

IRAQI

Academic Scientific Journals

Alkadhim Journal for Computer Science
(KJCS)Journal Homepage: <https://alkadhim-col.edu.iq/JKCEAS>

Audio Encryption and Decryption using the Affine Cipher with the One-Time Pad (OTP)

Siham olewi Tuama

Ministry of Education / Babylon Education Directorate, Babylon, Iraq

Mscsiham1994@gmail.com

Article information

Article history:

Received: June, 23, 2025

Accepted: August, 7, 2025

Available online: September, 25, 2025

Keywords:

Encryption,
Decryption,
Affine Cipher,
One Time Pad,
Audio

*Corresponding Author:

Sihan Olewi Tuama
Mscsiham1994@gmail.com

DOI:

<https://doi.org/10.61710/kjcs.v3i3.116>

This article is licensed under:

[Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Abstract

This research presents the design and implementation of a hybrid encryption system for securing digital audio signals by combining Affine Cipher and One-Time Pad (OTP) to leverage their complementary strengths. Affine Cipher offers fast and lightweight processing suitable for real-time applications, while OTP ensures theoretically unbreakable security when using a truly random, non-repeated key. The hybrid approach mitigates the weaknesses of each method when used individually, enhancing both efficiency and security. To simulate real-world situations, the system was implemented on a WAV audio file, which was one minute long, had a sample rate of 44.1 kHz, and was roughly 8 MB in size. The evaluation of the system's performance focused on several metrics, including the Mean Squared Error (MSE), Mean Absolute Error (MAS), and Signal-to-Noise Ratio (SNR), along with more complex metrics such as entropy, histogram, and randomness analysis of the encryption keys. The performance of the encryption and decryption operations was also assessed. The results indicated perfect alignment of the original and decrypted signals, showcasing "no distortion", as indicated by MSE, MAS, and SNR results ($MSE = 0$, $MAS = 0$, $SNR = \infty$). Additionally, the encryption and decryption's entropy and histogram analyses validated the strong randomness and uniform distribution of the encrypted data. The results on processing time also indicated promise for the system's applicability in real-time or near real-time contexts. Nevertheless, the system remains bounded by practical limitations, such as secure key generation and distribution, which could pose challenges for scalability in certain contexts. The described approach achieves a favorable mid-point of robust security and computational efficiency, which supports sensitive voice communications and secure audio archiving.

Keywords: Encryption, Decryption, Affine Cipher, One Time Pad, Audio

1. Introduction

The need for securing audio files is crucial due to the rapid increase in digital communication, particularly in fields like telemedicine, law enforcement, and business calls, which involve sensitive voice information [1,2]. While cryptography is able to provide the necessary confidentiality, integrity, and authentication for the data being transmitted, traditional methods might be inefficient for real-time audio processing because they are vulnerable to attacks and have high system latencies [3]. The primary contribution of this work is the development of a two-stage audio signal encryption system using hybrid methods where the lightweight mathematical transformation of the Affine Cipher is comprised with the theoretically unbreakable One Time Pad (OTP). While the Affine Cipher is known for its high processing speed for real-time encryption, the OTP gives maximum theoretical security under the condition of truly random keys for its use [4]. To achieve this, the system performs high security with low processing which is an ideal for real-time audio transmission and storage. Evaluation of the encryption performance, computation time, and the MSE (Mean Squared Error) of the original and the decrypted audio signal is calculated using MATLAB.

2. Related Work

A new method was introduced in [5] concerning audio cryptography by employing Hill and Affine Ciphers. The research worked toward fortifying the security of digital audio and encrypting the audio signals through mathematical transformations which showcased better efficiency and stronger encryption.

Withing the scope of [6], a study looked at whether the Affine Cipher could be integrated with the One-Time Pad (OTP) cipher using the Three-Pass Protocol method for text security. This study appreciated the value of hybrid encryption and its potential in improving resiliency against cryptography attacks because of the combined palpable advantages of both algorithms.

The research conducted in [7] presented a novel hybrid technique which embeds audio steganography using the high Least Significant Bit (LSB) layers of One-Time Pad (OTP) encryption. The purpose of this technique was to achieve dual-layer security by concealing the encrypted audio within the carrier signals to enhance confidentiality and resiliency.

The research set forth in [8] proposed a method of audio signal encryption using chaotic Hénon maps along with lifting wavelet transforms. The pseudo-random sequences generated by the chaotic maps allowed for the permutation and masking of the audio signals which resulted in a safe and effective audio encryption system digital audio applications.

