Secure Multimedia Data Transmission Using MATLAB

K.Sathyamoorthy, S.Balaji, S.Manoj, M.I.Mohamed Sabir

Abstract— **This paper approaches security applications for digital image and video processing. The techniques involve Video Compression, Elliptical Curve Cryptography Encryption Algorithm followed by Image Interleaving, and Pixel Integration to generate integrated multi-video. User can select one of the several videos displayed simultaneously with a unique key for each video. With the key specifically generated for the video, the original video is decrypted from multiple image/videos.**

Index Terms— **Elliptical Curve Cryptography ;Encryption; ; Image Processing; Pixel Integration; Security; Image Interleaving Multi view Systems**

I. INTRODUCTION

With the rapid growth of multimedia technology [3] many public, private and defence sectors across the world are using this technology for data transmission. There are potential privacy threats and risks during video transmission and hence the threats and risks should be eradicated. One possible way to protect multimedia data transmission is to prevent unauthorized entry. Another easy security approach is to encrypt the complete data with a cryptographic algorithm [1], [2] such as Advanced Encryption Standard or Data Encryption Standard. Generally, multimedia is a combination of different content forms such as text, audio, images, video and interactive content. With the advancement in wireless technologies and limited processing power, memory, and bandwidth, and is difficult to handle the heavy encryption processing load. Digital video [3] is a representation of a real-world visual scene or a natural, which sampled temporally and spatially, whereas video coding is the process of compressing and decompressing a digital video signal. Image or video transmission requires compression to decrease the size of data for fast and secure transmission and encryption [1] is used to protect the use of data against unauthorized access.

Compression [11] is the process of encoding a file in such a way that it consumes less space than the original file and is easier to transmit over the network. Overall, a encryption algorithm should provide sufficient security, high computational efficiency imposes little impact on the compression efficiency.

Data transfer in wireless mobile systems and limited processing power, memory, and bandwidth, and is rarely able to handle the heavy encryption processing load. Therefore, taking into consideration the specific characteristics for resource-limited systems, new video encryption algorithms need to be developed. Real world applications, a video encryption algorithm must consider various parameters like security, computational efficiency, compression efficiency and so on. Video applications require high levels of security. For example, for military purposes or transmitting satellite images, high level of security is required to completely prevent unauthorized access, whereas for Video on Demand, low security will be fine. Computational efficiency means that the encryption or decryption process should not cause too much time delay. For real- world applications, an encryption algorithm must consider various parameters like security, computational efficiency, compression efficiency and so on.

Video compression is a process of encoding a video file and removing repetitive images, sounds and scenes from a video. Video compression will remove all such data to reduce the video file size. It also eliminates redundant and non-functional data from the original video files.

Here we present, compression[4] and encryption [5] [6] as first stage and then process by image interleaving along with pixel integration method in order to enhance security. In our proposed method, nine sample input videos are taken and 3 frames per video are extracted for integration. These frames are converted as RGB with a size of m*m pixels are taken with block size of 4*4 is applied to test the performance. First compressing with H.264 standard and encrypting with ECC [2] then Interleaving with Pixel based Integration to generate multi video, decryption process is done by selection of the key in reverse order. The compression ratio of each layer,entropy and correlation are calculated and evaluated.

II. RELATED WORK

Ahmed Bashir Abugharsa et al. [13] proposed an algorithm for encryption for images which is based on the rotation. First dividing the input image into six sub-images and then these sub images are divided into small blocks and attached to the faces of magic cubes.

