RESEARCH ARTICLE OPEN ACCESS

Design and Implementation of Video Encryption for Multimedia Applications

Pranav Aggarwal*, Skanda Vishwanath*
*(Student, Department of Electronics and Telecommunication Engineering, K.J Somaiya College Of Engineering, Vidyanagar, Vidyavihar (E), Mumbai - 400 077, Maharashtra, India)

ABSTRACT
An explosion in the internet and other sharing technologies has made transfer and distribution of video content extremely easy. Unimpeded transfer of video and other multimedia content has lead to violation of several anti-piracy laws today. Hence, the need to prevent unauthorized distribution and protection of video data is on the rise. This paper demonstrates the lossless video encryption and decryption techniques. For encrypting the frames of the video, column and row shifting method is used, that is transposition cipher is generated. Further a password is used to encrypt the video as well.
Keywords – Color, Decryption, Encryption, Multimedia security, Password, transposition cipher.

I. INTRODUCTION

"A picture speaks a thousand words"- encapsulates the value of images in today's world. A video, being a stream of images provides a plethora of information. In the 21st century, targeted transfer of multimedia information has gained utmost importance. Hence security features as a key aspect in this targeted transfer. Classic encryption algorithms like DES, RSA etc. are not feasible for video data because of its large size and high computational requirements like in the case of textual data[1,2] . As a countermeasure, encryption algorithms use simple scrambling mechanisms for huge video data [3].

Owing to their large size, video encryption algorithms can be broadly classified into two parts. One method is the selective encryption technique. In selective encryption technique only parts of the video are encrypted, thereby reducing the computational requirement. Selective encryption algorithms typically use heavy weight encryption algorithms (DES and AES). Consequently, time taken for encryption is high and makes them unsuitable for real-time applications. This method is suitable, where the full content of the video stream is not critical. Another category of algorithms is the scramble only methods, wherein the pixel values of each frame of the video stream are scrambled randomly using a specific algorithm. In both these methods, there exists a trade off between computational efficiency and security.

In this paper we have tried and improved security by using an encrypt cum permute technique and at the same time tried and reduced the computational time. The process is lossless so all the information in the video is totally secured.

Our paper is organized as follows. In section 2 we shall explain the proposed algorithm in detail. This section gives an in depth analysis of various steps involved with the algorithm. In section 3 under the heading of experimental results, various parameters and their effects are discussed, implemented in MATLAB. Section 4 provides the security analysis for the password. Finally, the 5th section provides the conclusion.

Note that throughout the paper we shall experiment on a single frame within a video.

II. THE PROPOSED TECHNIQUE

The following section explains the proposed technique and its intricacies in detail.

2.1 Description of the Column Shifting Algorithm

Column Shifting Algorithm involves the scrambling of various pixel values of each frame. This is done by using the following technique.

(i). The eight digit password (or key) is taken from the user. This password is divided into two parts. The first part contains the first two digits of the password and the second part contains the rest.
Note that the password can be bigger than 8 bits but the speed of the process will be compromised.
(ii). The frames of the video are extracted one by one and individually encrypted. It is taken care that the frames extracted are in .png format if the encryption is meant to be lossless. If the frames are in .jpg format then due to JPEG standard quantization parameters there will be loss in information. The audio component of the video is eliminated by this process. The recovery of the audio component will be explained further.