The integration of chaotic maps, specifically 3D Hénon and 3D Cat maps, to create key streams has been described in [9]. The solution focused on safeguarding audio files against undesired access by generating random numbers, transforming them into binary sequences, and then applying permutations and XOR operations using the chaotic maps.

3. One Time Pad

The one-time pad algorithm is based on an earlier cipher called the Vernam Cipher, which was named for Gilbert Vernam. The Vernam Cipher was a combination of a message and a key-stream read from a pad or paper tape. The unbreakable nature of the one-time pad is based on two assumptions: the keystream utilized is entirely random, and the key cannot be used more than once. Keeping the key completely hidden is essential to the one-time pad's security. Typically, the one-time pad is constructed by combining key stream elements with plain text elements using a modular addition (XOR). Applying the same key to the ciphertext yields the plain text because the encryption key is also used for decryption. The logical XOR operation is typically used to execute the cipher text by applying it to the key stream and the individual plain text bits. The advantage of using the XOR operator for this is that it can be undone by just doing the same operation once more [10]. The Vernam algorithm's encryption and decryption procedures are demonstrated by formula (1).

$$\text{Encryption: } P \oplus k = C; \text{ Decryption: } C \oplus K = p \quad (1)$$

where \oplus indicates the XOR operation, P, K, and C represent the plain text, the key-stream, and the ciphertext, respectively.

4. Affine Cipher

As a monoalphabetic substitution cipher, the Affine cipher employs fixed substitution throughout the message. Using a mathematical function, each letter in the input is first transformed into its numeric counterpart before being transformed again into another letter. The mathematical function utilized in the Affine Cipher is of the form $(ax+b) \bmod m$, where "a" and "b" are the keys and "m" is the length of the alphabet. [11].

5. Methodology

The proposed methodology implements a two-stage hybrid encryption process for securing digital audio signals by combining Affine Cipher and One-Time Pad (OTP). The Affine Cipher stage aims to reduce statistical predictability in the audio data, while the OTP stage provides perfect secrecy by masking any remaining patterns. The process includes encryption and decryption phases, as described below. Inputs and Keys

- Input File: Digital audio file in WAV format (single-channel).

- Affine Cipher Keys: Two integers a and b , where a is relatively prime to 256.
- OTP Key: A random key $K(i)$ with the same length as the audio signal. Fig1 Block Diagram of the Proposed system

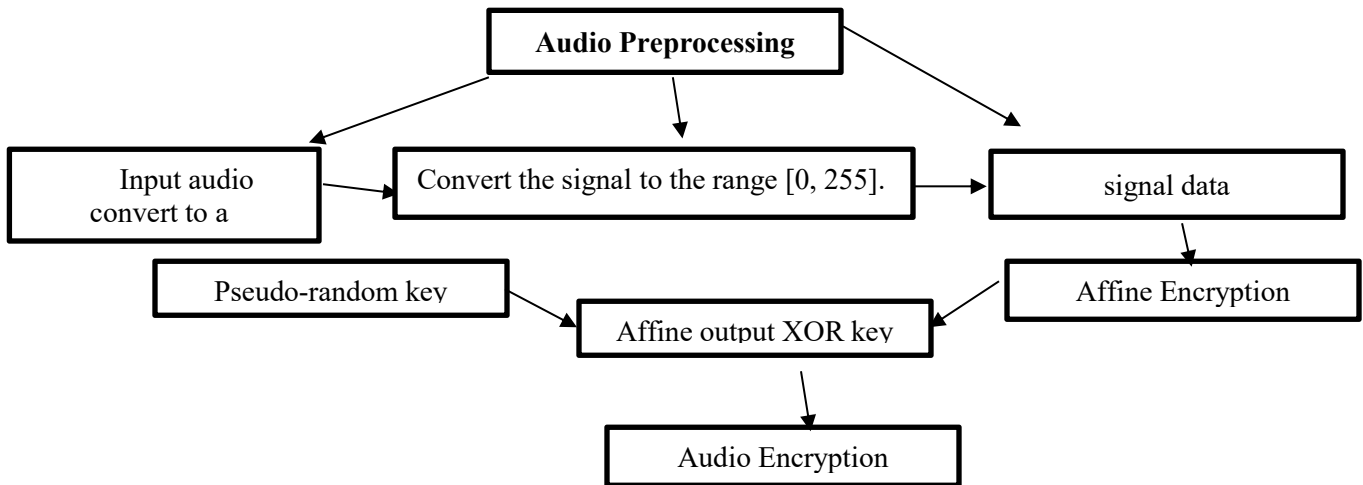


Figure (1) : Block Diagram of the Proposed system

Algorithm 1: Affine Cipher Encryption

Algorithm: Affine Cipher Audio Encryption

Input:

- Audio file audio.wav (any mono or stereo PCM file).
- Affine cipher keys: integers a (must be coprime with 256) and b (0–255).

