International Journal of Engineering &Technology, 7 (4) (2018) 6167-6170

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.23127
Research paper



Enhancing the performance of video encryption used for security and privacy protection in secure multimedia transfer

Khattab O. Khorsheed [1], Omar G. Abood [2*], Shawkat K. Guirguis [2]

[1] Ministry of Education, General Directorate of Education in Kirkuk, Iraq
[2] Department of Information Technology Institute of Graduate Studies and Researches, Alexandria University, Egypt.
**Corresponding author E-mail: omar.ghazi88@yahoo.com*

Abstract

It is taken for granted that the techy core transfer has showed an upward indicator recently. Data exchanges could be a mutual subject over unsecure network, the matter that made the multi-media security an inevitable and crucial issue. Applications that require image and video processing became extremely popular in many fields, e.g. Medical imaging, manufacturing, and security systems. Real time image and video processing is considered a vital matter, since it requires high computations for a huge a video data and complicated process in return. Thus, to guarantee the confidentiality via the vulnerable network, along transmission, a video encoding is considered a priority. As a matter of fact, valid algorithms are subject for violating. However, our academic research tackles an up-to-date system for real time video encrypting by using pixel encryption. Pixel encryption thesis relays on shuffling and manipulating pixel values. According to unscrambled order generated, the position of pixel values is changed. All in all, decrypting to edit the initial video would be hold by rearranging the pixel values first, then manipulating them reversely for a recipient side.

Keywords: *Key Exchange; Pixel Shuffling; RGB Pixel Displacement; Video Decryption; Video Encryption.*

1. Introduction

Day after day, multimedia files are exchanged exponentially everywhere to communicate. Video transmission from sender to receiver should be in a secure way. And the prominent examples are video conferencing and digital video broadcasting. That urges for an inevitable solution for a safe transaction into a smart way. Encryption is for securing the transmission of videos. The data would be unreadable when encrypted. So far, many algorithms are assumed e.g.: RSA, Diffie Hellman, DES, AES etc. [1]. Most of them encrypt texts; however, they are limited as far as the feasibility is. The basic target of these lines for video encryption is to boost security in addition to reduce time complexity. Actually, there are many ways for video encryption; permutation encryption, selective encryption, fully encryption, RGB displacement …etc. [2]. Whereas right in here the adopted thesis for video encryption is reliable on many definitions, such as pixel values shuffling, and RGB displacement. The 2nd part contains the Literature Survey of our work. The detailed mechanism is described clearly in the 3rd part and result analysis is induced in the 4th part. Eventually, the conclusion is in 5th part.

2. Literature survey

In this section contains the Literature Survey of our work with a focus to RGB Color Model, Permutation-Based Encryption for Video Files, Fully Layered Encryption, Selective Encryption Technique, and RGB Pixel Displacement

2.1. RGB colour model

RGB stands for the 3 primary colors, red, green, and blue. The RGB is a color model in which red, green, and blue light are mixed into a way to stimulate a miscellaneous spectrum of shades [3]. The 3 colored light beams must be superimposed, to establish a color with RGB. Every ray color is entitled a color ingredient, all of them can have a chaotic concentration from fully off to fully on. In computers, the ingredient values are often stored as integer numbers at the range of 0 to 255, a range that a single 8-bit byte can afford. These are demonstrated as either decimal or hexadecimal numbers.

2.2. Permutation-based encryption for video files

A system [4] [5] that shuffles the video component in a way, that the attacker finds it challenging to guess the shuffled content. Either totally or partially, shuffling could be carried out. The permutation list serves as a clue in most algorithms. Eventually, this clue is used to retrieve the basic file. Therefore, it is substantial to attach this key as well.

2.3. Fully layered encryption

Layered Encryption is a technique in which the whole video content is first compressed. Then, it is encrypted by AES or DES algorithms. [6]. This methodology is not possible for real time encryption due to the increased time complexity. Moreover, there can be a loss of video quality according to this situation [7].

Copyright ©2018 Khattab O. Khorsheed et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2.4. Selective encryption technique

It overcomes the drawback of the total layered approach. In this technique, instead of encrypting the entire video content, a selected portion is merely encrypted. This cuts down the encrypting time and enhances as much security as possible. [8].

