Scan Methodology Based Video Encryption and Decryption Scheme using Scrambling and Multilayer Technique

Vinay Kumar Soni[1], **Prashant Puri Goswami** [2]

[1, 2]Central College of Engineering and Management, Raipur, Chhattisgarh, India

Abstract: ***Security of data is very important issue for today's multimedia communication. The growth in communication and computer technologies, a lot of digital data communication through interment and teleconferencing applications is carried out. Such applications require highly secured. To provide security encryption is one of way. This paper provides a new approach for enhanced video encryption using SCAN methodology and multilayered approach. Also scrambling technique is done for the frames to make more complicated encryption for better security. The implementation and testing of the proposed method using different sample video inputs and our experimental results and security analysis are given and advantages of the new proposed algorithm is also found. The method is fast and security is also enough to be comparable to other methods. This method can be used in very broad range of industrial applications.***

Keywords: SCAN Methodology, Scrambling, Multilayer encryption, DNA encoding, Histogram, Entropy, Correlation.

1. Introduction

Securing the multimedia data has become very important issue in today's digital data transmission. Now a day's internet and other transmission media involve lot of video files to be transferred between end users. In such cases several confidential data is also transferred like military or medical applications. So encryption is done to ensure security. Video encryptions have applications in the field of multimedia systems, medical imaging, and military communication. There are several image and video encryption methods. The popular encryption schemes are DES, AES, RSA, 3DES, RC5. The video files have larger length and the time to encrypt video file may be considerably large. The main advantage of the encryption method presented here as compared to other methods is that this scheme is fast and the security is also high.

The experimental results are also given to evaluate the performance of the proposed scheme. The results show that the scheme is considerably fast and it can be applied for the different applications in securing video data.

.

2. The Proposed Methodology of Video Encryption and Decryption

The video encryption through this proposed scheme includes following steps:

Step 1: Reading input video
The very first step to encrypt any video is to read it from the specific location. The location may be any directory which will contain the video to be encrypted. In this dissertation work our MATLAB program will read video files from any directory or any folder which is in the hardware or computer.

Step 2: Frame Extraction
As any video is a combination of several image frames so to process any video involves dealing with the image frames of that video. MATLAB command can find the number of frames of any video. So this image frames can be extracted using the MATLAB inbuilt ability to find and store the frames. This work will first extract the frames and then stores those frames into a specified folder in the same directory from which the original video file was read. The video having different formats will have different number of frames.

Step 3: Frame Scrambling
Scrambling refers to change the position of image frames.

Step 4: Encryption stage 1
In this step the frames obtained through shuffling will be encrypted using SCAN algorithm. This step involves continuous encrypting all the frames of video one by one and converting them into cipher image frames.

Step 5: Encryption stage 2
Step 5 is same as step 4. In this Step the output obtained in previous step will be taken as input and then these frames will be encrypted through same SCAN algorithm.

Step 6: Encryption stage 3
This is the third level encryption performed by the methodology used to increase the security of data to be encrypted. In this step the output of previous step will be taken as input image frames and then these frames will be encrypted using SCAN algorithm adopted in previous two steps.

Step 7: Video Formation through frames
The cipher image frames are converted into a video format in this step. This is the last task performed by the scheme.

The encrypted video can be recovered into original video through the decryption scheme which involves reverse process of above steps.

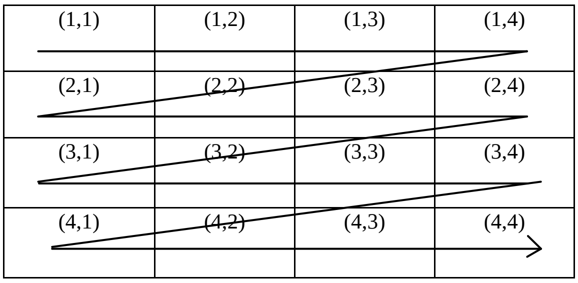
3. The Scan Methodology Encryption

SCAN methodology is basically an image preprocessing tool, committed to generate 2D scanning patterns. The path for scanning the image is a random code form and by providing the pixels order along the scanning path. It can be noted that scanning path of an image is simply a sort in which each pixel of the image is accessed just once. Such the encryption also involves the requirement to set undisclosed scanning paths. As a result, this encryption needs a methodology to specify and generate a bigger number of wide varieties of scanning paths effectively [7].

Following figures explain concept of pixel scanning.