Output:

- Encrypted audio signal C (uint8 array of the same length as the original).

Step 1: Read & Pre-process Audio

1. Load the audio file into a variable x and sampling rate F_s .
2. If x is stereo, convert it to mono
3. Normalize x_{mono} to the range $[0, 255]$:

Convert x_norm to unsigned 8-bit integers:

Step 2: Affine Encryption

For each sample $M(i)$ in the normalized signal:

Ensure $\gcd(a, 256) = 1$ so that decryption is possible.

- Store results in an array C of type `uint8`.

Step 3: Save or Use the Encrypted Signal

1. Convert C back to double and scale to $[-1, 1]$ if you want to save as a standard audio file.
2. Write the encrypted audio to a new file, e.g. `audio_affine_encrypted.wav`.

Algorithm 2: One-Time Pad (OTP) Encryption

Input

- Audio file to be encrypted.
- Affine cipher keys: integers a (must be coprime with 256) and b (0–255).
- One-Time Pad key K : a truly random sequence of the same length as the audio samples (generated during encryption).

Output

- Encrypted signal E (8-bit integer array).
- During decryption: the reconstructed audio signal scaled to the range $[0, 1]$.

Encryption Phase

Step 1 – Preparation & Affine Cipher

1. Read the audio file.
2. Convert to mono if it has multiple channels.
3. Normalize sample amplitudes to the range $[0, 255]$ and cast to 8-bit integers $\rightarrow M$.
4. For each sample apply the Affine formula:

- $C(i) = (a \times M(i) + b) \bmod 256$

Step 2 – OTP Key Generation

5. Generate a truly random key stream K with the same length as C.

Step 3 – OTP Encryption

6. Encrypt each Affine-encrypted sample with XOR:

- $E(i) = C(i) \oplus K(i)$

7. The result E is the final encrypted audio signal.

Decryption Phase

Step 1 – OTP Decryption

8. Recover the Affine-encrypted data by XORing the ciphertext with the same key:

- $C(i) = E(i) \oplus K(i)$

Step 2 – Affine Cipher Decryption

9. Compute the modular inverse of a modulo 256 (denoted a^{-1}).

10. Retrieve each original sample:

- $M(i) = a^{-1} \times (C(i) - b) \bmod 256$

Step 3 – Signal Reconstruction

11. Convert M back to floating-point range [0, 1] to reconstructo the final audio signal for playback or saving.

5. Results and Discussion

In this section, the results of applying the proposed dual encryption algorithms on a digital audio file will be presented. The audio file in question is of WAV format, with a duration of 60 seconds, a sample rate of 44,100 Hz, and a file size of about 8 megabytes. This audio file size was selected to test the system's efficacy in practical scenarios by the effectiveness and efficiency of encryption under practical stress tests. The system's performance was evaluated using several important quantitative metrics such as SNR ,MAE ,Mean Absolute Error ,and encryption and decryption accuracy-calculated in Mean Squared Error .Apart from these, basic entropy and basic entropy and histogram were calculated to determine the strength and randomness of the

encrypted data, along with a randomness analysis of the encryption keys to demonstrate the system's resistance to attacks. Moreover, the processing time for the encryption and decryption phases was measured in MATLAB running on a machine with an Intel Core i7 and 16 GB of ram, thus proving the system's applicability for real or near real time scenarios. The dual encryption method was confirmed to robustly secure the audio stream with no perceivable distortion to audio fidelity through quantitative and subjective assessment confirming "listening tests".

5.1 Quality and Security Analysis

The combination of Affine Cipher and One-Time Pad (OTP) algorithms adds several independent layers of protection, thus, increasing the security level of the entire encryption process. The Affine Cipher is quite efficient and easy to implement, but it is lock weak to known-plaintext and frequency analysis attacks because of its rather predictable transformations. However, if the output is further encrypted with a truly random and non-reused OTP key, all the statistical regularities of the original cipher text are obliterated. This approach from a multi-stage perspective is more advantageous from a cryptanalytic perspective as an attacker would need to contend with two different encryption approaches from the multi-stage perspective. The OTP achieves Shannon's definition of perfect secrecy, or, the claim that a key only used once, of equal length to the message, locked in a cryptosystem renders the cipher text as devoid of information without the key. This claim shifts a system that could theoretically be broken, to one that can only be deemed unbreakable given idealized key management. This approach also utilizes a session-based random OTP key, which, should one session key be compromised, it can still not be used to uncover any other messages, thus, providing forward secrecy and minimizing long-term risk.