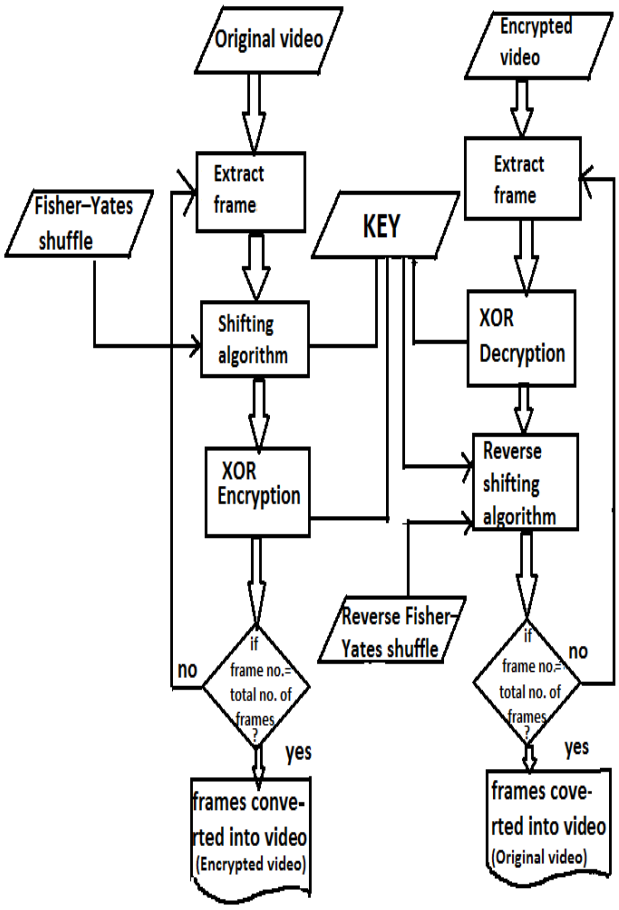


Fig 1.The algorithm flow chart is shown.

(iii). Using the Fisher- Yates shuffle algorithm we randomly generate a matrix equal to the size of rows in each frame.[4,5] The Fisher–Yates shuffle, in its original form, was described in 1938 by Ronald A. Fisher and Frank Yates in their book Statistical tables for biological, agricultural and medical research. The algorithm has two types i.e. Fisher–Yates Original method and Modern algorithm introduced by Richard Durstenfeld in 1964.We use the modern algorithm as it is more suitable for computer applications. In this method a random number is taken from numbers 1 to N. This number is then struck and moved to the end of the list by swapping them with the last unstruck number at each iteration. This step is carried out N times. After this is done the sequence got is nothing but the random permutation of the original numbers.

(iv). Each column is then redistributed depending on the Fisher Yates matrix. If we are using a color video then each pixel value is also split into its respective color values (namely red, green and blue) and then scrambling is enforced individually.

(v). To make the scrambling even more complex, after each frame is scrambled, the fisher Yates matrix is circularly shifted by the first two digits of the password provided by the user. Therefore, each frame is made less correlated to the preceding frame. This causes the encrypted video even harder to be decrypted.

2.2 Description of the Encryption Algorithm

The encryption algorithm provides frame by frame encryption using an eight digit password as per the user's preference. This is done by using the following technique.

(i). The second part of the password i.e. is the rest of the 6 digits are used to encrypt each and every pixel within every frame. The password itself will be divided into two parts- each part being a three digits or 8 bit password.

(ii). Note that, three digit numbers greater than 256 shall be truncated immediately by dividing the same into half or by a fourth. If the number is less than 512 but greater than 256 i.e. the number consumes 9 bits in its binary form, then the same shall be cleaved to half its value. Consequently for a three digit number greater than 512 shall be reduced to a fourth. The two digits that remain shall be used to encrypt the audio within the video.

(iii). The two parts of the password are then XORed with red, blue and green matrix each pixel.

2.3 Post- Encryption

After encryption of a frame is finished it is checked whether the frame number is equal to the total number of frames. If so then the encrypted frames are complied to form the video which is now encrypted. If not equal then the process is repeated for the following frame.

For the decryption of the video to take place, the person requires the Fisher- Yates shuffle generated code which is at least of the order 10^600 taking minimum width of any video as 240 pixels into account and the eight digit password created by the user.

2.4 Description of the Audio Encryption

Audio is also an essential part of a video which needs to be protected. As observed in the above steps the audio component is being lost during video encryption. Therefore, the audio has to be extracted read from the video before starting the video encryption process and encrypted separately.

Audio can be encrypted using successive addition technique. In this technique the values of stereo sound data of the video is extracted. The obtained stereo sound data are in the form of a row matrix having number of values (N) equal to

$$N = L * f \quad (1)$$

Where L=length of video in sec

f= sampling frequency

Now every value of the matrix is added with the value following it. This creates distortion in the audio signal. It is also seen that ideally the values are between -1 to 1 and over the value 1 distortion is witnessed. So after successive addition encryption, an additional addition of 1 can be done to all the value in the matrix to get perfect distortion.

After both audio and video decryption is over, they can be synchronized and clubbed together.

III. Experimental results:

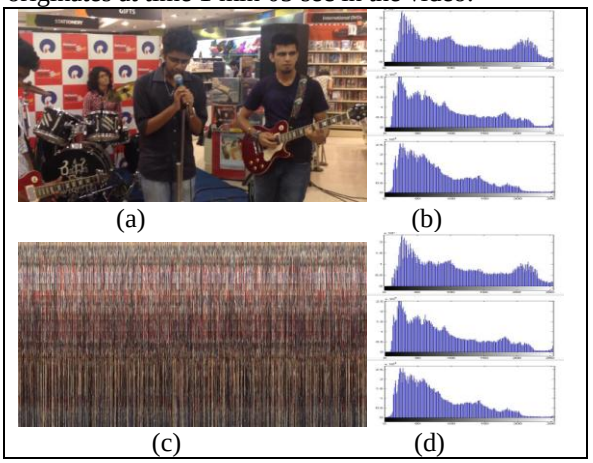
This section analyses various parameters that describe the effectiveness of the proposed encryption.