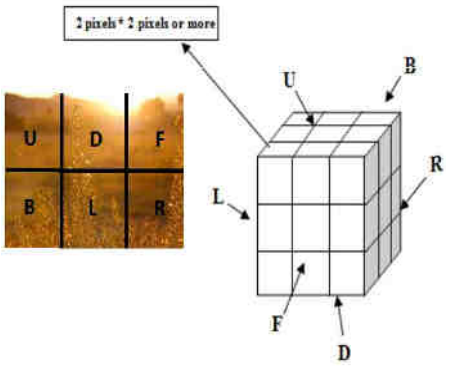

Fig. 1. Six sub-images of magic cubes

Manuscript received March 06, 2019

K.Sathyamoorthy, Assistant Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India

S.Balaji, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India

S.Manoj, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India

M.I.Mohamed Sabir, Department of Computer Science and Engineering, Panimalar Institute of Technology , Chennai, India

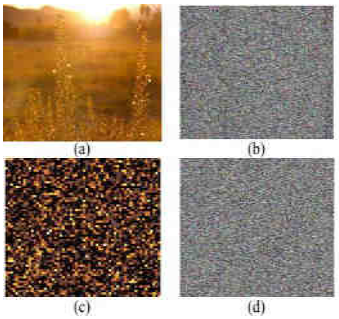

Fig. 2. (a) Input Image. (b) Encrypted image using AES (c) Rotation image. (d) Encrypted Image using Intergration Technique.

A.Alfalou et al. [7] proposed simultaneous compression and encryption method which is based on optical image set. The major strength of the method is in its robustness against various known-plain text attacks making this algorithm appealing for colour video images and the main drawback is it can be used only for optical setup images not for other images.
Daniel Schonberg et al. [11] proposed a framework on compression of encrypted images and video sequences.
Laiphrakpam Dolendro Singh et al. [12] proposed an algorithm for image encryption using ECC based on pixel grouping.The group of pixels will reduce the computation and are transformed into a big integer.These big integer values are paired and given as input in ECC operation.
Zhi-Hong Guan et al. [6] proposed a method based on shuffling the position and changing the image pixel grey values. These values are combined to camouflage the relationship between the cipher and plain image.
Guiliang Zhu et al. [10] proposed encrypting the image based on pixels by applying ECC. First, scrambling the image pixels, through the method of watermark. Getting final encryption image is by camouflaged image to vision.
Rogelio Hasimoto Beltran et al. [14] proposed an interleaving technique,the de-correlation process is applied to pixel or co-efficient level in the compressed domain.
Frank Dellaert et al. [15] proposed algorithm based on image tracking, which relies on the selective integration of a small subset of pixels that contain a lot of information about the state variables to be estimated.

III. Proposed Method

A. JPEG Compression

JPEG image frame consists of three 2-D patterns of pixels, one for luminance and two for chrominance. Because high-frequency color information is less sensitive to human eye, JPEG calls for the coding of chrominance (color) information at a reduced resolution compared to the luminance (brightness) information.
The input images are layered as RGB.JPEG compression is applied to all image layers individually for better performance. The JPEG image compression [12] technique consists of 3 functional stages.

1. Select RGB image.
2. Using discrete cosine transform (DCT) transformation of a blocked representation of the RGB Image data to a frequency domain representation.
3. 3.Quantization of the blocked frequency domain data per a user-defined quality factor.

B. H.264 Compression

H.264[4] defines a method of coding video that can give better performance than any of the preceding standards. It compresses video into a smaller space, which means that a compressed video clip takes up less storage space compared to older codecs and less transmission bandwidth. Generally, standard definition is available in DVD-video format, capable of supporting only a single movie where as High definition videos with H.264 compression, to record hours of video on a memory card and to deliver video streaming over in online.

First the given input videos are converted into frames in RGB format.JPEG compression is applied to all image layers individually for better performance. H.264 video compression [12] technique consists of 4 functional stages.

1. Converting the video into frames.
2. RGB image format.
3. Using discrete cosine transform (DCT) transformation of a blocked representation of RGB data to frequency domain representation
4. Quantization of the blocked frequency domain data per a user-defined quality factor.

