Yuzuncu Yil University
Journal of the Institute of Natural & Applied Sciences
https://dergipark.org.tr/en/pub/yyufbed

Research Article

Using the Sound of Scrambled Images for Innovative IoT Underwater Data Transmission

Ismail Burak PARLAK*

Galatasaray University, Faculty of Engineering and Technology, Department of Computer Engineering, 34349, İstanbul, Türkiye
*Corresponding author e-mail: bparlak@gsu.edu.tr

Abstract: The development of a hybrid approach for underwater IoT communication involves the integration of chaotic map algorithms with acoustic wave technology to ensure efficient transmission of data through the water. The Arnold Cat Map algorithm is a chaotic image scrambling technique that rearranges the pixels of an image through a mathematical transformation, creating a seemingly random pattern. A particularly intriguing application is the use of complex steganography, which is traditionally employed for image scrambling, to generate sound files for underwater communication. In this novel approach, the algorithm first scrambles an image, converting it into a sophisticated sound file. This sound file, which consists of a series of acoustic waves, is transmitted through the water, where sound waves are the primary communication medium due to their superior ability to travel underwater. Upon receipt, the sound waves are transformed back into their image form using an inverse transformation. By reversing the Arnold's cat map algorithm, the scrambled image is decoded, revealing the original message. This hybrid strategy leverages the power of acoustic waves in underwater communication and the encryption capabilities of image processing algorithms, providing a secure and efficient communication method. It addresses issues such as signal attenuation and noise interference, making it a promising solution for complex underwater IoT systems that require high security and reliability. The combination of image scrambling and acoustic wave transmission creates a sophisticated communication system capable of handling complex maritime IoT applications, thus enhancing the underwater communications.

Keywords: Acoustic wave, Chaotic maps, Data encryption, Image sound steganography, Underwater communication

Karıştırılmış Görüntülerin Sesini Yenilikçi Nesnelerin İnterneti Sualtı Veri İletimi için Kullanma

Öz: Su altı IoT iletişimi için hibrit bir yaklaşımın geliştirilmesi, verilerin su altından verimli bir şekilde iletilmesini sağlamak amacıyla kaotik harita algoritmalarının akustik dalga teknolojisiyle entegrasyonunu içerir. Arnold Cat Map algoritması, bir görüntünün piksellerini matematiksel bir dönüşümle yeniden düzenleyerek, görüntüyü rastgele bir desen haline getiren kaotik bir görüntü karıştırma tekniğidir. Bu yaklaşımın özellikle ilginç bir uygulaması, geleneksel olarak görüntü karıştırma için kullanılan steganografi algoritmasının, su altı iletişimi için ses dosyaları üretmek amacıyla kullanılmasıdır. Bu yenilikçi yaklaşımda, algoritma ilk olarak bir görüntüyü karıştırarak onu karmaşık bir ses dosyasına dönüştürür. Akustik dalgalardan oluşan bu ses dosyası, su altındaki ortamda iletilir; burada ses dalgaları, su altındaki mükemmel iletim özellikleri nedeniyle birincil iletişim ortamıdır. Alındığında, ses dalgaları ters dönüşüm işlemiyle tekrar görüntü formuna dönüştürülür. Arnold'un kedi haritası algoritması tersine çevrilerek karıştırılmış görüntü çözümlenir ve orijinal mesaj ortaya çıkar. Bu hibrit strateji, su altı iletişimindeki akustik dalgaların gücünden ve görüntü işleme algoritmalarının şifreleme yeteneklerinden yararlanarak güvenli ve verimli bir iletişim yöntemi sunar. Ayrıca, sinyal zayıflaması ve gürültü interferansı gibi sorunları ele alarak, yüksek güvenlik ve güvenilirlik gerektiren karmaşık su altı IoT sistemleri için umut verici bir çözüm sunar. Görüntü karıştırma ve akustik dalga iletiminin birleşimi, karmaşık deniz IoT uygulamalarını yönetebilecek sofistike bir iletişim sistemi oluşturur ve böylece su altı iletişimini geliştirir.

