# Multiple Fractal Keys Encryption for Audio

**Deepak Negi**
Associate Professor
Amrapali Group of Institutes, Haldwani, U.K. (India)
dr.deepaksinghnegi@gmail.com

**Mahadev**
Assistant Professor
Quantum University, Roorkee, U.K. (India)
mahadev.agra@gmail.com

**Basudeo Singh Roohani**
Assistant Professor
Quantum University, Roorkee, U.K. (India)
bsroohani2007@gmail.com

**Ravindra Sharma**
Assistant Professor
Swami Rama Himalayan University, Jolly Grant,
Dehradun, U.K. (India)
ravindrasharma97@gmail.com

## Abstract.

The security of multimedia applications over communication networks is an important and challenging issue, as they can easily be intercepted. Providing privacy and preventing unauthorized access is a core function of multimedia encryption. The encryption of data is one way keeping content secret in the field of information security. In order to accomplish this objective, the content must be altered and made intelligible only to users of the secret content. This paper is unique in that it uses a dynamical systems and fractals approach to audio file encryption and decryption to achieve completely different results.

**Keywords**. Fractals, Mandelbrot set, Julia Set.

## 1. INTRODUCTION

Internet transactions are reliant on the security of information. Information can be shared across a network using the web, which is a widely popular and interactive medium [9]. Virtually, users are in touch with each other thanks to their multimedia gadgets, which have a positive impact on human life [12]. Initially, the security of electronic networks has been a concern for keeping information secret between the parties. Data integrity, entity reputation, and data authentication are required in order for two parties to communicate securely using an unsecure channel [11]. Participants remain in the dark about the data because the confidentiality guarantees their privacy. The integrity of data refers to the fact that there has been no alteration to it. Cryptography is the science of converting data into unreadable formats called cipher text, which may consist of symbols or a blend of alphabetical characters with symbols [7, 14]. Thus, one can prevent cybercriminals from

gaining access to important data. Algorithms for encrypting data comprise a combination of public keys and function structures. We can infer that securely communicating on the internet, engaging in online transactions, and using secured instant messaging require secure communication [3, 5]. Computing systems rely on cryptography to protect information. Security issues are extremely complex and important for networks. Additionally, not all users engage in legal activities, making crime at networks a widespread issue. Most are linked to financial crimes, and these cases have risen repeatedly in recent years [2, 6]. There is a major issue with wireless devices regarding the loss of confidentiality, content privacy, and location privacy. Moreover, to secure the information on the user, all the identifying information has to be encapsulated in cryptography to prevent it from being accessed by others. With hybrid encryption, we are solving the security issue associated with audio and multi-media formats such as video, text and images [6, 9 and 13].

## 2. PRELIMINARIES

### *1.1. Dynamical systems and fractals*

The concept of fractals is a geometrical structure which has two major physical properties, namely self-similarity and dimension. In a dynamic system, changes take place over time. The dynamics of some systems are predictable whereas others are uncertain, i.e. chaotic [1, 4 and 7].

### *1.2. Mandelbrot set*

The Mandelbrot set define by symbol $M$ to denote the quadratic $Q_c(z) = z^n + c$ is describe as the group of all $c \in C$ where the orbit is bounded at the point 0, such as , $M = \left\{ c \in C : \left\{ Q_c^n(0) \right\}; \quad n = 0,1,2,3...is\,bounded \right\}$ [3, 12].

$M = \left\{ c \in C \left\{ Q_c^{\,n}(0)\, does\, not\, tends\, to \infty\, as\, n \to \infty \right\} \right\}$ we choose the initial point $0$, as $0$ is the only critical point of $Q_c$ [2, 4].

### *1.3. Julia set*

The Julia set is related to the set of points whose orbit is described by the function $Q_c(z)$. When the starting point is chosen as $0$, since $0$ is the most important critical point in iteration function $Q_c(z)$ [3, 5 and 8].

## 3. PROPOSED ALGORITHM FOR AUDIO FILES

Our discussion in this section centres on the encryption and decryption processes in sine wave form and their respective histograms. The histogram represents graphical information about data. The proposed audio encryption and decryption method implements fractal keys that are beneficial in keeping data secure [1, 14]. We used the common

"WAV" format file to test the scheme, since they are widely used as digital audio file formats on computers. In these formats, more information is provided about the data and higher quality audio is provided, as the waveform audio format has the sine wave, which is the simplest waveform, with only one frequency associated with it. Plain text of the audio file containing numeric data with the keys, superimposed on the matrix, yields the cipher text in mash format [3]. A picture of the original file in sine format can be seen in fig 1. As shown in fig 2, the encrypted sine file requires modifications after encryption, such that it is different from its original sine file format. The encrypted sine file after decryption yields its original sine file format, see fig 3.