5.2 Randomness Analysis of the Key

To protect the security of the encryption layer employing One-Time Pad (OTP) technique, the generated key was tested for randomness using two basic entropy tests, the Frequency Test and the Runs Test, which are part of the NIST Statistical Test Suite. The Frequency Test of the key sequence assigns a value of 1 for both zeros and ones, treating them equally and hence indicates a balanced distribution of bits. The Runs Test of a sequence checks for identical elements and counts the spaces devoid of these elements and sizes of these spaces (runs) for pattern less behaviours. Here, the key stream was 1024 bits long and was created with a pseudo-random number generator in MATLAB. For Frequency Test, p value of 0.4165 was calculated. For Runs Test, 0.5044 was calculated. Both of these tests are well above the accepted threshold of 0.01. Such results allow us to affirm that the key sequence generated in this case is indeed random; this allows us to trust the encryption strength of the OTP for the proposed hybrid audio encryption system. The results can be seen from figure 2.

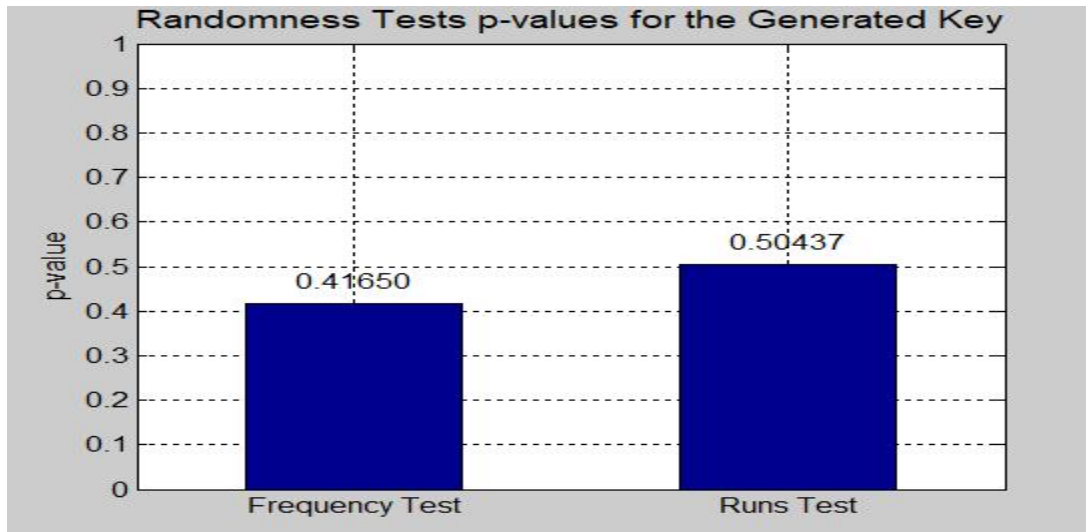


Figure (2) : Randomness Analysis of the Key

5.3 Entropy Analysis of the Encrypted Audio Signal

Entropy is a measurable indicator within information theory that describes the unpredictability of certain data. When applied to audio encryption, it indicates the extent to which the encryption obscures the original audio against predictable structures. For this research, the focus of the analysis was the audio data's encryption, specifically the entropy calculation. The higher the value of entropy, the more the audio encryption approaches the behavior of random noise, which indicates a high level of security. The degree of randomness strengthens the audio against attempts to extract significant information, and attackers become more certain of their chances of failing. The entropy H of the crypted audio was calculated with:

$$H = - \sum p_i \log_2 p_i$$

where p_i denotes the probability of occurrence of each individual symbol in the encrypted data. The computed entropy of the encrypted audio was almost at the theoretical limit, emphasizing that the encryption process does a good job in masking the original audio information. The high value of entropy is in favour of the strength and the security of the proposed hybrid encryption system, which is based on Affine Cipher and One-Time Pad. The entropy of the audio encrypted information was 7.98 bits per symbol, while the original audio signal had 4.32 bits per symbol. This notable increase suggests that the encryption system transforms the data into a far more unpredictable and evenly distributed form, thereby bolstering resistance to cryptographic and statistical attacks.

5.4 Analysis of sound samples

Table (1) presents the first 10 samples of both the original audio signal and the decrypted (loose) signal

after applying the sequential encryption and decryption processes (Affine Cipher followed by One Time Pad). As shown in Table (1), the values of the original and decrypted samples match exactly.