2.5. RGB pixel displacement

Along this system the numerical value of the RGB pixel is displaced from its original position. In this method, no change occurs into the file's size in the encrypting process. Whereas, pixel values undergo a reverse displacement [7][9].

3. Proposed algorithm

A multiple mode for video encryption which uses shuffling of pixel values and RGB pixel manipulation has been illustrated.

3.1. Encryption

The video is in AVI format. First of all, fetch the resolution of the primitive frame (image) captured. After that and since the target is to permute the pixel values of every single frame, we need a random sequence. The random sequence should be as accurate as the number of elements in a single frame. The next step is pixel displacement. Graphics file formats store RGB images as 24-bit images. Each of the Red, Green and Blue components is of 8-bit. Their values range from 0 to 255. In order to manipulate each pixel value, a median of the range (0 to 255) is calculated so that we can scale up or scale down the pixel values according to the median, as shown in Figure1. All the pixel values, less than a median, are added to 128. The final values as shown in Figure2. The above phase solely is not enough in terms of security, as it involves shifting by a fixed value that can be unveiled easily by experts, too. Therefore, to increase security later, we will use the indiscriminate succession, produced earlier. Fig 7 illustration for the flow chart of the encryption process.

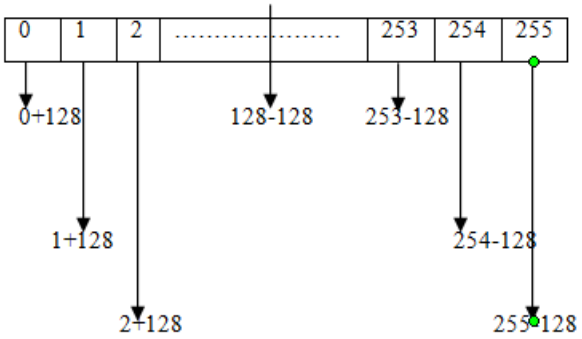


Fig. 1: Final Values.

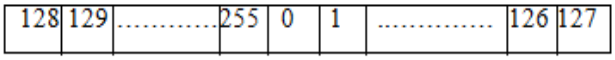


Fig. 2: Pixel Values According to the Median.



Fig. 3: Original Frame.



Fig. 4: Frame after RGP Pixel Manipulation.

45	34	189	230	87
156	67	90	23	89
78	156	81	90	67
4	115	178	104	124
236	105	111	32	241
59	120	118	199	45
34	144	120	41	253

Fig. 5: Original Matrix.

165	187	209	58	7
14	125	233	201	98
253	144	120	251	41
67	132	32	100	23
209	118	124	27	59
210	236	105	169	19
35	178	199	197	4

Fig. 6: Shuffled Matrix.

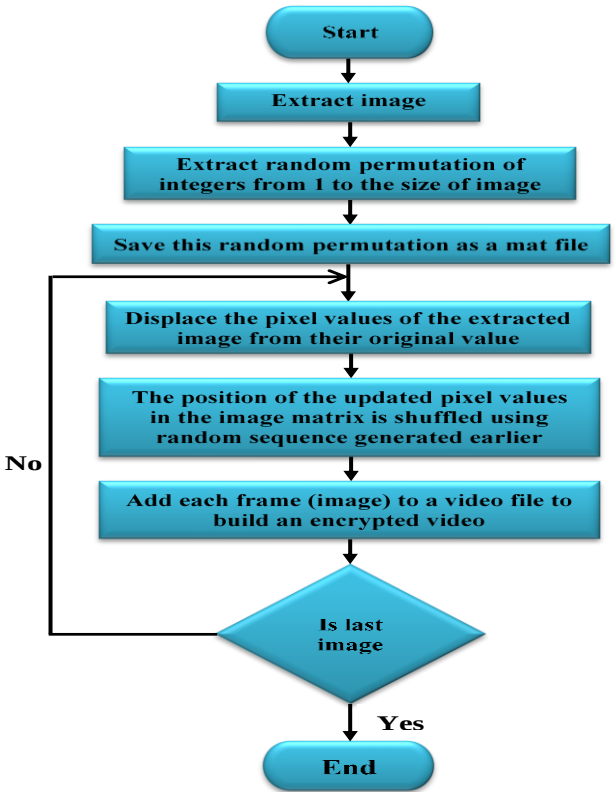


Fig. 7: Flow Chart for Encryption.

