International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 July – 2022
DOI:10.46647/ijetms.2022.v06i04.0037 ISSN: 2581-4621

A Review on Audio Encryption Using Chaotic Sequences and Finite Field

Rehda Febin T[1], Rafeeda K[2]
1PG Scholar, Dept. of Computer Science & Engineering, M.Dasan Institute of technology Ulliyeri, Koyilandi, Kozhikode,673620
2AssistantProfessor,Dept.ofComputerScience&Engineering,M.Dasan Instituteoftechnology Ulliyeri, koyilandi, Kozhikode,673620

ABSTRACT

Audio data are used in various fields such as education, engineering, mathematics, art, advertisement, military, medicine, scientific research, and many more. This excessive growth of audio data boosts the importance of multimedia data processing tools and digital documentation. This access to multimedia data through the internet has created inappropriate prospects which are hazardous for the confidentiality and integrity of the data. To encounter these threats, the domain of audio data security gains broad attention. A considerable number of algorithms have been established to protect personal information over open networks. Finite fields are well-studied algebraic structures with enormous efficient properties which have applications in the fields of cryptology and coding theory. Here, an existing system uses lossless binary Galois field extension based efficient algorithm for audio data encryption. The architecture hired a special type of curve in the diffusion module which depends on efficient elliptic curve arithmetic operations. So, it generates pseudo-random numbers (PRN) and with slight computational efforts, it produces optimum diffusion in the encrypted multimedia files. The method is compared with the proposed system using a scheme uses Henon chaotic map and 128-bit AES secret key in order to generate the cipher audio data. Henon chaotic map is a two dimensional iterated discrete dynamic system that shows chaotic character on specific values of the constants used. Chaotic maps are very sensitive to the initial parameters, i.e., a slight change in the initial conditions drastically changes the overall output generated by the chaotic system. The investigational outcomes through different analyses and time complexity demonstrated the ability of the techniques to counter various attacks. Furthermore, two schemes are compared and more appropriate to be applied for data security.

Keywords—Galois field, Henon map, AES, PRN, Cipher data.

1. Introduction

The amount of data that has been stored transmitted over a medium has been increased in the past ten years. The data processing, storage capacity has changed very much in the past decades. One of the reasons is that the emerging technology, and the amount of data created should be handled properly in such a way that the security and confidentiality of the data should not be compromised. The mostly used method to provide security to the data is cryptography. Several cryptographic techniques have been introduced and researches are ongoing in the same area to provide better performance. One of the mostly used techniques is AES. AES is used for all type of data like image, audio and video. Here, in this manuscript a combination of scrambling data, Henon map, AES is used for the encryption of audio data. The resulting values are compared with the method that used ECC and finite fields.

The most prominent field to provide security is cryptography which can be further divided into symmetric and asymmetric key methods. Some of the prominent algorithms such as data encryption standard (DES) [1], international data encryption standard (IDES) [2], triple data encryption standard (TDES) [3], advanced encryption standard (AES) [4], and RSA are widely used for the security purposes and considered as well protected and reliable. Since multimedia data contains a large amount of data that is highly correlated, therefore, the only dependency on the algorithms like AES, RSA, and DES is not good enough for multimedia data security. Since multimedia data contains a large amount of data that is highly correlated, therefore, the only dependency on the algorithms like AES, RSA, and DES is not good enough for multimedia data security.

Finite fields are well-studied algebraic structures with enormous efficient properties which have applications in the fields of cryptology and coding theory. The proposed architecture hired a special type of curve in the diffusion module which depends on efficient elliptic curve arithmetic operations. So, it generates good quality pseudo-random numbers (PRN) and with slight computational efforts, it produces optimum diffusion in the encrypted audio files.

The audio technology is used to store, manipulate, reproduce, and generate the sound using the arrays of the audio signals encoded in digital format. Digital audio also refers to the sample of discreet sequences, which are choosing from the audio wave format. The digital audio data is virtually consisting of discreet sockets that indicate the amplitude of the wave of digital data. Here, manipulate the discrete sockets of the digital audio and encrypt the original content of the original audio. Different analysis methods are performed on both scheme and the scheme using Henon and AES generate better encrypted cypher data.