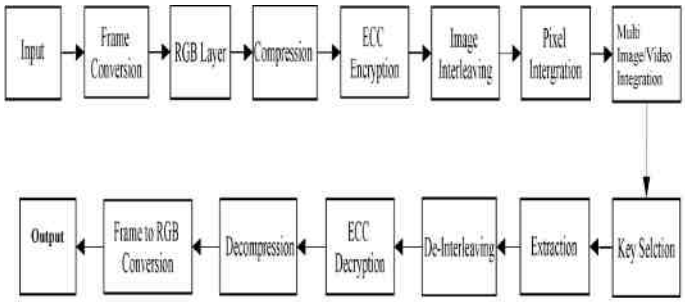

Fig. 3. Block Diagram of Proposed System

C. Eliptic Curve Cryptography

Elliptical curve cryptography (ECC) [8] [9] is based on public key function based on elliptic curve theory that can be used to create smaller, faster, and efficient cryptographic keys. Key generated through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. ECC encryption is based on encrypting the image intensity and thus converting it into a new intensity. This new intensity is decrypted to obtain the original intensity.

- First find the intensity I of the RGB frame from the image intensity matrix.
- Convert the intensity of the frame I into an elliptic curve point E using Mapping-1
- Elliptic curve point from Mapping-1 Encrypted to a new point(E').
- The new point (E') is converted to a corresponding integer M, using Mapping-2.
- This integer M is used to calculate the new encrypted intensity I.
- The decryption is done in reverse process of encryption.

D. Image Interleaving

Encrypted RGB frames are divided into small blocks [16], [17] as 4*4. Small sub-blocks give better encryption. These sub-block images are interleaved column wise. The number of sub-block pixel values in each block is fixed for a given

interleaver. Applying block based interleaving by selecting the initial location randomly. Interleaving scheme is divided into column-wise and row-wise interleaving randomly. Then assign the value of seed as column-wise seed and row-wise

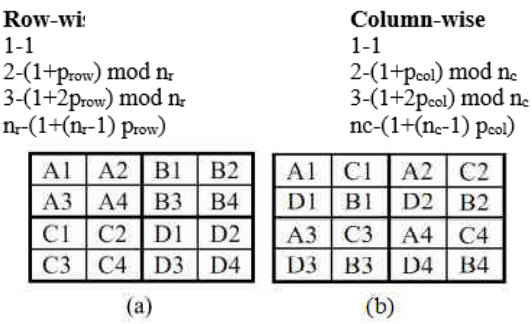

Fig. 4. (a)Block interleaver input sequence(b) Proposed block interleaver sequence

E. Pixel Integration Technique

After interleaving, pixel integration for all RGB frames is processed. Here the input images are represented in pixel value format for RGB layers ranging from 0-255. Table for pixel integration is formed for each layer separately in row wise and column wise, assigning the input frames are taken as row wise

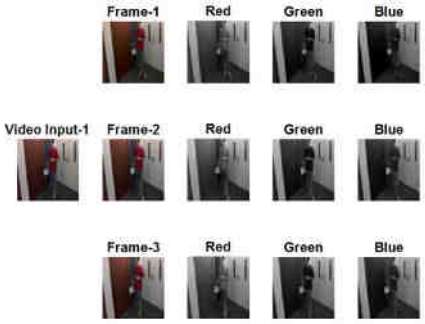

Fig. 5. Input Video to Frame Process

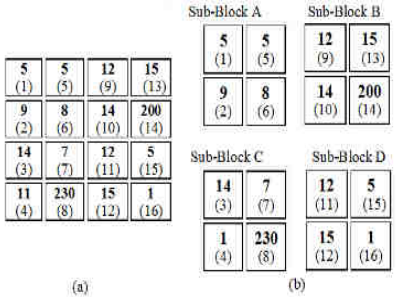

Fig. 6. (a) Input Frame Pixel value for 4*4 Size (b)Sub-blocks value for (a)

pixel values and column wise with starting value as 1 to ending value 266. Here we consider the colour depth of each frame as 16-bit and thus choosing the sub-blocks as 4x4.

Considering the RGB input frame as shown in fig.6 with size of 64x64 and dividing into 4x4 blocks as shown in fig.7 will produce 16 blocks which are represented as A, B, C, and D. A(i,j) is first sub-block of A, where i is pixel value and j is index location of pixel. Pixel integration table is created as shown in fig.8.