Anahtar Kelimeler: Akustik dalga, Görüntü ses steganografisi, Kaotik haritalar, Sualtı iletişimi, Veri şifreleme

Received: 20.01.2025
Accepted: 02.04.2025

How to cite: Parlak, İ. B. (2025). Using the sound of scrambled images for innovative IoT underwater data transmission. *Yuzuncu Yil University Journal of the Institute of Natural and Applied Sciences*, *30*(1), 113-128. https://doi.org/10.53433/yyufbed.1623589

1. Introduction

Over the last decade, underwater data security has evolved significantly, driven by the increasing complexity and demand for underwater technology. As global dependence on underwater communication systems has grown through Internet of Things (IoT) commercial systems, the need to safeguard sensitive information in these environments has become crucial (Strelkoff, 2021). The challenges of underwater data security are unique, given the reliance on acoustic waves for communication and the inherent vulnerabilities such as signal attenuation, noise interference, and potential interception (Pradhan et al., 2016; Wang & Li, 2022).

In underwater IoT communication, acoustic waves are the primary means of data transfer (Mileva, 2018). However, the security protocols and encryption techniques are coupled with these protocols to overcome the specific challenges of the medium (Yin et al., 2015). In order to protect the data from unauthorized access and tampering, symmetric encryption algorithms such as Advanced Encryption Standard (AES) are commonly used due to their efficiency in handling the low bandwidth and high latency typical of underwater environments. Message authentication codes (MACs) and the digital signatures are employed for ensuring data integrity and authenticity (Mandal et al., 2022; Kumar et al., 2023). The error correction codes like Reed-Solomon and Turbo codes are also mitigating the effects of signal distortion and noise prevalent in underwater channels. Additionally, to address the unique constraints of underwater communication, adaptive modulation techniques are used to adjust the transmission parameters dynamically, enhancing both security and performance. These specialized approaches are crucial for safeguarding sensitive information and maintaining reliable communication across challenging underwater conditions (Ray et al., 2021). Advances in cryptographic methods, signal processing, and hybrid communication systems have played a crucial role in enhancing the protection of underwater data. This development has triggered the emergence of innovative approaches, including the use of chaotic algorithms and advanced scrambling techniques, which have redefined how data is secured beneath the surface. As underwater IoT applications expand, the field of underwater data security remains at the forefront of technological advancement, striving to meet the ever-growing demands for secure and reliable communication in challenging underwater conditions.

IoT is a rapidly growing field that connects multiple devices and systems, enabling them to communicate and interact autonomously. This interconnectivity facilitates automation and efficiency across various sectors, including healthcare, smart homes, and industrial control systems (Pradhan et al., 2016; Wang & Li, 2022). However, the proliferation of IoT devices has introduced significant security challenges. The sensitive nature of the data transmitted, and the sheer volume of devices create vulnerabilities that could be exploited by malicious usage. As a result, securing IoT systems is critical to ensure data integrity, confidentiality, and overall system reliability. An innovative approach to enhancing IoT security is the use of steganography (Hussain & Hussain, 2013; Hussain et al., 2018). The steganography offers a novel method for safeguarding data in IoT networks. Traditionally, it is associated with hiding information within digital media such as images or audio files. Unlike cryptography, which secures data by making it unreadable without the proper key, steganography hides the existence of the data itself. The primary goal is to prevent the detection of hidden information, making it a valuable tool for maintaining privacy and security. In the context of IoT, steganography can be employed to protect sensitive data communicated between devices (Goel et al., 2013; Ray et al., 2021). The data packets transmitted over a network can be embedded within benign-looking packets or encrypted payloads. This concealed data can include authentication tokens, control signals, or other critical information necessary for the operation of IoT devices.