2. Related works

In the literature, numerous digital audio encryption algorithms are presented. Servetti and De Martin [19] proposed an encryption algorithm for the encryption of telephonic speech relying based on the perception method in 2002.The author recommended two techniques for the encryption of partial speech. The first scheme was envisioned tohave a high bit of rate and low-security capability. Consequently, the cryptanalysis couldeasily reveal the cipheredspeech. But, the second scheme is considered to encryptadditional bitstream, thusprovides more security to theciphered audio. Thorwirth *et al.* [20] gave an algorithm forthe selectiveencryption technique of perceptual audio codingbased on the standard compression in which the author'smainfocus was on examining the encryption of the encodedMP3 files. Subsequently, Servetti *et al.* [21] proposed anMP3 audio selective partial encryption algorithm; the suggested algorithm has considerably low time complexity andalso preserves the contents of the audio information butunfortunately compromises the qualityof the original audiosequences to preserves the perceptual information. Next,in 2004, Bhargava *et al.* [22]proposed four fast encryptionalgorithms for MPEG video, where a key is used to randomly change the sign bitsof the Discrete Cosine Transform(DCT) coefficients and/or the sign bits of motion vectors.These schemes puton a small overhead to the MPEG codec.Grange *et al.* [23] introduced a new framework that relies onrandomized arithmetic coding for the security of multimediadata. In the recommended framework, the securitypurpose ofmultimedia data was achieved by producing some randomness in the arithmetic coding process. In2008, Yan *et al.* [24]introduced progressive multimedia data security by scrambling audio data in a compresseddomain. In the proposedscheme, the secrete MP3 audiowas twisted via a shared secretkey before transmission.However, Zhou and Au [25] showedthat theYan scheme is conquerable against key search attacks.In [26],Lima and Neto presented an encryption scheme fordigital audio that relies on cosine number transform. Theencryption procedure recursively applies to a block of uncompressed audio data and uses simple overlapping toselect theblock and produce diffusion in the encrypted data.

3. Proposed system

After performing an exhaustive literature survey of various image encryption technique, we realize a need of an efficient algorithm which is secure as well as is less complex and fast. It is concluded that the algorithm should perform well on various security parameters so that it may sustain various kinds of attacks. In our work, we designed an approach based upon the Henon chaotic map and externally supplied 128-bit secret key.

3.1 Henon Map

Henon map may be stated as a two-dimensional iterated discrete-time dynamical system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated by two equation.
With x0, y0 as initial point, (x, y) denote the present state of the system. Henon showed that if S is the area bounded by four points (−1.33, 0.42), (1.32, 0.133), (1.245, −0.14) and (−1.06, −0.5), and if the initial point lies in the area S, then the subsequent points (xi, yi) for i ≥ 1, also lie in S [12]. The proposed work generates permutation matrix for shuffling of values of matrix (confusion phase) and cipher data for encryption of the shuffled matrix (diffusion phase) using Henon chaotic map and the 128 bit externally supplied AES secret key. As it is a private key algorithm, we assume the same key to be available at both sender and receiver ends.
Here the original data file is processed and converted to its corresponding matrix.Sampling rate of audio is taken as frequency Fs.Taking a sample of the range10000 and then displayed the audio file as a wave which has time in x axis. Whichis calculated as

Time =1/Fs

Then a prime number is generated, which is higher than the size of the data(>10000). Using this prime number some random numbers are generated stored this value to a variable sigma.Scrambling is done according to sigma. Henon key is generated and XOR operation is done with the previous matrix.Then using AES, a key is generated and encrypted the data.

3.3.Decryption.

For decrypting, we follow the same algorithm in reverse order as of encryption process just replacing the permutation matrix by its inverse which is nothing but its transpose. All other steps remaining the same make the algorithm very simple to implement it on encryption side as well as decryption side.

4.Results and Discussions

4.1Security Analysis

It is mandatory for a standard encryption scheme to counter different kinds of attacks that try to hit the confidentiality, integrity, non-repudiation, and authentication of the data. Here, we evaluate the strength and robustness of the proposed technique against different malicious attacks. These all analyses are performed by using Python on a personal computer.