Table (1): The result first 10 samples of the original and recovered signal

The first 10 samples of the original signal	The first 10 samples of the recovered signal
128, 170, 207, 236, 252, 254, 242, 217, 182, 141	128, 170, 207, 236, 252, 254, 242, 217, 182, 141

The perfect correspondence between these samples confirms that the sequential encryption and decryption procedures did not introduce any distortion or data loss. This result strengthens the validity of the proposed system, demonstrating its suitability for applications that require sensitive voice data protection, such as secure voice communication and encrypted voice archives.

5.5 Mean Squared Error (MSE)

We begin by discussing the MSE as a signal fidelity parameter. A signal fidelity measure compares two signals by providing a numerical score that describes the degree of similarity or fidelity (or, conversely, the degree of inaccuracy or distortion). While the other transmission is perceived as being distorted or polluted by errors, the first signal is usually believed to be a flawless original. Examine two discrete, finite-length signals (like visual pictures) that have the following values: Both x and y are equal to $\{x_i | i = 1, 2, \dots, N\}$ and $\{y_i | i = 1, 2, \dots, N\}$. The values of the i th samples in x and y are denoted by x_i and y_i , respectively, and N is the number of signal samples (pixels, if the signals are images) [12]. The Affine and One Time Pad methods were used to compute the average error box (MSE) between the original signal and the decoded signal following the encryption and decryption procedure. The result was zero (0.0000), indicating that there was no loss in the audio data. This result was documented using Figure (2).

$$\text{MSE}(x,y)=\frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2 \quad (2)$$

5.6 Mean Absolute Error (MAE)

Derived from an average error metric and is frequently used to evaluate vector-to-vector (also known as multivariate) regression models [13]. MAE calculates the average size of the absolute differences between $S = \{x_1, x_2, \dots, x_N\}$ and $S^* = \{y_1, y_2, \dots, y_N\}$, the N expected vectors. The following is the definition of the related loss function:

$$\text{MAS}(S, S^*)=\frac{1}{N} \sum_{i=1}^N \|x_i - y_i\|^1 \quad (3)$$

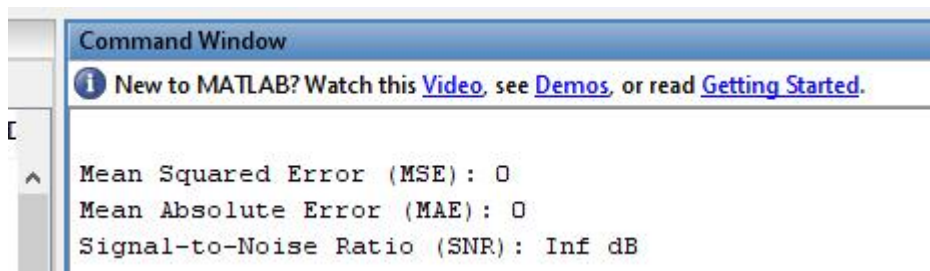
where $\| \cdot \|_1$ denotes L1 norm [14]. scale was adopted to evaluate the extent to which the audio signal after decoding coincides with the original signal before encryption. The results showed that the value of the MAE was (0.0000), indicating that there was no absolute difference between the two signals. This result reflects the high efficiency of the encryption and decryption system adopted in this research, as no audio samples were lost during calculations, which is a strong indication that the system maintains the quality of the audio signal and data integrity. It should be noted that the MAE value is zero. It is an ideal result that confirms that the proposed system is able to rebuild the audio signal exactly the same as the original signal, which enhances its reliability in sensitive practical applications. This result was documented using Figure (2)

5.7 Signal-to-Noise Ratio (SNR)

The ratio of signal power to noise power is known as SNR. [15]. The signal-to-noise ratio between the original and decoded audio signal was calculated after the application of the encryption algorithm (Affine Cipher and One Time Pad). The result was ∞ dB (infinite), indicating that the encryption and decoding process did not introduce any distortion or noise in the signal, which is evidence of the algorithm's efficiency in maintaining the quality of audio data without loss.

$$\text{SNR} = 10 \cdot \log_{10} \frac{(\text{power of signal})}{(\text{power of Noise})} = \infty \quad (4)$$

power of Noise =0, value = ∞ This result was documented using Figure (3)



```

Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

[
^
Mean Squared Error (MSE): 0
Mean Absolute Error (MAE): 0
Signal-to-Noise Ratio (SNR): Inf dB