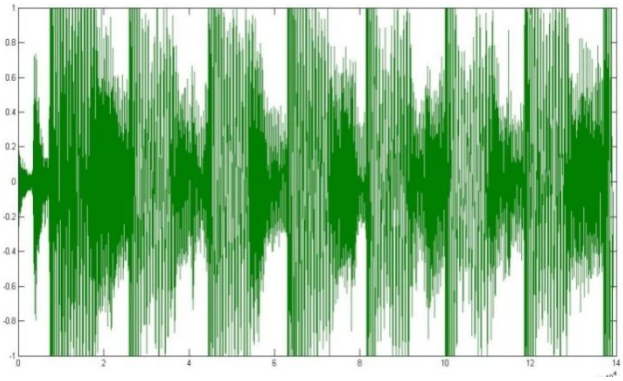
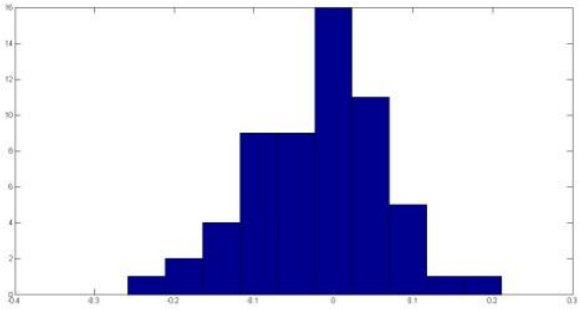


Fig1. Original audio file



Histogram original audio file

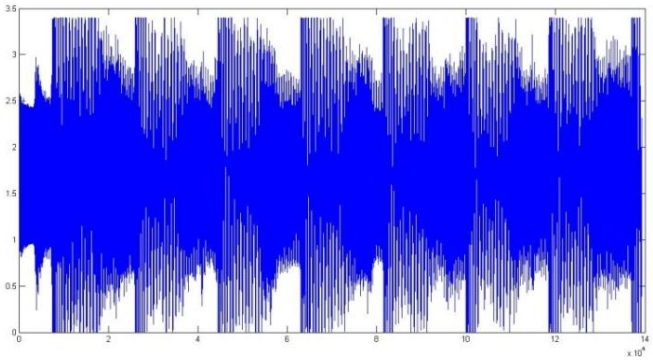
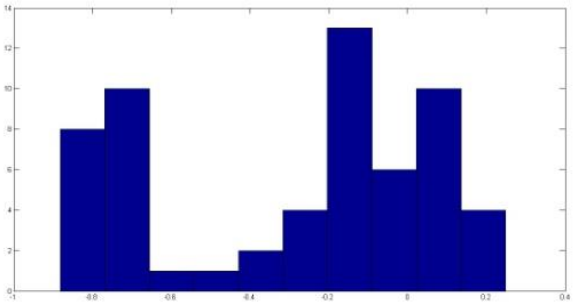


Fig2. After encryption



Histogram after encryption audio file

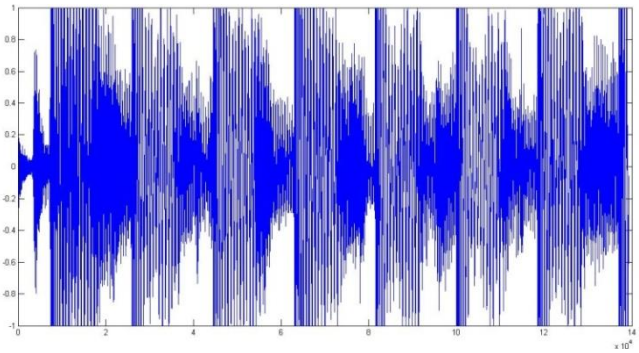
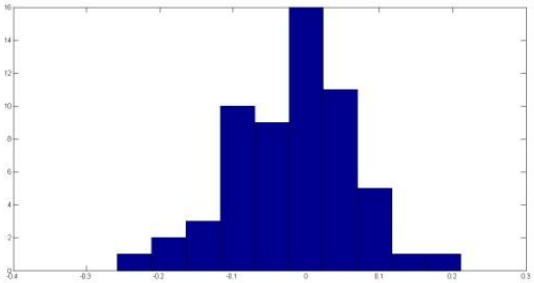