(1,1)	(1,2)	(1,3)	(1,4)
(2,1)	(2,2)	(2,3)	(2,4)
(3,1)	(3,2)	(3,3)	(3,4)
(4,1)	(4,2)	(4,3)	(4,4)

Figure 1: A basic 4X4 array

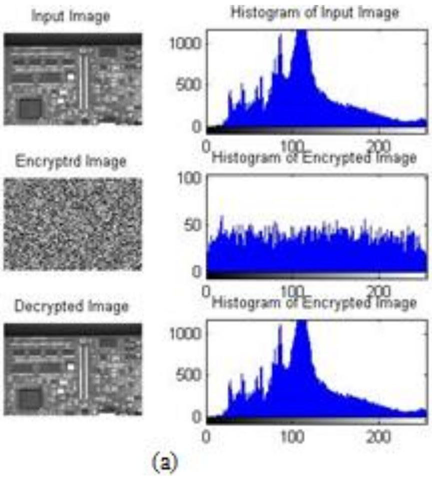


(1,1)	(1,2)	(1,3)	(1,4)
(2,1)	(2,2)	(2,3)	(2,4)
(3,1)	(3,2)	(3,3)	(3,4)
(4,1)	(4,2)	(4,3)	(4,4)

Figure 2: An example of raster scanning

4. Experimental Results

The scan methodology based video encryption scheme is tested through MATLAB 2014 software and the histograms of original video frame, encrypted video frame and decrypted video frame are plotted. The correlation plot is also obtained which is shown in the figure below:



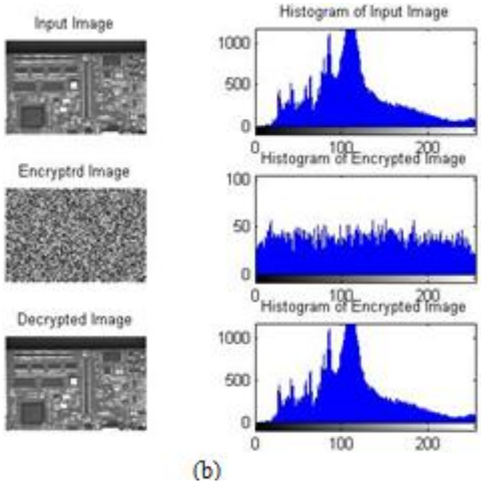


Figure 3: Histogram of input image frame, encrypted image frame and decrypted image frame.

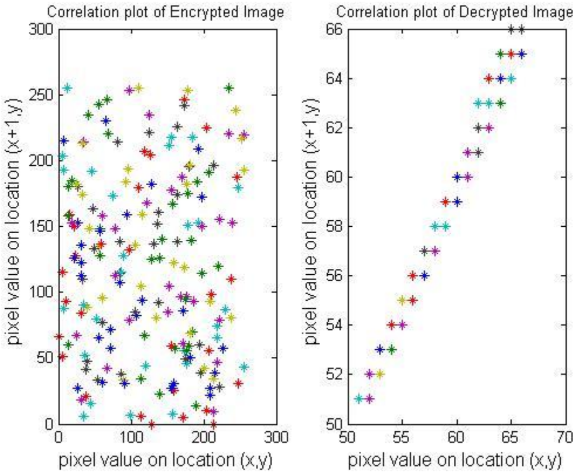


Figure 4: Correlation plot obtained through experiment

5. Conclusion

This multilayer and frame scrambling based video encryption technique is found to be enough secure for digital data transmission. The correlation is also good. The encryption time and decryption time is also moderate. So in overall performance matter this scheme can be used to encrypt video.

References

[1] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar, "Fast and Secure Real-Time Video Encryption", Sixth Indian Conference on Computer Vision, Graphics & Image Processing, IEEE, pp 257-264.

[2] 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, March 2013, pp 1-5.

[3] T. Pradeep Pai, M.E. Raghu and K. C. Ravishankar, "Video Encryption for Secure Multimedia Transmission - A Layered Approach", Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference, IEEE.

[4] M Yang, N. Bourbakis and Shujun Li, “Data-image-video encryption”, IEEE Potentials (Volume: 23, Issue: 3, Aug.-Sept. 2004).pp 28-34.

[5] Cuixia Li, Yang Zhou ,Y inghua Shen and Cheng Yang, “A Video Selective Encryption Strategy based on Spark”, IEEE 2016, pp 957-960.

[6] Alvin Mustafa and Hendrawan, “Calculation of Encryption Algorithm Combination for Video Encryption using Two Layers of AHP”, IEEE 2016, pp 1-7.

[7] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani, “A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No.5 (2013), pp.275-290.

[8] Parameshachari B D, K. M. Sunjiv Soyjaudah and Sumithra Devi K A, “Secure Partial Image Encryption Scheme Using Scan Based Algorithm”, International Journal of Advances in Engineering & Technology, Mar. 2013, pp 264-273.

[9] Mr. Ravi Mohan, Hira Lal Dhruw and Raghvendra, “An Effective Image Encryption Based on the Combination of Scan and Elgamal Method”, International Journal of Engineering And Computer Science ISSN:2319-7242, Volume 4 Issue 5 May 2015, Page No. 11793-11796.

[10] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, “A Survey On Different Image Encryption and Decryption Techniques”, International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116.