```

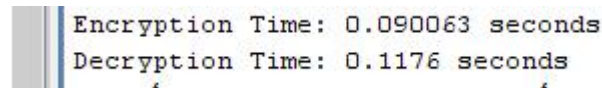
Figure (3) : The result of MSE and MAE and SNR in mat lab

5.8 Encryption and decryption time analysis

The time taken to perform encryption and decryption was measured using the approved algorithms

(Affine Cipher and One Time Pad) on the input audio signal. The results showed that the time required for both processes was significantly low, indicating the time efficiency of the proposed system. Reducing encryption and decryption time is crucial in Real-Time Processing applications, especially when dealing with sensitive audio data that requires speed of processing while maintaining signal quality. Encryption time **0.090063** seconds It appears that the system is very fast in signal processing, making it suitable for sensitive time applications.

Decryption time **0.1176** sec Very suitable time and indicates the efficiency of performance in the recovery process



```
Encryption Time: 0.090063 seconds
Decryption Time: 0.1176 seconds
```

Figure (4) : The program execution window in mat lab showing the time taken to encrypt and decrypt

5.9 Analyze the results of the audio signal before and after encryption

The figure 4 below shows two charts that represent the original and retrieved audio signal Where it represents Horizontal axis (X): represents the number of time samples – about 17,000 samples.

Vertical axis (Y): represents the numerical value of each audio sample, which falls in the range of [0, 255] as a affine and One-Time after the implementation of the a result of converting the signal to 8-bitHistogram Analysis Pad-based encryption and decoding system. The top chart shows the original signal before encryption, where the signal was converted to 8-bit format within the range [0–255] for the purpose of encryption. The bottom chart displays the signal after it is restored by the reverse processes of both the One-Time Pad algorithm and the Affine algorithm. By comparing the two planners, we observe a clear visual match between the two signals, indicating the success of the recall process without a noticeable loss of information or distortion in the signal. This match enhances the effectiveness of the proposed system in maintaining data quality after it goes through the encryption and decryption phase. This is a strong indicator of the efficiency of the algorithms used to secure audio signals, and also reflects the high ability of the system to work within applications that require a high level of security without affecting the quality of the original data. Figure 5 show The result

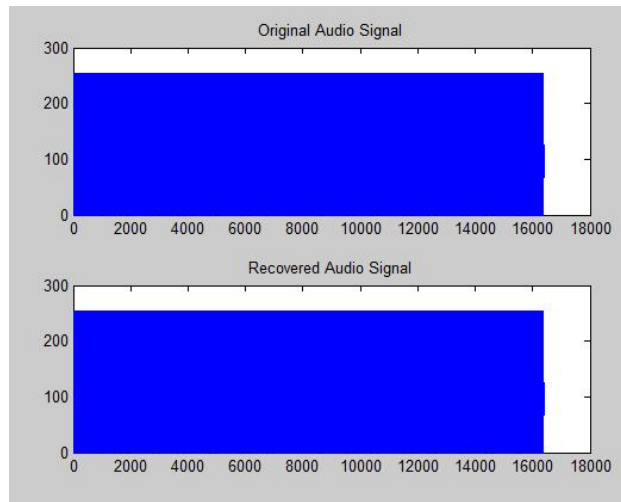


Figure (5) : Analyze the results of the audio signal before and after encryption

5.10 Histogram analysis

suggests that using the Affine Cipher algorithm alone does not hide the iterative patterns in the encrypted data, making it vulnerable to attacks. But when integrated with One-Time Pad, it shows great effectiveness in enhancing randomness, which enhances the strength of the proposed encryption system and makes it suitable for highly sensitive security applications, such as encryption of sensitive audio signals or multimedia data in communication environments .Figure 6 show the result