Assign the pixel index to the corresponding pixel value for the first block of all RGB input frames and then second block of every frames. This process is continued for all blocks of input frames.

16-bit colour representation is used in case of multiple indices with the same pixel value in a block. The value is calculated by representing them in the 16-bit colour RGB palette with reference to fig.5, and finding their corresponding value as shown in fig.9.

This process is repeated for all the blocks of the input RGB frames individually. By summing all the RGB pixel indices value for each pixel value for all the frames, Image Integration is done.

Image/Pixel	1	2	3..	10
1	4,16			
2	9			
3				
4				
5	1,5,15			
6				
7	7			
8	6			
9	2			
10				
11				
12	9,11			
13				
14	10,3			
15	13,12			
.				
.				
200	14			
230	8			
256				

Fig. 7. Pixel Integration Table with values

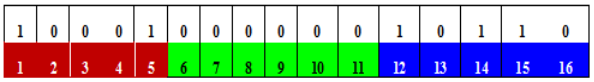

Fig.8. Multiple values location in RGB format

IV. Experimental Details And Results

The proposed method has been implemented in MatLab 8.6 in windows environment with a system configuration of I7 Intel Pentium VI Generation processor with 16 GB RAM. The proposed algorithm has been tested with various images. A good quality encryption algorithm should be strong against all types of attack. Another important factor that evaluates the efficiency of algorithms is measuring the amount of time required for overall process.

A. Correlation Co-Efficient

The correlation [18] is calculated between input image and encrypted image. The correlation coefficient values ranges from -1.0 to 1.0.If the correlation value of encrypted image is equal to 0 or very near to 0 then the encrypted image and original image are totally different. A mistake or wrong encryption has been made when the calculated correlation is greater than 1.0 or less than -1.0. A negative correlation is indicated when correlation value is -1.0 , while perfect

positive correlation is indicated with value of 1.0. The equation (1) shows correlation coefficients calculation,

$$Cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - D(x)) \quad (1)$$

B. *Information Entropy*

Entropy [19] is a quality of an image, i.e. the amount of information which must be coded for by a compression algorithm. Low entropy images have very little contrast and large runs of pixels with the same or similar DN values whereas higher entropy images such as an image of heavily cratered on the moon have a great deal of contrast from one pixel to the next. The equation (2) is used to calculate entropy of the image.

$$H = -\sum_{i=1}^{n} p_i \times log_2\, p_i \quad (2)$$

C. *Compression Ratio*

Compression ratio is the process of reducing the size of a data file. In transmission of data, it is called source coding in opposition to channel coding. Compression is useful because it reduces resources required to transmit and store the data. Compression ratio is called with the below formula,

$$\text{Compression Ratio} = \frac{\text{Uncompressed Data Rate}}{\text{Compressed Data Rate}}$$

D. *Result Analaysis*

High compression ratio with entropy value and low correlation values provides good encryption. The time taken for video encrypting and video decrypting with key is 197.1251 seconds. Results for the compression ratio,correlation and the entropy values for image and video inputs are shown in Tables I-V.