Fig3. Decrypted



Histogram decrypted audio file

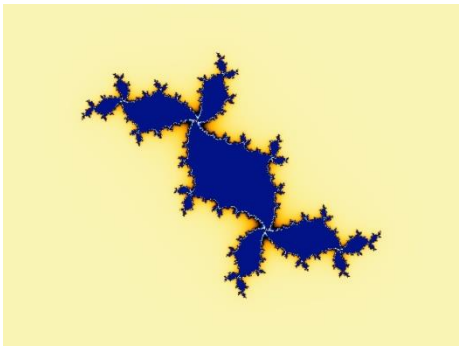


Fig4. Connected Julia set for( -0.16875 , 0.775*i* )

**AT TRANSMITTER SIDE**

**First Step:** From the connected Julia set transmitter chooses one public key $c$ .

**Second Step:** To generate the three private keys $d, d', d''$ , a public key $c$ is used along with a function $f(n)$ .

**Third Step:** Read original audio ***wav*** file.

**Fourth Step:** Audio ***wav*** file is superimposed with private keys.

**Fifth Step:** Encrypted audio ***wav*** file is sent to the recipient.

**AT RECIPIENT SIDE**

**First Step:** An encrypted audio ***wav*** file is received by the receiver.

**Second Step:** To generate the three private keys $e, e', e''$, a public key $c$ is used along with a function $f(n)$.

**Third Step:** A private keys $e, e', e''$ is used to decrypt an encrypted audio ***wav*** file

## 4. RESULTS AND DISCUSSIONS

### *4.1. Encryption and Decryption Process*

There are connections between all Julia sets in the Mandelbrot set [1, 7 and 14], the proposed method begins by choosing a public key, $c$, and a connecting parameter over the connected Julia set corresponding to $f(n)$. A random Julia set is chosen. A fixed point along the iteration function $f(n)$ for each of the three private keys is used to initialize them; Finally, the audio wav file is encrypted by these three private keys and throw over the Network channel. Reversing the decryption process at the receiver end is necessary for the decryption to occur. We can generate the private keys by applying the public key and function to the received encrypted message and by applying these keys to the original audio data we can obtain the original audio data. A detailed description of the system works is given in Table 1.

| Description of Process | Transmitter Side | Recipient Side |
|---|---|---|
| **Select a complex public key** $c$ | -0.16875 , 0.775*i* | -0.16875 , 0.775*i* |
| **Generate private keys** $d, d', d''$ **along with function** $f(n)$ | 0.1002 - 0.0098i<br>-0.1588 + 0.7730i<br>-0.7411 + 0.5295i | 0.1002 - 0.0098i<br>-0.1588 + 0.7730i<br>-0.7411 + 0.5295i<br>$e, e', e''$ |

| **Superimpose audio message along with function** | $f(n) = f_e(msg)$<br>0.1002 - 0.0098i<br>-0.1588 + 0.7730i<br>-0.7411 + 0.5295i<br>$d, d', d''$ | $f(n) = f_e(msg)$<br>0.1002 - 0.0098i<br>-0.1588 + 0.7730i<br>-0.7411 + 0.5295i<br>$e, e', e''$ |
|---|---|---|
| **Encrypted message** | 0.2331 -0.8661 -0.1077 -0.3541 -0.7894 0.1861 -0.1002 -0.8271 -0.0794 -0.2916 -0.7765 0.0455 -0.3653 -1.0380 -0.0883 -0.1666 -0.6951<br>0.0689-0.5416 -1.0467 -0.0873 -0.3772 -1.0927 -0.3486 -0.6666 -1.3204 -0.5092<br>-0.6673 -1.0380 -0.0080 -0.2291 -0.9251 -0.2123 -0.4713 -0.9208<br>0.0406-0.2604 -1.0306 -0.3451 -0.5891 -1.0380 -0.1116 -0.4244 -1.1099 -0.2514-0.3676 -0.8896 -0.1800 -0.5729 -1.0888 -0.0717 -0.2538 -0.8817 -0.0862 | 0.2331 -0.8661 -0.1077 -0.3541 -0.7894 0.1861 -0.1002 -0.8271 -0.0794 -0.2916 -0.7765 0.0455 -0.3653 -1.0380 -0.0883 -0.1666 -0.6951<br>0.0689-0.5416 -1.0467 -0.0873 -0.3772 -1.0927 -0.3486 -0.6666 -1.3204 -0.5092<br>-0.6673 -1.0380 -0.0080 -0.2291 -0.9251 -0.2123 -0.4713 -0.9208<br>0.0406-0.2604 -1.0306 -0.3451 -0.5891 -1.0380 -0.1116 -0.4244 -1.1099 -0.2514-0.3676 -0.8896 -0.1800 -0.5729 -1.0888 -0.0717 -0.2538 -0.8817 -0.0862 |
| **Type of message** | **Encrypted audio Message**<br>$f(n) = f_e(msg)$ | **Decrypted audio Message** |