3.2. Key exchange

The shuffled sequence in the time being is set into a file that would later be sent. However, it requires subtle average of security to avoid the jeopardy while sending from one side to another. To encounter this drawback, before sending the file, it has to be encoded in advance. So far, the file consists of many subsets. Finally, the actual pixel values are shuffled to their basic positions, in addition to the previous subsets. Obviously, the greater the subset size is, the higher the invulnerability would be. Fig 8 illustration for the Flow chart of the key exchange process.

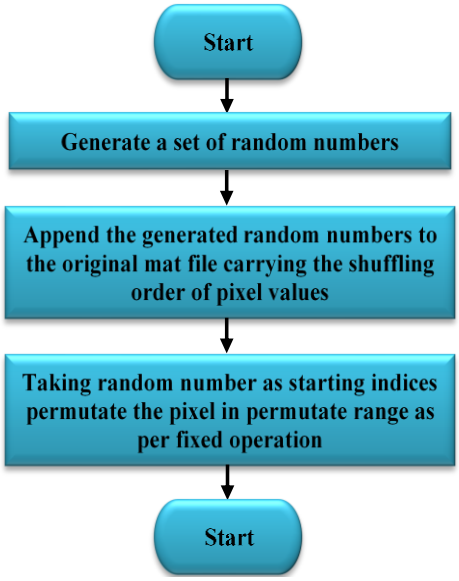


Fig. 8: Flow Chart for Key Exchange.

3.3. Decryption

With the help of the decrypted key, the video is shuffled again to retrieve the basic one. Finally, for decoding the video, reverse displacement of pixel values is performed. Fig 9 illustration for the Flow chart of the decryption process.

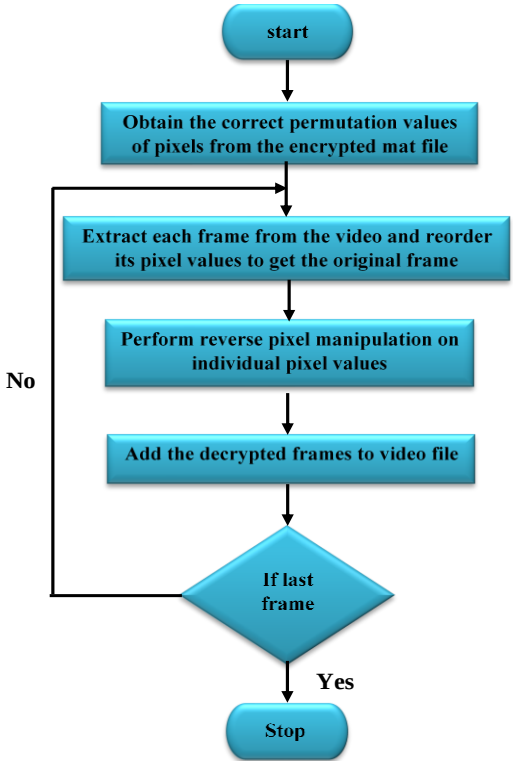


Fig. 9: Flow Chart for Decryption.

The following is illustration pseudocode for the encryption process

```
Let N be the number of frames in the video.
while j<N
img=getsnapshot(vid);
img_size=size(img);
img1=zeros(img_size(1),
img_size(2),img_size(3));
if(j==0)
idx=randperm(numel(img));
end;
for a = 1:img_size(1)
for b=1:img_size(2)
for c=1:img_size(3)
img1(a,b,c) = img(a,b,c);
end;
end;
end;
for a =1:img_size(1)
for b=1:img_size(2)
for c=1:img_size(3)
if(img1(a,b,c)>=128)
img1(a,b,c)=img1(a,b,c)-128;
else if(img1(a,b,c)<128)
img1(a,b,c)=img1(a,b,c) +128;
end;
end;
img(a,b,c)= img1(a,b,c);
end;
end;
end;
shuffled_im=reshape(img(idx),size(img));
aviobj=addframe(aviobj,shuffled_im,shuffled_im);
j=j+1;
end;
```

4. Result analysis

The algorithm is accomplished in MATLAB R2016b. The video is captured in AVI format. Simultaneously, the algorithm is encrypting. Thus, the video is successfully done. Technically, it is the ultimate style, indeed. Our algorithm also provides efficient security rather than the existed permutation techniques. Table I emulates the recommended algorithm and the previous techniques. In table 2 comparative Performance of [10] and Proposed Algorithm for encryption and decryption time on video of different sizes. Fig 10 illustration the encrypted and decrypted frames.