4.2 Key Space Analysis

Large key-space is required for an efficient digital image encryption algorithm in order to resist brute-force attack. In our proposed algorithm, we use 128-bit external secret key making the key space 2128 and furthermore if we include two seed points of the Henon map as part of secret key, then the key space becomes even larger. If the floating point precision of the machine is 10–14, it makes the key space of the algorithm as large as 2128×1014 * 2 which is enough to resist brute-force attacks.

4.3 Key Sensitivity Analysis

An efficient digital image encryption algorithm needs to be highly key sensitive. The algorithm must give a totally different output even after a slight change of one bit in the security key. In the proposed algorithm, Henon chaotic map is used which due to its chaotic character, is highly sensitive to initial conditions. Also, we are using 128-bit external key for image encryption, which is highly sensitive as well.

4.4 Histogram Analysis

Histogram of an image provides information about the frequency distribution of its pixels and regarding density estimation. Performance analysis is done using the correlation of data.Entropy analysis, differential analysis, correlation analysis, histogram analysis security analysis need to be done to prove the performance of the system.For an audio signal, the average amplitude value is calculated by using the Root mean square (RMS).

$$RMS = \sqrt{\frac{1}{N} \sum_{i=1}^{N} |A_i|^2}$$

4.5 ENTROPY

The amount of uncertainty is measured by using information entropy analysis. The entropy is directly proportional to the rate of uncertainty.

$$H = -\sum_{k=0}^{\mathcal{L}} \mathcal{P}(k) \, log_2 \mathcal{P}(k)$$

4.6 UACI and NPCR

The number of pixel change rates (NPCR) and Unified Average Changing Intensity (UACI),which calculate the sensitivity regarding the cryptosystem.

$$NPCR = \frac{\sum_{u,v} \mathcal{B}(u, v)}{K} \times 100$$

$$UACI = \frac{1}{K} \sum_{u,v} \frac{|\mathcal{A}_1(u, v) - \mathcal{A}_2(u, v)|}{2^K - 1} \times 100$$

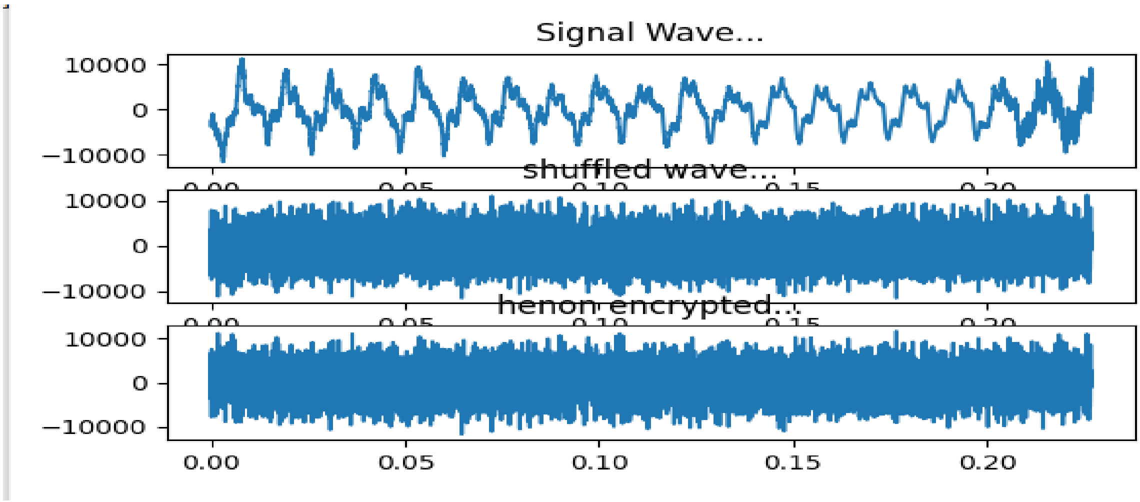
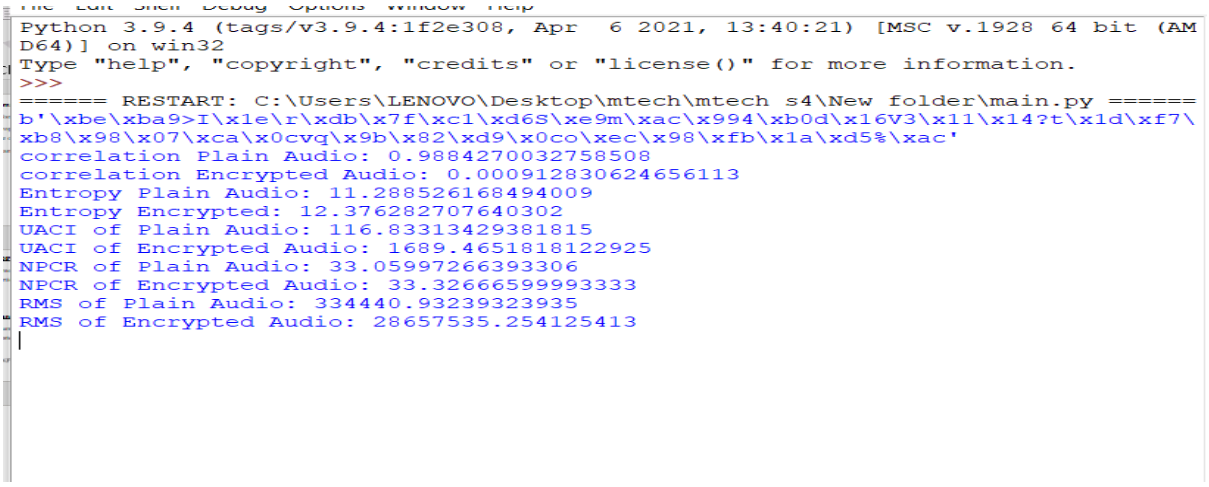


