Annual of Konstantin Preslavsky University of Shumen
vol. XX C, 2019, pp. 57 - 66

OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS FOR VIDEO FILES*

GEORGI G. DIMITROV, KRASIMIR M. KORDOV

ABSTRACT: *Proving the efficiency, reliability and security of every cryptographic algorithm requires extensive cryptographic analysis. In this paper we overview the most used indicators concerning encryption of video files. In order to perform successful video encryption and cryptographic analysis it is important to analyze the video structure for further processing.*

KEYWORDS: *Cryptographic analysis, Cryptographic algorithms, Cryptography, Video files, Video cryptography*

2010 Math. Subject Classification: *94A60, 68P25, 68U10, 62B10*

1 Introduction

In general, cryptography is an ancient science for secret communication with transforming messages into unreadable kind, impossible to read from third parties. Cryptographic analysis has the opposite purpose, to uncover secret messages, restoring their initial look.

In the first signs of cryptography the messages were only text symbols transformed into different symbols, but later complex of mathematical algorithms for message transformations appeared for more successful encryption. In modern cryptography the information is mostly digital, stored and transferred with computer system which inflicts/calls for different approaches. Encrypting digital data requires processing the information as a sequence of digits.

Applying a cryptographic algorithm to a specific type of file is one the most used approaches to prove the properties and the quality

*This paper is (partially) supported by Scientific Research Grant RD-08-71/29.01.2019 of Konstantin Preslavski University of Shumen

of the encryption process. Digital video files are widely used for data information carriers in modern days, which also makes them usable in encryption algorithms.

Processing video files for their encryption and decryption is related to the structure of the video files type. The standard digital video files contain header information (that includes meta data about the file such as file size, video compression, number of frames, etc.), array of frames containing static images building the video file. Encryption process is focused on transforming the frames, leaving no information of the original look of the (visual) information.

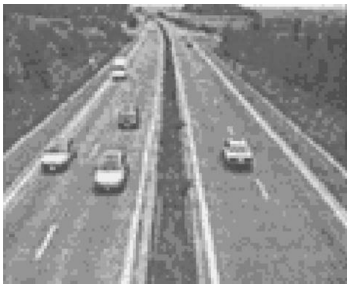
The other sections of this paper describe the most used cryptographic analysis tests concerning digital video files.

2 Visual Analysis

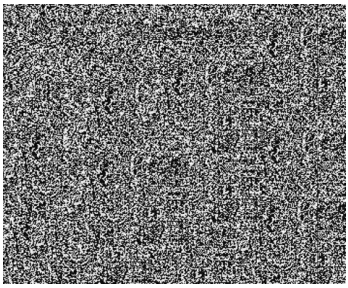
The visual analysis compares frames from plain video files with their corresponding encrypted files. The goal of this test is to see with naked eye if there is any similarity between the compared frames. The good cryptographic algorithms successfully transform the encrypted frames without any trace of color values of the original pixels from the plain files. This can be achieved by replacing the color value or/and changing pixels positions. The replacement process is called substitution and the position changing process is called permutation. Those processes are often realized by using pseudo-random generators (PRG) [14, 15, 16] for chaotic pixel value and position changing. PRGs [10, 12, 17] provide endless bit stream used for extracting random numbers for color and/or position values.

Video encryption algorithms are implemented to work with video files with gray scale color (8 bit color) or color videos with RGB color scheme (8 bits for Red color, 8 bits for Green color and 8 bits for Blue color).

Figure 1 represents the results of encryption algorithms for gray scale video files from Ref. [18] and color video file from Ref. [7].



(a) Plain gray scale video frame



(b) Encrypted gray scale video frame

(c) Plain color video frame

(d) Encrypted color video frame

Figure 1: Visual Analysis - comparison of video frames

3 Key-space Analysis

One of the most important elements of every cryptographic system is the secret key. Usually the secret key is composed by the initial variables of the cryptographic system and the variety of the possible initial values builds the key-space. According to the IEEE floating point standards the key-space should be greater than 2^{100} to be considered large enough to withstand against brute-force attacks. Usually the cryptographic systems are based on PRGs and the key space is entirely composed by the initial values of the used pseudo-random generator.

Table 1 gives examples of obtained key-spaces in cryptographic systems.