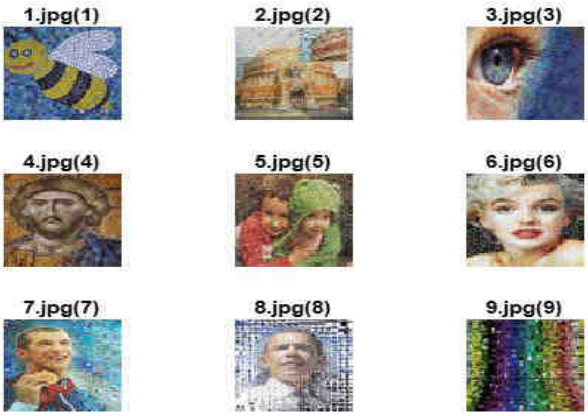

Fig. 9 Mosaic Input Image

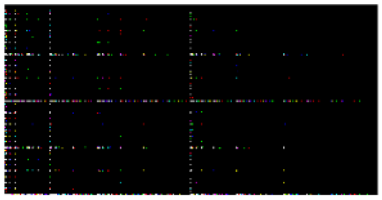

Fig. 10. Pixel Encrypted Image

Fig.11. Decrypted Image with Key No.4

Table 1 Entropy and Correlation Value For Texture Image

IMAGE NAME	ENTROPY	CORRELATION
1	1.7015	0.0347
2	1.7744	0.0522
3	1.8929	0.0546
4	1.8898	0.0506
5	1.8752	0.0438
6	1.8648	0.0470
7	1.7461	0.0470
8	1.5968	0.0493
9	1.6002	0.0442

Table 2 Compression Ratio for Mosaic image

IMAGE NAME	ENTROPY	CORRELATION
1	1.7015	0.0347
2	1.7744	0.0522
3	1.8929	0.0546
4	1.8898	0.0506
5	1.8752	0.0438
6	1.8648	0.0470
7	1.7461	0.0470
8	1.5968	0.0493
9	1.6002	0.0442

Fig. 12. Input Videos with Frame-1

Fig. 13. Input Videos with Frame-2

Fig. 14. Input Videos with Frame-3

Fig.15. Encrypted Video

Fig.16. Decrypted Video with Key No.4

Fig.17. Decrypted Video with Key No.7

Table 3 Compression Ratio, Entropy and Correlation Value for Input Video-Frame-1

Image No	Compression Ratio			Entropy Value	Correlation Value
	R	*G*	*B*		
1	0.5469	0.5625	0.5625	0.0537	-0.0130
2	0.6875	0.6719	0.7188	0.0009	-0.0065
3	0.3906	0.4063	0.3906	0.0001	0.0061
4	0.4844	0.5625	0.5313	0.0005	-0.0014
5	0.5781	0.5469	0.5469	0.0000	0.0346
6	0.5313	0.5313	0.5313	0.0253	-0.0240
7	0.3906	0.4844	0.5000	0.1739	-0.0050
8	0.5469	0.5781	0.5938	0.3185	-0.0071
9	0.5000	0.5625	0.5469	0.0158	0.0320

Table 4 Compression Ratio, Entropy and Correlation Value for Input Video-Frame-2

Image No	Compression Ratio			Entropy Value	Correlation Value
	R	*G*	*B*		
1	0.5469	0.5625	0.5625	0.5459	-0.0129
2	0.6875	0.6719	0.7188	0.6875	-0.0065
3	0.3750	0.3750	0.3750	0.0001	0.0060
4	0.5000	0.5938	0.5313	0.0005	-0.0015
5	0.5781	0.5469	0.5469	0.0000	0.0343
6	0.5313	0.5313	0.5313	0.0252	-0.0238
7	0.3594	0.4688	0.5000	0.1739	-0.0050
8	0.5469	0.5781	0.5781	0.3186	-0.0071
9	0.4844	0.5469	0.5156	0.0158	0.0317

Table 5 Compression Ratio, Entropy and Correlation Value for Input Video-Frame-3

Image No	Compression Ratio			Entropy Value	Correlation Value
	R	*G*	*B*		
1	0.5469	0.5625	0.5625	0.0537	-0.0128
2	0.6875	0.6563	0.7031	0.0010	-0.0065
3	0.3594	0.375o	0.3594	0.0001	0.0060
4	0.5156	0.5938	0.5313	0.0005	-0.0015
5	0.5625	0.5469	0.5625	0.0000	0.0341
6	0.5313	0.5313	0.5313	0.0252	-0.0237
7	0.3281	0.4844	0.5000	0.1739	-0.0049
8	0.5469	0.5781	0.5781	0.3186	-0.0071
9	0.4688	0.5625	0.5625	0.0158	0.0315

CONCLUSION

Security has become highly important since the communication by transmitting of digital products over the network occur very frequently. Compression and Encryption with pixel integration method is approached in this paper. First, compressing the input video frame and encrypting along with the interleaving is done, then through the method of pixel integration increasing the difficulty of decoded. At last, a camouflaged all the input videos, getting the final encryption video. Experimental result shows good performance with low correlation, high entropy and compression ratio which shows that the pixel-based algorithm is highly secure. With this approach, it is also able to encrypt large volume of data more securely and simultaneously. Our new approach is expected to be useful for transmission applications and real time system.