Steganography reduces the likelihood of unauthorized access or interception by hiding the sensitive information within benign data (Bachrach & Shih, 2012). This is particularly useful in IoT environments where the data might be transmitted over insecure networks, especially in maritime and underwater environments (Hamid et al., 2012; Ghoul et al., 2023). Traditional encryption methods can sometimes attract attention due to the noticeable nature of encrypted traffic. The steganography obscures the presence of data altogether, making it less conspicuous to potential attackers. Moreover, combining steganography with other security measures, such as encryption and authentication, creates a multi-layered defense system (Mustafa et al., 2018; Kaur et al., 2022). This approach enhances the overall

security posture of IoT devices and networks. Steganographic techniques can be adapted to various types of IoT data and communication protocols. This flexibility allows for the integration of steganography into existing security frameworks without significant modifications (Qin et al., 2019; Koptyra & Ogiela, 2023).

The aim of this study is to develop a novel hybrid approach for underwater IoT communication that integrates chaotic map algorithms with acoustic wave technology to enhance the security, efficiency, and reliability of data transmission in marine environments. The proposed method leverages the Arnold Cat Map algorithm, a chaotic image scrambling technique, to encrypt data by converting it into a scrambled image. This image is then transformed into a sound file, which is transmitted underwater using acoustic waves. Upon reception, the sound file is decoded back into the original image through the inverse transformation of the Arnold Cat Map algorithm. By combining the encryption capabilities of image processing with the robustness of acoustic waves for underwater communication, this method addresses challenges such as signal attenuation, noise interference, and the need for secure data transfer in complex underwater IoT systems. The study aims to demonstrate that this hybrid approach can provide a more secure and efficient solution for underwater communication, making it suitable for a wide range of marine applications.

The study is organized as follows. Section 2 reviews related works in steganography techniques and its recent applications on IoT and underwater environments. Section 3 details the proposed methodology Section 4 shows encoding results and highlights the scope of the study through obtained results. Finally, Section 5 concludes the study with the effects of findings and the future steps.

2. Literature Review

While the steganography offers significant advantages, its implementation in IoT security comes with several challenges. Incorporating steganography into IoT systems requires careful planning and execution. Ensuring that hidden data does not interfere with the normal operation of devices and communications can be complex. The process of embedding and extracting hidden data can introduce additional computational overhead. This is a crucial consideration for the resource-constrained IoT devices where the processing power and the bandwidth are limited. Although the steganography aims to hide data, sophisticated techniques and tools can potentially detect the steganographic methods. It is essential to continuously update and refine steganographic techniques to stay ahead of detection methods. Securing IoT systems is essential as the number and complexity of connected devices continue to expand. The steganography offers a promising approach to enhancing IoT security by concealing sensitive information within seemingly harmless data. Its potential benefits include improved data privacy, reduced attack susceptibility, and flexibility in integration (Ray et al., 2021). However, the challenges such as integration complexity, performance impact, and detection risks must be carefully managed. The integration of steganography with other security measures, such as encryption and robust authentication protocols, can contribute to a more comprehensive and resilient IoT security strategy.

Figure 1 illustrates a general scheme of modern maritime and underwater communication channels. The maritime industry is increasingly leveraging IoT technologies to enhance operational efficiency, safety, and navigation. The integration of IoT into underwater operations also introduces significant security challenges, including potential cyber threats and data breaches. Securing IoT systems in maritime services is therefore essential to ensure the safety and efficiency of maritime operations. In order to reduce security risks and protect IoT systems in underwater services, several strategies can be employed (Fabbri et al., 2018). The implementation of Multi-Factor Authentication for accessing IoT devices and systems ensures that only authorized personnel can access critical data and control functions. Also, assigning access permissions based on user roles helps limit access to sensitive information and system functions. In advanced approaches, the encryption of data transmitted between IoT devices and centralized systems protects it from interception and unauthorized access. Network security is considered a severe problem in maritime IoT systems. Deploying firewalls to protect IoT networks from unauthorized access, cyber threats, the intrusion detection systems become a regular activity for potential security breaches to monitor the network traffic for suspicious activities. As the underwater industry continues to embrace IoT, ongoing vigilance and adaptation to emerging threats will be crucial. By adopting a proactive and layered security approach, the organizations can ensure the

resilience and security of their IoT systems, ultimately contributing to safer and more efficient maritime operations.

