Annual of Konstantin Preslavsky University of Shumen
vol. XXII C, 2021, pp. 23 - 31, https://doi.org/10.46687/QWXZ2886

OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS FOR AUDIO FILES AND THEIR PROPERTIES*

Tsvetelina R. Ivanova

ABSTRACT: *Any cryptographic algorithm that is claimed to be effective must be properly analysed to prove its effectiveness, reliability and security. In this paper the most used quality indicators are reviewed and classified. The principles of the audio encryption are reviewed. A classification of the analysing methods is made.*

KEYWORDS: *Security analysis, Cryptography, Cryptographic algorithms, Audio encryption*

2020 Math. Subject Classification: *94A60, 68P25, 68W40, 62B10*

ПРЕГЛЕД НА КРИПТОГРАФСКИТЕ АЛГОРИТМИ ЗА КРИПТИРАНЕ НА АУДИО ФАЙЛОВЕ И ТЕХНИТЕ СВОЙСТВА

Цветелина Р. Иванова

РЕЗЮМЕ: *Всеки криптографски алгоритъм, за който се твърди, че е ефективен, трябва да бъде правилно анализиран, за да се докаже неговата ефективност, надеждност и сигурност. В тази статия са разгледани и класифицирани най-използваните показатели за качество. Прегледани са принципите на изследване на криптирането на звукови файлове. Направена е представяне на методите за анализ.*

*This paper is (partially) supported by Scientific Research Grant RD-08-107/02.02.2021 of Shumen University.

1 Въведение

Криптографията е стара наука, наричана още Науката за Тайнопис, която дава възможност за секретни комуникации, като преобразува съобщенията така, че да бъдат неразбираеми от трети лица. Нейните принципи, средства и методи се биват широко и обстойно използвани за осигуряване на кибер сигурност в съвременната информатика. Криптографските анализи имат точно обратното предназначение и по тази причина се развиват успоредно с криптографията. Те служат за откриване на скрити съобщения и връщането им към начално състояние. Криптографията създава защита на информацията, докато криптографският анализ създава методи и средства за разрушаването на тази защита. Първоначално криптографията се е състояла в това текстовите символи в съобщението да се заместват с други символи, но по-късно се появяват набор от математически алгоритми за преобразуване на съобщенията и по-добра защита. Съвременната криптография съществува в пресечната точка на дисциплините математика, компютърни науки, електротехника, комуникационни науки и физика. Приложенията на криптографията включват електронна търговия, разплащателни чип-базирани карти, цифрови валути, компютърни пароли, военни комуникации и др. Съвременната криптография силно се основава до голяма степен на математическата теория и компютърните науки. Криптирането на цифрови данни изисква обработка на информация, която е представена като последователност от цифри. Макар че теоретично е възможно да се пробие добре проектираната система, на практика е невъзможно да се направи. Ако са добре проектирани, такива системи се наричат изчислително сигурни. Теоретичните постижения, например подобренията в алгоритмите за целочислено факторизиране и по-бързата изчислителна технология изискват тези системи да бъдат непрекъснато преоценявани и, ако е необходимо, адаптирани. Прилагането на криптографски алгоритъм върху конкретен тип файлове е един от най-използваните подходи за доказване на свойс-

твата и качеството на процеса на криптиране. Дигиталните аудио файлове са широко използвани за пренос на информация в днешни дни, което ги прави много удобни за използване на криптиращи алгоритми. Аудио файловете с импулсно-кодова модулация са известни с предимството да са от некомпресиран формат, разработен от IBM и Microsoft. Алгоритмите за криптиране на аудио файлове често са реализирани чрез използването на генератори за псевдослучайни числа[1, 2, 3, 13]. В тази статия фокусът ще бъде върху най-използваните криптографски методи, изследващи и доказващи високата защита при криптиране на аудио файлове.

2 Визуални анализи

Визуалните анализи [4] сравняват изчертаните върху координатната ос цифрови данни, като абцисната ос е време, а ординатната - амплитуда. Това са цифровите данни от които се състоят оригиналния файл и криптираният му съответен. Целта на този анализ е да се види с просто око дали има сходство между сравняваните графики. Добрите криптографски алгоритми успешно преобразяват аудио файловете и при такова сравнение не се вижда никакво сходство. В статии [1, 2, 3, 13] алгоритмите са имплементирани да работят с аудио файлове тип WAV, MP3 и др. В тях могат да се видят тези визуални анализи.