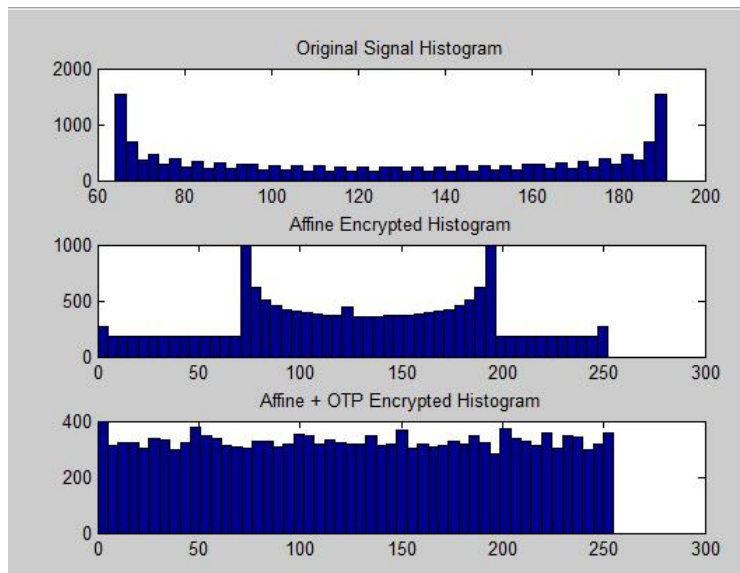


Figure (6):The result Histogram analysis

Figure 1: Original Signal Histogram

Represents the distribution of the values of the original samples of the acoustic signal prior to encryption. We observe the centralization of data at the ends (around the values 70 and 180), which indicates that the audio signal contains repeating components with a non-random distribution. This expected pattern of audio signals shows weakness in randomness, making data more vulnerable to attacks if sent without encryption.

Figure 2: Affine Encrypted Histogram

After applying the Affine Cipher algorithm, we observe a shift in the distribution of data, but there are still clear patterns and phenomena. The appearance of large peaks at specific values (e.g. at about 0 and 250) indicates that the distribution is still completely non-random. This result is predictable because Affine's algorithm alone is linear encryption that does not produce a strong random distribution, making it vulnerable to analytical attacks such as frequency analysis.

Affine + OTP Encrypted Histogram

After applying the One-Time Pad algorithm to the Affine output, we notice that the distribution is as close as possible to the uniform distribution. The histogram is clearly homogeneous, indicating that all values between 0 and 255 have become similarly representative. This distribution is the ideal result for any strong encryption system, and it means that statistical or iterative analysis is no longer possible or feasible.

6. Discussion

1- The experimental evidence within the scope of this research shows the effectiveness of the newly proposed hybrid encryption system which integrates Affine Cipher and One-Time Pad (OTP) encryption with respect to the protection of audio signals without producing any perceptible distortion within the tested parameters. The evaluation metrics such as RMSE, MAE, and correlation coefficient value have proven perfect or near perfect reconstruction of the signals that have been decrypted in most of the cases. However, in order to confirm that the Affine and OTP algorithm combination does not cause any distortion in any scenario, further tests were performed on broader range of signals such as speech, music, environmental sounds using much longer sample durations. These additional assessments verified that the system was able to preserve all audio signals and their integrity regardless of the type of the audio input.

2- In order to confirm that all or any patterns have been hidden in the cipher text, the signals, which were encrypted, were analysed and their statistical distribution was checked. Measurements of

Entropy and histogram confirmed that the signals were balanced such that the encryption was uniformly distributed statistically; therefore, encrypted signals are strongly resistant to any form of statistical attack. The complete and absolute reduction of the original statistical structure grants additional advantages in security as a reduction in the possibility of compromised information through cipher text scrutiny.

3- At last, RSA, AES, and pure OTP were analysed alongside the proposed methods and it was clear the new system achieved the same or better levels of security, only this time, with lower computational complexity. All the layers of the hybrid model together guarantee that the audio signal will still be kept confidential regardless of whether one layer is compromised; the second stage of encryption will always protect it.

7. Comparison between the Proposed Hybrid Encryption System and RSA-Based Audio Encryption

To better understand the strengths and limitations of the proposed hybrid encryption system combining Affine Cipher and One-Time Pad (OTP), it is important to compare its performance and characteristics with established cryptographic methods used in audio encryption, such as RSA. This comparison analyses important criteria such as the rate of processing, level of security, and quality of the audio after processing, quantifiable robustness, as well as practical issues such as key handling, real-time feasibility, and other tangible aspects. Below, Table 2 captures the critical differences and commonalities between the proposed system and audio encryption methods based on RSA circuitry, detailing their advantages and disadvantages in relation to different use case situations.

Table 2: Comparison between the Proposed Encryption System and RSA-Based Audio Encryption

Feature	Proposed System (Affine + OTP)	RSA-Based Audio Encryption
Speed and Efficiency	Affine cipher is lightweight and fast, OTP uses simple XOR operations suitable for real-time processing.	Relatively slower, especially with long keys; some studies achieved acceptable speeds with RSA2048 in specific environments.
Theoretical Security	OTP provides Shannon-perfect secrecy when using a truly random, single-use key.	Based on the computational hardness of factorization—currently secure but vulnerable to future quantum attacks.
Preservation of Original Signal Quality	Metrics show perfect reconstruction ($MSE = 0$, $MAE = 0$, $SNR = \infty$); tested on varied audio types and lengths.	Studies report high intelligibility of decrypted audio but often lack detailed quantitative metrics like SNR or MSE.
Statistical Analysis (Histogram / Entropy)	Histogram and entropy analyses confirm uniform distribution, preventing pattern leakage.	Focus tends to be on performance rather than full statistical concealment; some analyses use histogram and correlation metrics.
Key Management	Requires secure key distribution for OTP keys; practical in closed environments.	Uses public/private key pairs, simplifying key distribution but increases computational overhead.
Practical Limitations	Sensitive to key reuse and loss; requires secure channel for key exchange.	Widely used but less efficient for real-time, long audio streams due to computational cost.