3.1 Histogram analysis

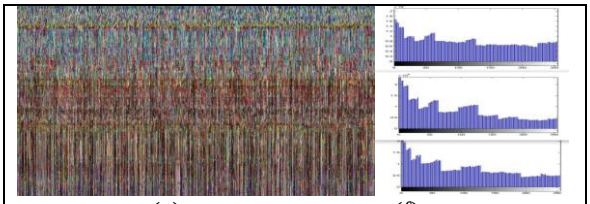
Image histograms may reflect the distribution of image elements. An attacker can examine the histogram of an encrypted image (red, green and blue) using the algorithms of attack and the statistical analysis of the encrypted image to obtain useful information concerning the original image. It is important to ensure that the original image and encrypted image do not have any statistical similarities. The histogram analysis clarifies how the pixels in an image are distributed by plotting the number of pixels at each intensity level.

The histogram of the original image shows how graphically the distribution of the number of pixels at each grey level. It is clear that the histogram of the encrypted image is almost uniformly distributed and significantly different from the respective histograms of the original image. Thus, the encrypted image does not provide any evidence to use in any statistical attack on the encryption of an image using the proposed technique. The algorithm makes statistical attacks difficult. The histogram of the encrypted image produces a uniform distribution which is very different from the histogram of the plain image.

Let us consider "Video 1"* which is of 5 min and 24 sec and contains 9732 frames, with frame rate of 29.97 frames per sec. The figure below shows the frame number 1948 as the test frame which originates at time 1 min 05 sec in the video.



(a) (b) (c) (d)

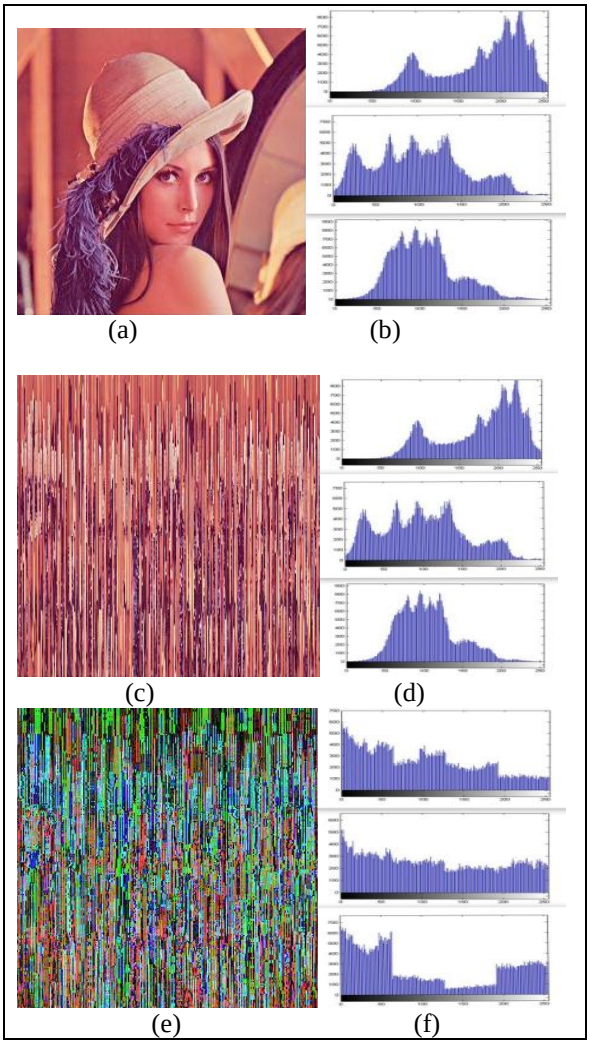


(e) (f)

*Video 1 is a self recorded video and does not violate any privacy laws or encroach upon a third party's privacy.

Fig 2: (a) denotes the original test frame from the video. (b) Denotes histogram of the test frame. (c) Denotes the shuffled frame. (d) Denotes histogram of the shuffled frame. (e) Denotes the encrypted frame and (f) Denotes histogram of the encrypted frame.