3 Корелационен анализ

Полезна мярка за оценка на качеството на криптиране на всяка криптосистема е корелационния коефициент или зависимостта между сходни сегменти от оригиналния и криптирания аудио файл [5]. Корелационният коефициент, получен от този анализ, е винаги между [-1,1]. Ако стойностите са между [1, 0.7] се счита, че има силна зависимост между началните стойности; между [0.7,0.3] има средна зависимост между измерените стойности; ако корелационния коефициент е между [0.3,0] има много слаба зависимост, а близостта до 0.0 се счита за липса на линейна връзка.

Корелационният коефициент се изчислява както следва:

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

където:

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

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \overline{y})^2, \quad (3)$$

$$cov(x,y) = \sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y}), \quad (4)$$

съответните фрагменти от стойности от оригиналния и криптираният файл са x_i и y_i, x и y са средните стойности на сегменти, N е общият брой сегменти и накрая $cov(x, y)$ е ковариацията между двата файла. Таблица 1 представя корелационния коефициент при криптиране на аудио файлове.

Литература	Размер на файла	Дължина на файла	Корелационен коефициент
Ref. [1]	2.33 mb	13.85 s	0.0004710
Ref. [2]	-	-	0.0008190
Ref. [9]	-	7 s	0.0233000
Ref. [10]	-	-	0.0000900
Ref. [11]	103/kB	-	0.0038000
Ref. [13]	200 kb	2.32 s	-0.0248023
AES [10]	-	-	0.0097100

Таблица 1: Корелационен коефициент

4 Честота на изменение на криптираните файлови фрагменти

Оценката на броя променени фрагменти (Number of Sample Change Rate, NSCR) определя качеството на алгоритъма в проценти. Сравняват се оригиналните фрагменти с криптираните и се показва колко процента е разликата между тях. Изчислява се по следния начин:

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} x100\% \tag{5}$$

където:

$$D_i = \begin{cases} 1, x_i \neq y_i \\ 0, otherwise \end{cases} \tag{6}$$

Във формула (5), съответните извадки от стойности от оригиналния и криптираният файл са x_i и y_i, а общият брой на всички извадки е N. Таблица 2 дава примери за NSCR коефициента между оригиналния и криптирания файл.

Литература	NSCR коефициент
Ref. [1]	99.998%
Ref. [9]	99.998%
Ref. [10]	99.998%
Ref. [13]	99.998%
AES [10]	99.603%

Таблица 2: NSCR коефициент

5 Съотношение сигнал/шум

Пресмятането на съотношението сигнал/шум (Signal-to-Noise Ratio, SNR) [6] измерва на разбираемостта на звуковия сигнал. Пресмята се по следния начин:

$$SNR = 10log_{10} \frac{\sum_{i=1}^{N} x_i^2}{\sum_{i=1}^{N} [x_i - y_i]} dB, \tag{7}$$

където x_i и y_i съответните извадки от стойности от оригиналния и криптираният файл, а N е броя фрагменти.

Резултати от това изследване за различни алгоритми са показани в Таблица 3.

6 Пиково съотношение сигнал/шум

Пиковото съотношение сигнал/шум
(Peak Signal-to-Noise Ratio, PSNR) [7] е друг начин да се изчисли силата на чистият сигнал срещу силата на шума. Този анализ е почесто използван в криптирането на изображения [8], но може да се използва и като тест за качеството на предлагания алгоритъм. Изчислява се по следния начин:

$$PSNR = 10log_{10}\frac{MAX^2}{MSE}dB \tag{8}$$

където максималната възможна стойност на аудио потока е MAX. Тук максималната стойност може да бъде 65,535. В този случай има възможност за квадратична грешка между оригиналния и криптирания файл и тази средна крадратична грешка може да бъде изчислена по следния начин:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \tag{9}$$

Получените резултати от този тест за различни алгоритми са показани на Таблица 3.