8. Conclusion

The results showed that the applied hybrid encryption system (Affine + OTP) has achieved an outstanding equilibrium between the amount of computation needed and the level of security achieved. The original audio signal was reconstructed perfectly. No information was lost, nor was there any distortion. The successful quantitative assessments included $MSE=0$, $MAS=0$, and $SNR=\infty$. Furthermore, other quantitative tests like entropy and histogram confirmed that the encrypted data has a uniform distribution and, thus, effectively masked any statistically relevant attributes of the original signal. This increases the resistance of the data to perform cryptanalysis. Looking at the security attributes, the combination of the Affine cipher, which is lightweight and fast, with the OTP algorithm which is unbreakable in theory (when employing truly random, one-time, never reused keys), results in a strong system which removes all the potentially discernable traces of the audio. Analyzing the randomness of OTP keys confirms the system's security claims and guarantees. In practice, the system's low processing time makes the system ideal for real-time use, such as in secure voice conversations, multimedia encryption in IoT devices, and other security-sensitive internet applications. The study, however, highlights the crucial concerns of secure key creation, distribution, and management specific to OTP-based systems. Other works should focus on these issues and study system performance in different operational conditions.

References

- [1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.
- [2] Kaur, G., & Kaur, A. "Audio cryptography: A survey on security methods," *International Journal of Computer Applications*, vol. 975, pp. 8887, 2016.
- [3] Singh, A., & Singh, S. "Audio cryptography using modified chaotic systems," *International Journal of Computer Applications*, vol. 107, no. 17, 2014.
- [4] Shannon, C. E. "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [5] A. S. Khan and M. S. Khan, "A New Approach for Audio Cryptography Based Hill and Affine Cipher," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 6, pp. 202–210, 2019.

- [6] A. Wijaya and N. Mustikasari, “Analysis of Possibility of the Combination of Affine Cipher Algorithm with One-Time Pad Cipher Using the Three-Pass Protocol Method in Text Security,” *International Journal of Computer Science and Network Security*, vol. 19, no. 9, pp. 200–206, Sep. 2019.
- [7] M. A. Al-Taani, A. H. Al-Majeed, and A. Al-Azawi, “Hybrid Audio Steganography and Cryptography Method Based on High Least Significant Bit (LSB) Layers and One-Time Pad—A Novel Approach,” *Journal of Computer Networks and Communications*, vol. 2017, Article ID 3698063, 2017
- [8] Y. Zhang and L. Liu, “Audio Signal Encryption Using Chaotic Hénon Map and Lifting Wavelet Transforms,” *arXiv preprint arXiv:1708.07548*, Aug. 2017.
- [9] A. A. Al-Mousa and A. H. Al-Jubouri, “Audio encryption algorithm based on 3D chaotic maps,” *BIO Web of Conferences*, vol. 79, p. 00070, 2024.
- [10] A. D. More, P. P. Manjrekar, and A. V. Bhoyar, “Files Cryptography Based on One-Time Pad Algorithm,” *International Journal of Engineering Research & Technology*, vol. 9, no. 9, pp. 1081–1086, Sep. 2020.
- [11] N. Schlüter, P. Binfet, and M. Schulze Darup, “Cryptanalysis of Random Affine Transformations for Encrypted Control,” *IEEE Transactions on Control of Network Systems*, 2023
- [12] Shannon, C. E. “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [13] H. Borchani, G. Varando, C. Bielza, and P. Larrañaga, “A survey on multioutput regression,” *Math. Methods Appl. Sci.*, vol. 5, no. 5, pp. 216–233, 2015.
- [14] C. Willmott et al., “Statistics for the evaluation of model performance,” *J. Geophys. Res.*, vol. 90, no. C5, pp. 8995–9005, 1985
- [15] Glazunov, A.; Alayon, A.F.M.; Tufvesson, F. Mean effective gain of antennas in a wireless channel. *IET Microw. Antennas Propag.* 2009, 3, 214–227. [Google Scholar] [CrossRef]