Pol Yee De Silva L.C,"application of multilayer perceptron network as a one way hash function".
[3] Khalil Shihab,"a backpropagation neural network for computer network security"
[4] Francia G.A,"applied image processing to multimedia information security".
[5] William Stallings," networksecurity essentials,applications and standards"
[6] Su S"Lin,A"design and realization of new choaticneural encryption\decryption network"
[7] http://en.wikipedia.org/wiki/Authenticated_encryption
[8] http://en.wikipedia.org/wiki/Authenticated_encryption
[9] http://en.wikipedia.org/wiki/Video
[10] Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo, "Recent Advances in Multimedia Information System Security," International Journal of Computing and Informatics, Vol. 33, No.1, 2009, pp. 3-24.
[11] Shiguo lian, Multimedia Content Encryption: Algorithms and Application, CRC Press, 2008.
[12] B. Furht, D. Socek, and A. M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques," Multimedia Security Handbook, CRC Press, 2005.
[13] ISO/IEC 13818:1996, Coding of Moving Pictures and Associated Audio (MPEG-2); Part 1: systems, Part2 : video.
[14] Mitchell J. L., Pennebaker W.B., fogg C.E. and LeGall D.J. MPEG Video Compression Standard, Chapman & Hall, 1996.
[15] ITU-T Rec. H.264/ISO/IEC 11496-10. Advanced Video Coding. Final Committee draft, Document JVT-E022, 2002.
[16] Iain E G Richardson. H.264/MPEG Part10, 2002. Available: http://www.vcodex.com.
[17] NIST: Data Encryption Standard, FIPS 46-3, 1999.
[18] NIST: Advanced Encryption Standard, FIPS 197, 2001.
[19] Adam J. Slaggel. Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm. Available:http://eprint.iacr.org