Figure : encryption of audio wave using henon and AES

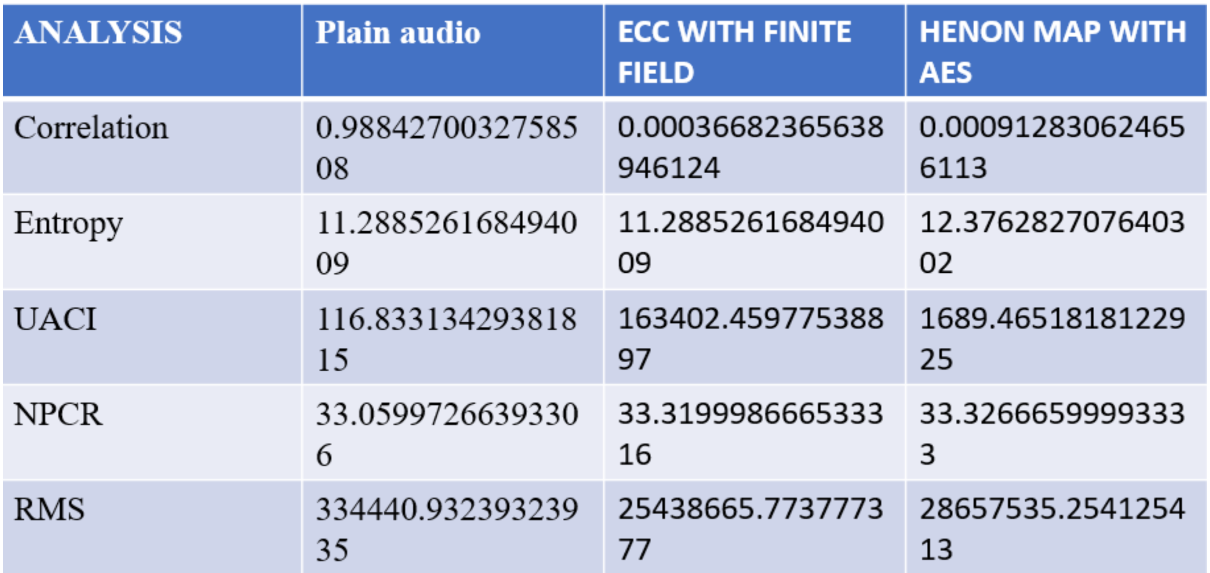


```
Python 3.9.4 (tags/v3.9.4:1f2e308, Apr  6 2021, 13:40:21) [MSC v.1928 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
====== RESTART: C:\Users\LENOVO\Desktop\mtech\mtech s4\New folder\main.py ======
b'\xbe\xba9>I\x1e\r\xdb\x7f\xc1\xd6S\xe9m\xac\x994\xb0d\x16V3\x11\x14?t\x1d\xf7\
xb8\x98\x07\xca\x0cvq\x9b\x82\xd9\x0co\xec\x98\xfb\x1a\xd5%\xac'
correlation Plain Audio: 0.9884270032758508
correlation Encrypted Audio: 0.000912830624656113
Entropy Plain Audio: 11.288526168494009
Entropy Encrypted: 12.376282707640302
UACI of Plain Audio: 116.83313429381815
UACI of Encrypted Audio: 1689.4651818122925
NPCR of Plain Audio: 33.05997266393306
NPCR of Encrypted Audio: 33.32666599993333
RMS of Plain Audio: 334440.93239323935
RMS of Encrypted Audio: 28657535.254125413
|
```