REFERENCES

[1] Christof Paar and Jan Pelzl," Understanding Cryptography: A Textbook for Students and Practitioners," Springer, 2010,pp.1-24

[2] Darrel Hankerson , Alfred J. Menezes and Scott Vanstone," Guide to Elliptic Curve Cryptography," Spinger,2004

[3] Chris Solomon and Toby Breckon,"Fundamentals of Digital Image Processing," Wiley,2010, pp1-18

[4] Iain E. Richardson,"THE H.264 ADVANCED VIDEO COMPRESSION STANDARD",Willey,2010,pp 81-98

[5] I. Ozturk and I. Sogukpinar,"Analysis and comparison of image encryption algorithm,"Journal of transactions on engineering, computing and technology, pp.38, Dec 2004.

[6] G.Zhi-Hong, H.Fangjun, and G.Wenjie, "Chaos-base, Image Encryption Algorithm,"Elsevier, pp. 153-157, Oct 2005.

[7] A.Alfalou, C.Brosseau,and N.Abdallah," Simultaneous compression and encryption of color video images",Elsevier, pp.371-379, Oct 2014.

[8] Moncef Amara and Amar Siad,"Elliptic Curve Cryptography and its applications ",Systems, Signal Processing and their Applications (WOSSPA),pp 247-250,May 2011.

[9] Kamlesh Gupta and Sanjay Silakari,"Performance Analysis for Image Encryption Using ECC",Computational Intelligence and Communication Networks (CICN),pp 79-82,Nov 2010

[10] Guiliang Zhu ,Weiping Wang ,Xiaoqiang Zhang and Mengmeng Wang , "Digital Image Encryption Algorithm Based on Pixels",IEEE 2010.

[11] Daniel Schonberg,Daniel Schonberg ,Chuohao Yeo and Kannan Ramchandran,"Toward Compression of Encrypted Images and Video Sequences",IEEE 2010.

[12] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh,"Image Encryption using Elliptic Curve Cryptography"Eleventh International Multi-Conference on Information Processing,pp 472-481,2015.

[13] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush,"A Novel Image Encryption Using an Integration Technique of Blocks Rotation Based on the Magic Cube and the AES

Algorithm," International Journal of Computer Applications, pp.38-45, March 2012.

[14] Rogelio Hasimoto-Beltran and Ashfaq Khichari,"Pixel Level Interleaving scheme for Robust Image Communication," Scalable and Parallel Algorithm Labs, University of Delaware, Newark, Oct 1998.

[15] Frank Dellaert and Robert Collins, "Fast Image-Based Tracking by Selective Pixel Integration,"Computer Science Department and Robotics Institute Carnegie Mellon University,Pittsburgh,Sep 1999

[16] Hanpinitsak and C. Charoenlarpnopparut,"2D Interleaver Design for Image Transmission over Severe Burst-Error Environment," International Journal of Future Computer and Communication, pp.308-312, Aug 2013.

[17] Shengyong Guan, Fuqiang Yao and Chang Wen Chen,"A novel interleaver for image communications with theoretical analysis of characteristics," Communications, Circuits and Systems and West Sino Expositions,IEEE 2002 International Conference (Volume:1), July 2002.

[18] Satoru Yoneyama and Go Murasawa, "Digital Image Correlation," Encyclopedia of Life Support Systems, Digit Imaging. 2008 Sep.

[19] Du-Yih Tsai, Yongbum Lee and Eri Matsuyama,“Information Entropy Measure for Evaluation of Image Quality", 2008 Sep.