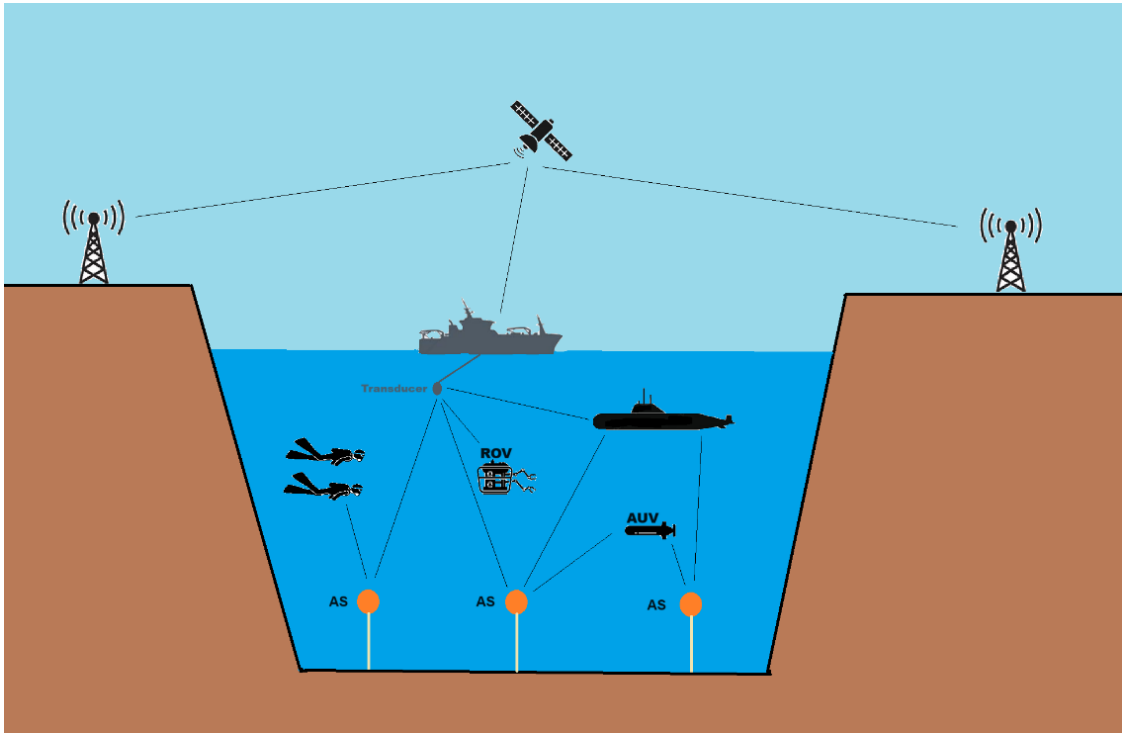

Figure 1. Illustration of marine and underwater communication through antennas, satellites and acoustic sensors (AS). ROV: Remote Operating Vehicle, AUV: Autonomous Underwater Vehicle.