Figure :analysis of system using gallois field

4.7 Comparisons

The two systems are compared and the scheme use henon map and AES is more efficient than the scheme using gallois field. A lossless audio encryption technique that depends on the arithmetic operation of the elliptic curve and Galois field is compared with an another technique. Audio encryption technique that uses AES, Henon map and scrambling is performed. Both scheme is thoroughly securitized over various simulation analyses. The results of the simulation experiment evidenced that the AES with henon map scheme is more secure against various cryptanalysis methods. It is mandatory for a standard encryption scheme to counter different kinds of attacks that try to hit the confidentiality, integrity, non repudiation, and authentication of the data. Here, we evaluate the strength and robustness of the proposed technique against different malicious attacks.



ANALYSIS	Plain audio	ECC WITH FINITE FIELD	HENON MAP WITH AES
Correlation	0.9884270032758508	0.00036682365638946124	0.00091283062465 6113
Entropy	11.288526168494009	11.288526168494009	12.376282707640302
UACI	116.83313429381815	163402.45977538897	1689.4651818122925
NPCR	33.05997266393306	33.3199986665333 16	33.32666599993333
RMS	334440.93239323935	25438665.773777377	28657535.254125413

Table: comparison of two scheme

5. Conclusion

In this manuscript offered a lossless audio encryption technique that depends on the arithmetic operation of the elliptic curve and Galois field. Initially, introduced a novel random number generator scheme, which is used to generate quality random numbers and passed all the tests successfully. The generated random sequence is then used to shuffle the original audio data set. In the confusion phase of the idea, a new S-box construction scheme is deployed, which generates multiple S-boxes without much computational effort. The S-boxes are then used to substitute the shuffled audio. The substitution with multiple S boxes produced optimum confusion in the encrypted and make capable the scheme robust against differential attacks.In this paper, a new method for multimedia encryption is proposed. The technique is based upon using chaotic properties of Henon map as pseudo-random number generator along with 128 bit secret key to obtain permutation matrix for shuffling of the original image and a cipher image that is used to finally encrypt the shuffled image. The method is vigorously tested on standard test images based upon various security parameters of digital image encryption. The focus is kept on keeping the mechanism simple enough, making it easy to implement in practical applications. The future scope of the work may constitute the optimization of the algorithms for applications in sensor nodes and military applications where the processing ability of the nodes is extremely low. As, any algorithm that is costly in terms of computational cost, that can not be implemented in the discussed scenario. The scheme was thoroughly securitized over various simulation analyses. The results of the simulation experiment evidenced that the proposed scheme is secure against various cryptanalysis methods. Accordingly, the proposed scheme is secured and suitable for multimedia data encryption applications.

6.References

[1] *Data Encryption Standard (DES)*, Standard FIPS PUB 46-3, 1999.

[2] S. Basu, ``International data encryption algorithm (IDEA)_A typicalillustration,'' *J. GlobalRes. Comput. Sci.*, vol. 2, no. 7, pp. 116_118, 2011.