Reference	Key-space	Reference	Key-space
Ref. [13]	2^{126}	Ref. [11]	2^{149}
Ref. [5]	2^{172}	Ref. [2]	2^{179}
Ref. [3]	2^{199}	Ref. [4]	2^{199}

Table 1: Key-space Analysis

4 Histogram Analysis

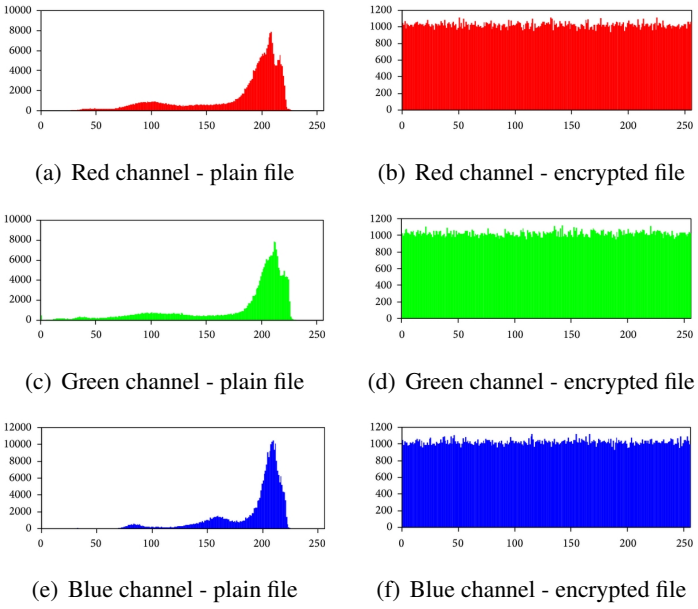
The histogram analysis compares the frames (processed as images) of plain video files with their corresponding encrypted frames. Image histograms represent the tonal distribution of the colors in the images.

Figure 2 is an example of histogram analysis of a color image. Figure 2(a) represent red color distribution and Figure 2(b) - red color distribution after the encryption. Figures 2(c), 2(d), 2(e) and 2(f) show the corresponding Green and Blue channels.

Other examples of histogram analysis are proposed in [6, 8, 9]

5 Correlation Analysis

The correlation analysis is a statistical test assessing the values' dependence. This test can be applied to video encryption algorithms with the adjacent pair of pixel values of the encrypted frames. The correlation analysis is performed by calculating the correlation coefficient values which are always in range $[-1,1]$ and if the values are between $|1,0.7|$ it is considered that we have strong dependence between the initial values, if the correlation coefficient is between $|0.7,0.3|$ we have medium dependence between the measured values, and if the correlation coefficient is between $|0.3,0|$ we have weak dependence of the initial values. When the correlation coefficient is very close to zero it



(a) Red channel - plain file (b) Red channel - encrypted file

(c) Green channel - plain file (d) Green channel - encrypted file

(e) Blue channel - plain file (f) Blue channel - encrypted file

Figure 2: Histogram Analysis - comparison of Red, Green and Blue channels of a plain and encrypted image

is considered as absence of dependence between the measured values, which is indication of strong encryption.

Correlation coefficient can be calculated as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{1}$$

where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2,$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \overline{y})^2,$$

$$cov(x,y) = \sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y}),$$

N is the number of pixels processed from a frame (plain or encrypted), x_i and y_i are the values of corresponding pixel colors of both files, $\overline{x}$ and $\overline{y}$ are mean values of pixel colors for each frame, and $cov(x,y)$ is covariance between both files.

Reference	Direction	Plain	Encrypted
Ref. [18]	Horizontal	0.9671	0.00251
	Vertical	0.9655	0.00237
	Diagonal	0.9683	0.00198
Ref.[19]	Vertical	0.9655	0.00237
	Diagonal	0.9683	0.00198
Ref. [1]	Horizontal	0.9452	-0.0112
	Vertical	0.9471	-0.0813
	Diagonal	0.9127	0.0009

Table 2: File size comparison

Table 2 demonstrates that the values of the adjacent pixel colors have strong dependence before the encryption and have no dependence after the encryption (close to zero) which is indication of good cryptographic properties.

6 Information Entropy

In general, the entropy is statistically calculated value that measures the uncertainty in information theory. Concerning video frames, information entropy measures the probability of certain pixel value appearance. Entropy is calculated as follows:

$$H(X) = -\sum_{i=0}^{N} p(x_i) log_2 p(x_i), \tag{2}$$

where X is a variable , $p(x_i)$ is function of the probability of x to have certain value - x_i. Colors values of every pixel of the frame can be from 0 to 255 for every color of RGB scheme. For truly chaotic system the best value of entropy is $H(X) = 8$.

Reference	Entropy of plain file	Entropy of encrypted file
Ref. [19]	6.234655	7.997266
Ref. [9]	7.4318	7.9968
Ref. [1]	-	7.941

Table 3: Information Entropy Analysis

Table 3 shows the encrypted files have Information Entropy value very close to 8, which is indicator of chaotic information behavior.

7 Number of Pixel Change Rate (NPCR) and Uniform Average Change Intensity (UACI)

As a part of differential analysis Numbers of Pixel Change Rate (NPCR) and Uniform Average Change Intensity (UACI) are indicators that measure the difference between compared frames from plain video file and the corresponding frames from encrypted video file. NPCR and UACI are calculated as follows:

$$NPCR = \frac{\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} D(i,j)}{W \times H} \times 100\%, \tag{3}$$

$$UACI = \frac{1}{W \times H} \left(\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} \frac{|C_1(i,j) - C_2(i,j)|}{N} \right) \times 100\%, \tag{4}$$

where W and H are width and height of the frames.