Fig 3 shows the experiment being implemented on a standard test image "Lena" treated as a frame.



(a) (b) (c) (d) (e) (f)

Fig 3: (a) denotes the original test image. (b) Denotes histogram of the test image. (c) Denotes the shuffled image. (d) Denotes histogram of the shuffled image. (e) Denotes the encrypted image and (f) Denotes histogram of the encrypted image.

Fig 4 shows the experiment being implemented on the standard test image "cameraman" which is in gray scale.

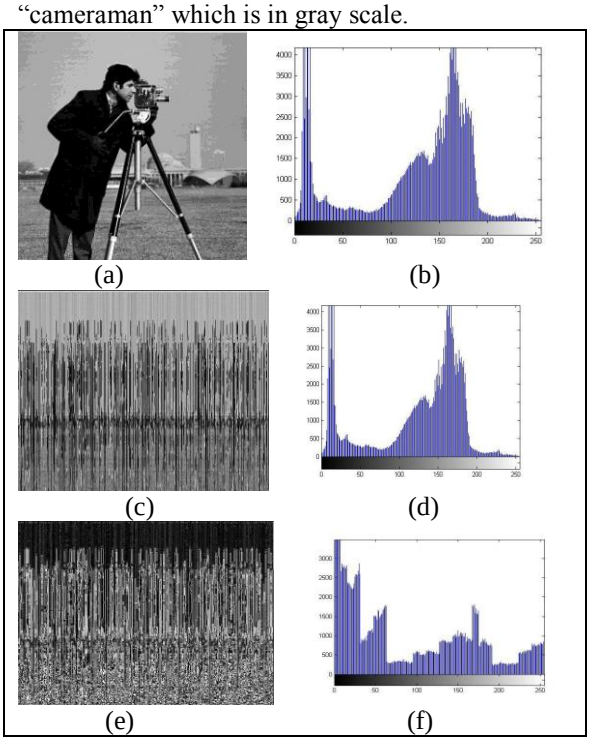


Fig 4: (a) denotes the original test image. (b) Denotes histogram of the test image. (c) Denotes the shuffled image. (d) Denotes histogram of the shuffled image. (e) Denotes the encrypted image and (f) Denotes histogram of the encrypted image

It is seen that the histograms of encrypted images from figure 2 and 3 are quite uniformly distributed. Thus, the encrypted image does not provide any evidence to use in any statistical attack on the encryption of an image using the proposed technique. The algorithm makes statistical attacks difficult. The histogram of the encrypted image produces an uniform distribution which is very different from the histogram of the plain image.

3.2 Correlation coefficient

The correlation coefficient is a quantity that gives the quality of a least squares fitting to the original data[6]. The correlation between the original image and the scrambled image as well as the correlation between:

1- original image and itself (a)
2- original image and scrambled (c)
3 -original image and encrypted image (e)
have been analyzed, in that order.

If the correlation of the encrypted image is equal to zero or very near to zero, then the original image and its encrypted image are totally different, i.e., the encrypted image has no features and is highly independent from the original image. If the correlation is equal to -1, this means the encrypted image is a negative of the original image. The correlation values for every figure are given below.

As seen, from the tables, the correlation between the original and scrambled- encrypted image tends towards zero. Hence, the algorithm in effect has reduced the correlation between the two images.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \quad (2)$$

Fig 2:

	Red	Green	Blue
a	1	1	1
c	0.0392	0.0430	0.0517
e	0.0162	0.0028	0.0095

Fig 3:

	Red	Green	Blue
a	1	1	1
c	0.0741	0.0630	0.0513
e	-0.0430	0.0134	0.0271

Fig 4:

a	1
c	0.2470
e	-0.1368

Where a, c, e denote the image within a given figure.

It is observed that the correlation coefficient between the encrypted frames and the original frame are close to 0 which makes the encrypted frame significantly different from the original frame.

3.3 Entropy Analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon[7]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy H(m) of a message source m can be calculated as:

$$H = -\sum p(x) \log p(x) \quad (3)$$

where P (mi) represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 28 symbols with equal probability, i.e., 1 2 28 m = {m ,m ,...,m }.