[3] E. Barker and N. Mouha, ``Recommendation for the triple data encryption algorithm(TDEA) block cipher,'' Nat. Inst. Standards Technol.,Gaithersburg, MD, USA, Tech. Rep.NIST SP 800-67, Revision 2, 2017.

[4] J. Daemen andV. Rijmen, ``Reijndael: The advanced encryption standard,"*Dr. Dobb's J.,Softw. Tools Prof. Programmer*, vol. 26, no. 3, pp. 137_139,2001.

[5] Y. Naseer, D. Shah, and T. Shah, ``A novel approach to improve multimediasecurityutilizing 3D mixed chaotic map," *Microprocessors Microsyst.*,vol. 65, pp. 1_6, Mar. 2019.

[6] A. Algha_s, H. M. Waseem, M. Khan, and S. S. Jamal, ``A hybridcryptosystem for digitalcontents con_dentiality based on rotation ofquantum spin states," *Phys. A, Stat. Mech. Appl.*,vol. 554, Sep. 2020,Art. no. 123908.

[7] Y. Naseer, T. Shah, and D. Shah, ``A novel hybrid permutation substitutionbase coloredimage encryption scheme for multimedia data," *J. Inf. Secur.Appl.*, vol. 59, Jun. 2021, Art. no. 102829.

[8] U. Arshad, M. Khan, S. Shaukat, M. Amin, and T. Shah, ``An efficientimage privacyscheme based on nonlinear chaotic system and linear canonical transformation," *Phys. A, Stat.Mech. Appl.*, vol. 546, May 2020,Art. no. 123458.

[9] D. Shah, T. Shah, and S. S. Jamal, ``A novel efficient image encryptionalgorithm based onaffine transformation combine with linear fractionaltransformation," *Multidimensional Syst.Signal Process.*, vol. 31, no. 3,pp. 885_905, Jul. 2020.

[10] M. Tanveer, T. Shah, A. Ali, and D. Shah, ``An efficient imageprivacy-preserving schemebased on mixed chaotic.

[11] Chen, C.-S., Chen, R.-J.: Image encryption and decryption using SCAN methodology. In: 7thInternational Conference on Parallel and Distributed Computing, Applications and Technologies,2006. PDCAT06, pp. 61–66. IEEE (2006)

[12] Sankpal, P.R., Vijaya, P.A.: Image encryption using chaotic maps: a survey. In: 2014 Fifth International Conference on Signal and Image Processing (ICSIP), pp. 102–107. IEEE (2014)

[13] Rajput, A.S., Mishra, N., Sharma, S.: Towards the growth of image encryption and authenticationschemes. In: 2013 International Conference on Advances in Computing, Communicationsand Informatics (ICACCI), pp. 454–459. IEEE (2013)

[14] Jolfaei, A., Mirghadri, A.: An image encryption approach using chaos and stream cipher. J.Theor. Appl. Inf. Technol. **19**(2), 117–125 (2010)

[15] Kumar, M., Aggarwal, A., Garg, A.: A review on various digital image encryption techniquesand security criteria. Int. J. Comput. Appl. **96**(13) (2014)

[16] Wei-bin, C., Xin, Z.: Image encryption algorithm based on Henon chaotic system. In: 2009International Conference on Image Analysis and Signal Processing. IEEE (2009)

[17] Ping, P.,Mao, Y., Lv, X., Xu, F., Xu, G.: An image scrambling algorithm using discrete Henonmap. In: 2015 IEEE International Conference on Information and Automation, pp. 429432.IEEE (2015)

[18] Nithin, N., Bongale, A.M., Hegde, G.P.: Image encryption based on FEAL algorithm. Int. J.Adv. Comput. Sci. Technol. (2013)

[19] Hamad, S., Khalifa, A., Elhadad, A., Rida, S.Z.: A modified playfair cipher for encryptingdigital images. Mod. Sci. (2013)

[20] Soleymani, A., Nordin, M.J., Sundararajan, E.: A chaotic cryptosystem for images based onHenon and Arnold cat map. Sci. World J. (2014)