Reference	NPCR	UACI
Ref. [8]	99.5850 %	28.6210 %
Ref. [9]	99.6149 %	13.8349 %

Table 4: NPCR and UACI

Table 4 represents some of the obtained results of cryptographic algorithms. The difference of the plain and the encrypted file is almost 100%.

8 Conclusion

Cryptographic algorithms are designed for information security. Part of developing a new encryption models is proving they are reliable enough. This can be achieved by applying the algorithm to the specific file types for further cryptographic analysis. One of the used file types are digital video files.

In this paper we overview the base cryptographic properties for evaluation of the video encryption schemes such as visual analysis, key-space, histogram analysis, correlation analysis, information entropy, Numbers of Pixel Change Rate and Uniform Average Change Intensity.

REFERENCES:

[1] Deshmukh, P., Kolhe, V. (2014, February). Modified AES based algorithm for MPEG video encryption. In: International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE.

[2] Kordov, K. (2015). Modified pseudo-random bit generation scheme based on two circle maps and XOR function. *Applied Mathematical Sciences*, **9**(3), 129-135.

[3] Kordov, K. M. (2014, November). Modified Chebyshev map based pseudo-random bit generator. *AIP Conference Proceedings* (Vol. **1629**, No. 1, pp. 432-436). AIP.

[4] Kordov, K. (2015). Signature Attractor Based Pseudorandom Generation Algorithm. *Advanced Studies in Theoretical Physics*, **9**(6), 287-293.

[5] Kordov, K., Stoyanov, B. (2017). Least Significant Bit Steganography using Hitzl-Zele Chaotic Map. *International Journal of Electronics and Telecommunications*, **63**(4), 417-422.

[6] Kordov, K., Valchev, G. (2019). Video steganography with steganalysis. *Mathematical and Software Engineering*, **5**(1), 15-22.

[7] Lian, S., Liu, Z., Ren, Z., Wang, Z. (2005, November). Selective video encryption based on advanced video coding. In: Pacific-Rim Conference on Multimedia (pp. 281-290). Springer, Berlin, Heidelberg.

[8] Loukhaoukha, K., Chouinard, J. Y., Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering*, 2012, **7**.

[9] Sathishkumar, G. A., Bagan, K. B. (2011). A novel image encryption algorithm using pixel shuffling and base 64 encoding based chaotic block cipher (IMPSBEC). *WSEAS Transactions on computers*, **10**(6), 169-178.

[10] Stoyanov, B. P. (2012, October). Chaotic cryptographic scheme and its randomness evaluation. *AIP Conference Proceedings* (Vol. **1487**, No. 1, pp. 397-404). AIP.

[11] Stoyanov, B. P. (2014, November). Using circle map in pseudorandom bit generation. *AIP Conference Proceedings* (Vol. **1629**, No. 1, pp. 460-463). AIP.

[12] Stoyanov, B. (2008). Improved cryptoanalysis of the self-shrinking p-adic cryptographic generator. *Advanced Studies in Software and Knowledge Engineering*, 112.

[13] Stoyanov, B., Szczypiorski, K., Kordov, K. (2017). Yet another pseudorandom number generator. *International Journal of Electronics and Telecommunications*, **63**(2), 195-199.

[14] Stoyanov, B., Kordov, K. (2014). Novel zaslavsky map based pseudorandom bit generation scheme. *Applied Mathematical Sciences*, **8**(178), 8883-8887.

[15] Stoyanov, B., Kordov, K. (2013, June). Pseudorandom bit generator with parallel implementation. In: International Conference on Large-Scale Scientific Computing (pp. 557-564). Springer, Berlin, Heidelberg.

[16] Stoyanov, B. P., Kordov, K. M. (2013, October). Cryptanalysis of a modified encryption scheme based on bent Boolean function and Feedback with Carry Shift Register. *AIP Conference Proceedings* (Vol. **1561**, No. 1, pp. 373-377). AIP.

[17] Stoyanov, B., Kolev, M., Nachev, A. (2012). Design of a new self-shrinking 2-adic cryptographic system with application to image encryption. *European Journal of Scientific Research*, **78**(3), 362-374.

[18] Yang, S., Sun, S. (2008). A video encryption method based on chaotic maps in DCT domain. *Progress in natural science*, **18**(10), 1299-1304

[19] Yang, T., Li, Y., Lai, C., Dong, J., Xia, M. (2018). The improved hill encryption algorithm towards the unmanned surface vessel video monitoring system based on Internet of Things technology. *Wireless Communications and Mobile Computing*, 2018.

Georgi Dimitrov
Department of Computer Informatics,
Faculty of Mathematics and Informatics,
Konstantin Preslavski University of Shumen, 9712 Shumen, Bulgaria
g.dimitrov@shu.bg

Krasimir Kordov
Department of Computer Informatics,
Faculty of Mathematics and Informatics,
Konstantin Preslavski University of Shumen, 9712 Shumen, Bulgaria
krasimir.kordov@shu.bg