Table 1: Protocol for exchanging keys based on Fractals

## 5. CONCLUSION

In modern communication technologies, security is a crucial issue. Therefore, we must utilize a technique called cryptography to ensure the security of digital communications. As the Mandelbrot set contains infinite number of Julia sets, this paper provides a method that is efficient for encrypting and decrypting the audio "WAV" files. It is this property that allows researchers to use complex numbers and fixed point iterations to design efficient encryption/decryption codes. The Mandelbrot and Julia fractal sets are intrinsically connected to each other, so selecting a random key for each of these sets is possible. The level of security is, therefore, extremely high

## 6. REFERENCES


[1] D. Gulick, "CHAOS AND FRACTALS."

[2] D. Negi and A. Negi, "A behavior of Tricorns and Multicorns in N-Orbit," *International Journal of Applied Engineering Research,* vol. 11, pp. 675-680, 2016.

[3] D. Negi, A. Negi, and S. Agarwal, "The complex key cryptosystem," *International Journal of Applied Engineering Research, ISSN,* pp. 0973-4562, 2016.

[4] G. A. Edgar, Classics on fractals: CRC Press, 2019.

[5] G. Emmanuel, G. G. Hungilo, and Pranowo, "Numba acceleration of image steganography using Mendelbrot set fractals," in *AIP Conference Proceedings*, 2020, p. 030009.

[6] I. El Hanouti and H. El Fadili, "Security analysis of an audio data encryption scheme based on key chaining and DNA encoding," *Multimedia Tools and Applications,* vol. 80, pp. 12077-12099, 2021.

[7] M. Akhmet, M. O. Fen, and E. M. Alejaily, "Dynamics with fractals," *Discontinuity, Nonlinearity, and Complexity,* vol. 10, pp. 173-184, 2021.

[8] M. Khan, F. Masood, and A. Alghafis, "Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system," *Neural Computing and Applications,* vol. 32, pp. 11837-11857, 2020.

[9] M. T. GENÇOĞLU, "Enhancing The Data Security by using Audio Steganography with Taylor Series Cryptosystem," *Turkish Journal of Science and Technology,* vol. 16, pp. 47-64, 2021.

[10] S. Agarwal, "A fractal based image cipher using Knuth shuffle method and dynamic diffusion," *IJCNC,* vol. 11, pp. 81-100, 2019.

[11] S. Agarwal, "Preserving Information Security Using Fractal-Based Cryptosystem," in *Handbook of Research on Cyber Crime and Information Privacy*, ed: IGI Global, 2021, pp. 539-566.

[12] S. Banerjee, M. K. Hassan, S. Mukherjee, and A. Gowrisankar, *Fractal Patterns in Nonlinear Dynamics and Applications*: CRC Press, 2020.

[13] T. Mythili, A. Sofiabanu, R. Mohanasundari, and K. Sreekanth, "Data Hiding with Image and Audio Steganography Cryptosystem in Network," *International Journal of Recent Trends in Engineering & Research,* vol. 5, pp. 5-10, 2019.

[14] W. R. Smith, *Chaos, Fractals, and Dynamics*: CRC Press, 2020.

**Biographies**

**Dr. Deepak Negi** received his Bachelor of Science degree from Kumaun University Nainital, India in 2006. He received Masters in Computer Science degree from Uttarakhand Technical University, Dehradun India in 2009 and Doctorate in Computer Science and Engineering degree from Uttarakhand Technical University, Dehradun India in 2018. My area of research is application of fractal and dynamical systems, Network security, databases and data privacy.

**Dr. Mahadev** received his PhD degree in Computer Science from Gurukula Kangri Vishwavidyalaya, Haridwar in 2019. He received MCA degree from Dr. B. R Ambedkar University, Agra in 2001. His area of specialization is in web Technology and Machine Learning

**Mr. Basudeo Singh Roohani** received his bachelor degree in Computer Science. & Engineering from Bundelkhand Institute of Engineering & Technology (BIET) in 1999, Jhansi, Uttar Pradesh, India. He received a Master's degree in Computer Science and Engineering from Uttar Pradesh Technical University in 2006 Lucknow, Uttar Pradesh, India.. He is currently pursuing. Doctorate in Computer Science and Engineering degree from Dr. A.P.J. Abdul Kalam Technical University Lucknow,Uttar Pradesh, India. His research areas include Artificial Intelligence and Machine Learning.