Table 1: Comparison Between Our Proposed Algorithm and the Presently Used Techniques

Methodology	Security level	Speed	Suitable for real time encryption
Fully Layered	High	Slow	NO
Selective Encryption	Low	Fast	NO
Proposed Algorithm	High	Very Fast	YES

Table 2: Comparison Between Our Proposed Algorithm and [10] For Encryption and Decryption Time (Second)

File Name	File Size (MB)	MAES [10]		Proposed Algorithm	
		Encryption	Decryption	Encryption	Decryption
Foreman.mpeg	1.26	781	923	621	781
Panasonic.mpeg	2.45	981	1027	812	963
Space.mpeg	4.11	1571	1611	1215	1333



Fig. 10: Encrypted Frame and Decrypted Frame.

5. Conclusion

As long as this research is concerned, it has tackled into details the role and necessity of security for video transfer. By transferring the video core, encryption plays a significant role to guarantee the confidentiality of it. In brief, the ultimate choice to encrypt a real time video is the recommended algorithm, it affords premium security in a relatively short computational phase, and it copes with different video sizes & types, and multiple devices, too.

References

[1] S. Somaraj and M. A. Hussain, "A Novel Image Encryption Technique using RGB Pixel Displacement for Color Images," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Feb. 2016. https://doi.org/10.1109/IACC.2016.59.

[2] Q.-A. Kester, L. Nana, and A. C. Pascu, "A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud Using AES and RGB Pixel Displacement," 2013 European Modelling Symposium, Nov. 2013. https://doi.org/10.1109/EMS.2013.51.

[3] A. Kulkarni, "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study," International Journal of Computer Applications, vol. 102, no. 16, Mar. 2013. https://doi.org/10.5120/10885-5777.

[4] K. Thiyagarajan, R. Lu, K. El-Sankary, and H. Zhu, "Energy-Aware Encryption for Securing Video Transmission in Internet of Multimedia Things," IEEE Transactions on Circuits and Systems for Video Technology, 2018. https://doi.org/10.1109/TCSVT.2018.2808174.

[5] M. A. Saleh, N. M. Tahir, E. Hisham, and H. Hashim, "An Analysis and Comparison for Popular Video Encryption Algorithms," 2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Apr. 2015. https://doi.org/10.1109/ISCAIE.2015.7298334.

[6] F. Sbiaa, S. Kotel, M. Zeghid, R. Tourki, M. Machhout, and A. Baganne, "A Selective Encryption Scheme with Multiple Security Levels for the H.264/AVC Video Coding Standard," 2016 IEEE International Conference on Computer and Information Technology (CIT), Dec. 2016. https://doi.org/10.1109/CIT.2016.53.

[7] O. G. Abood, M. A. Elsadd, and S. K. Guirguis, "Investigation of Cryptography Algorithms used for Security and Privacy Protection in Smart Grid," 2017 Nineteenth International Middle East Power Systems Conference (MEPCON), Dec. 2017. https://doi.org/10.1109/MEPCON.2017.8301249.

[8] S. K. Abd-El-Hafiz, S. H. Abd ElHaleem, and A. G. Radwan, "Permutation Techniques based on Discrete Chaos and Their Utilization in Image Encryption," 2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Jun. 2016. https://doi.org/10.1109/ECTICon.2016.7561265.

[9] A. Goel and N. Chandra, "A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based on Sorting Group-Wise of RGB Values and Explosive Inter-Pixel Displacement," International Journal of Image, Graphics and Signal Processing, vol. 4, no. 2, Mar. 2012. https://doi.org/10.5815/ijigsp.2012.02.03.

[10] P. Deshmukh and V. Kolhe, "Modified AES based Algorithm for MPEG Video Encryption," International Conference on Information Communication and Embedded Systems (ICICES2014), Feb. 2014. https://doi.org/10.1109/ICICES.2014.7033928.