Литература	SNR коефициент	PSNR коефициент
Ref. [1]	−16.0483 dB	1.4524 dB
Ref. [2]	-23.89dB	-
Ref. [9]	33.7464 dB	59.7989 dB
Ref. [10]	−133.0000 dB	-
Ref. [13]	-42.3697 dB	4.6583 dB
AES [10]	−1.4461 dB	-

Таблица 3: Peak signal-to-noise ratio.

7 Скорост на криптиране

Важно свойство на криптиращите алгоритми е скоростта на криптиране. В Таблица 4 са резултатите, получени при различни криптиращи алгоритми.

Литература	Размер	Дължина	Време за криптиране
Ref. [1]	2.33 mb	13.85 s	5.767 s
Ref. [9]	-	7 s	0.012 s
Ref. [13]	200 kb	2.32 s	0.865 s
AES [2]	800 kb	-	0.003 s

Таблица 4: Скорост на криптиране.

8 Чувствителност на ключа

Друга важна характеристика на корелационния анализ е чувствителността към ключовете. Добрите аудио криптиращи алгоритми са чувствителни по отношение на секретният ключ и съответно към лека промяна на същия. Примери за това са предложени в следните статии: [1], [9], [12] и [13].

9 Заключение

Криптографските алгоритми са създавани и моделирани за защита на информацията. Част от разработването на нов криптиращ алгоритъм е да се докаже неговата сигурност и устойчивост на атаки. Това се постига чрез прилагането на алгоритъма към специфични файлови типове за по-нататъшни криптографски анализи. Един от най-използваните файлови типове са дигиталните аудио файлове.

В настоящата статия разгледахме базовите криптографски свойства за оценяване на аудио криптиращите схеми, като визуален анализ, корелационен анализ, скорост на криптиране, пиково съотношение сигнал/шум(PSNR), съотношение сигнал/шум и брой променени фрагменти в проценти (NSCR).

ЛИТЕРАТУРА:

[1] Kordov, K. (2019). A novel audio encryption algorithm with permutation-substitution architecture. Electronics, 8(5), 530.

[2] Farsana, F. J., & Gopakumar, K. (2016). A novel approach for speech encryption: Zaslavsky map as pseudo random number generator. Procedia computer science, 93, 816-823.

[3] R. I. Abdelfatah, "Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations,"in IEEE Access, vol. 8, pp. 69894-69907, 2020, doi: 10.1109/ACCESS.2020.2987197.

[4] Jozwiak, M., Monnet, X., & Teboul, J. L. (2018). Pressure waveform analysis. Anesthesia & Analgesia, 126(6), 1930-1933.

[5] Taylor, R. (1990). Interpretation of the correlation coefficient: a basic review. Journal of diagnostic medical sonography, 6(1), 35-39.

[6] Johnson, D. H. (2006). Signal-to-noise ratio. Scholarpedia, 1(12), 2088.

[7] Korhonen, J., & You, J. (2012, July). Peak signal-to-noise ratio revisited: Is simple beautiful?. In 2012 Fourth International Workshop on Quality of Multimedia Experience (pp. 37-38). IEEE.

[8] Poobathy, D., & Chezian, R. M. (2014). Edge detection operators: Peak signal to noise ratio based comparison. IJ Image, Graphics and Signal Processing, 10, 55-61.

[9] Sathiyamurthi, P., & Ramakrishnan, S. (2017). Speech encryption using chaotic shift keying for secured speech communication. EURASIP Journal on Audio, Speech, and Music Processing, 2017(1), 1-11.

[10] Farsana, F. J., Devi, V. R., & Gopakumar, K. (2020). An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. Applied Computing and Informatics.

[11] Shah, D., Shah, T., & Jamal, S. S. (2020). Digital audio signals encryption by Mobius transformation and Hénon map. Multimedia Systems, 26(2), 235-245.

[12] Ahamad, M. M., & Abdullah, M. I. (2016). Comparison of encryption algorithms for multimedia. Rajshahi University Journal of Science and Engineering, 44, 131-139.

[13] Stoyanov, B., & Ivanova, T. (2021). Novel Implementation of Audio Encryption Using Pseudorandom Byte Generator. Applied Sciences, 11(21), 10190.

Tsvetelina Ivanova
Department of Computer Informatics
Konstantin Preslavsky University of Shumen
9712 Shumen, Bulgaria
e-mail: ts.r.ivanova@shu.bg