Truly random source entropy is equal to 8. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the image is encrypted, their entropy should ideally be 8 or at least close. As the entropy decreases below 8, the system becomes vulnerable to various forms of attack. Consider the figure below. The occurrences for various colour and grey image levels are computed and recorded. The value of entropy for each image in the figure is given below:

Fig 2:

	Red	Green	Blue
a	7.7588	7.5832	7.4278
c	7.7588	7.5832	7.4278
e	7.9505	7.8668	7.8014

Average entropy value= 7.8729

Fig 3:

	Red	Green	Blue
a	7.3303	7.6247	7.1551
c	7.3303	7.6247	7.1551
e	7.8513	7.9528	7.6777

Average entropy value= 7.8272

Fig 4:

a	7.0843
c	7.0843
e	7.5405

It is seen that in all the tables the entropy of the image has remained same after scrambling of the image but has increased after encrypting the images by xoring the pixels with the password provided by the user. This makes the image more secure and resistant from attacks.

3.4 Video size analysis

Taking the above video "Video 1" for this analysis. The video size is originally of 4.91 MB but after encryption the video size increase to 119 MB. When the video is decrypted back again the size of the video is 55.2 MB. So it is seen that the size of the original video has increased considerably after encryption but it again falls after decrypting the encrypted video. The decrypted video has the exact same pixel information as the original one, making the process a lossless.

VI. Security analysis

For any multimedia data, the encryption algorithm is said to be secure if the cost of breaking the proposed method is greater than the investment of buying the key. Bit ciphers, where plaintext bits are combined with a cipher bits by an exclusive-or operation (xor), can be very secure if used properly. However they are vulnerable to attack if certain precautions are not followed. First and foremost, the bit xor method is vulnerable only when the same key is used twice. In this case, the algorithm clearly, ensures that the same key is never used when the plaintext is encrypted. At every stage of encryption the plaintext is encrypted using two different keys. Hence the possibility of the plaintext being revealed due to errors such as the one mentioned above has been avoided.

The algorithm performs xors with the following column. The last column itself is xored with the 8 bit key. As neighbouring pixels have high correlation[8] their xored values inch towards the darker side. Hence the picture is completely different from each other. Thus a fairly bright and appealing picture would seem rather dark after xoring. The frame is vulnerable to brute force attacks. . However the pixel values are first scrambled amongst themselves. Hence even if the attacker uses brute force algorithm, his success would be short lived. The algorithm and the matrix to unscramble the pixels is known only to the source computer. Also the size of the Fisher- Yates shuffle code is atleast of the order 10^600 which makes it very difficult for the hacker to crack the code using statistical or brute-force attack.

V. Conclusion

The proposed algorithm described in this paper has improved image security using an integration of a shifting algorithm. The algorithm succeeds as far as its impact on the correlation among image pixels in a plain image to increase the security level of the encrypted image is concerned. The proposed technique needs further improvement in order to increase the entropy from an average value of 7.7468 to 8. Experimental results show that the proposed algorithm has a high security level. It can withstand against known and chosen plain text, brute force,

statistical and differential attacks, and is able to encrypt large data sets efficiently. Various levels of security on the algorithm have resulted in increase in size of the same. The same increase in size could be obstructed had we used a compression algorithm after encryption. This would make the decryption and the frames obtained henceforth lossy. Further work on the same algorithm can be to decrease (compress the encrypted video increase the uniformity in histogram distribution, thereby increasing the level of encryption in the same.

References

[1] M. Van Droogenbroeck , R.B., "Techniques for a selective encryption of uncompressed and compressed images". In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002(2002).

[2] Mohammad Ali Bani Younes, A.J., "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption". IJCSNS International Journal of Computer Science and Network Security, 2008. 8(april 2008): p. 191-197.

[3] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," in Proc. of ACM Multimedia, pp. 219–229.

[4] Ade-Ibijola, Abejide Olu, " A Simulated Enhancement of Fisher-Yates Algorithm for Shuffling in Virtual Card Games using Domain-Specific Data Structures", International Journal of Computer Applications (0975 – 8887) Volume 54– No.11, September 2012

[5] Fisher, Ronald A.; Yates, Frank (1948) [1938]. Statistical tables for biological, agricultural and medical research (3rd ed.). London: Oliver & Boyd.

[6] Edwards, A. L. "The Correlation Coefficient." Ch. 4 in An Introduction to Linear Regression and Correlation. San Francisco, CA: W. H. Freeman, pp. 33-46, 1976.

[7] Shannon, C.E., "Communication Theory of Secrecy Systems". Bell Syst Tech J. 1949.

[8] S. P. Nana'Vati, K.P.P., "Wavelets: Applications to Image Compression-I". Scientific and Engineering Computing, 2004. 9 No 3: p. 7.