Signal steganography has become a crucial technique in securing communications in IoT applications (Sharda & Budhiraja, 2013; Setiadi et al., 2023). In maritime and underwater systems, where secure and covert communication is critical due to operational and environmental constraints, steganography offers an important technique. Underwater communication systems face unique challenges due to the complexity of the environment, including high noise levels, limited bandwidth, and the need for robust data protection. The signal steganography helps address these challenges by embedding hidden information within communication signals. The acoustic steganography is particularly relevant in underwater systems where traditional radio frequency (RF) communication is impractical due to the attenuation of RF signals in water. The acoustic communication is commonly used for underwater data transmission, and steganography can be applied to these acoustic signals. Underwater environments can cause distortion and attenuation of acoustic signals, which may affect the integrity of the embedded data. The limited bandwidth available for acoustic communication can restrict the amount of data that can be hidden. RF Steganography is used in maritime environments where RF communication is feasible, such as in satellite communications and surface vessel communications. In these systems, steganography can be applied to various types of RF signals modifying the modulation scheme, such as phase-shift keying or amplitude modulation, to embed secret data (Khan et al., 2021; Subramanian et al., 2021). Slight adjustments in the modulation parameters can encode additional information. Data can be hidden within the shape of transmitted RF pulses. By altering the pulse characteristics subtly, hidden messages can be embedded without significant impact on the signal's primary function. RF communication generally supports higher data rates compared to acoustic systems, enabling the embedding of larger amounts of data. RF signals can be transmitted over longer distances compared to acoustic signals, providing greater flexibility for maritime applications.

Even if the steganography and the cryptography are both crucial techniques in data security, they serve different purposes and offer distinct advantages. While cryptography secures data by making it unreadable without the correct key, the steganography embeds the data within other data. This means that an observer cannot even detect that there is a hidden message, making it less likely to attract attention from potential attackers. Steganography can be used to transmit information within regular,

everyday data such as images, audio files, or text. Since the carrier data appears normal, it avoids drawing suspicion. In contrast, cryptographic methods often result in noticeable patterns that can signal to an observer that a message is being transmitted. The steganography offers a range of methods for embedding data, such as within images, audio files, or even network packets. This versatility allows for the integration of hidden messages into various types of digital content, making it adaptable to different communication scenarios and environments (Fabbri et al., 2018; Djebbar, 2021). While steganography offers several advantages, it also has notable disadvantages when compared to cryptography. Steganography often has limitations on the amount of data that can be effectively embedded within a source message. Furthermore, steganography can be susceptible to steganalysis, which involves techniques used to detect the presence of hidden data (Mishra & Bhanodiya, 2015). Sophisticated tools and methods can sometimes reveal hidden information by analyzing patterns or anomalies in the carrier data, potentially compromising the effectiveness of steganography. Embedding data within a carrier can lead to perceptible changes or degradation in the quality of the source message file, such as an image or audio file. Even small alterations can be detected through careful inspection, which can reveal the presence of hidden information. Cryptography does not inherently affect the quality of the data being encrypted (Mishra & Bhanodiya, 2015; Das & Das, 2016).

Designing and implementing effective steganographic methods can be complex and require careful consideration to avoid detection and maintain data integrity (Subhedar & Mankar, 2014; Tao et al., 2018). The process of embedding and extracting data must be precisely managed to prevent introducing detectable artifacts. In summary, while steganography provides unique benefits in hiding the existence of data, it has limitations compared to cryptography, such as smaller data capacity, vulnerability to detection, and lack of data integrity protection (Wani & Sultan, 2023; Yu et al., 2024). Cryptography offers robust data security with well-defined standards for encryption, key management, and data integrity, making it a complementary approach to steganography for comprehensive data protection (Das & Das, 2016; Khari et al., 2020).

Altaay et al. (2012) provided a comprehensive overview of various image steganography techniques. They reviewed the fundamental concepts and methods used to conceal information within digital images, detailing techniques such as Least Significant Bit (LSB) substitution, pixel value differencing, and frequency domain methods. They emphasized the importance of these techniques in ensuring secure communication by embedding secret data into image files in a way that is imperceptible to the human eye. They discussed the trade-offs between embedding capacity, image quality, and security, offering insights into the practical applications and challenges associated with image-based steganography. Alhaddad et al. (2020) explored the enhancement of secret data detection accuracy in audio steganography, particularly within the context of securing 5G-enabled IoT networks. The study focused on evolutionary algorithms to improve the reliability and precision of hidden data detection embedded within audio files. They discussed various techniques for optimizing the detection process, evaluating their effectiveness in maintaining data security and integrity amidst the high-speed, high-volume data exchange characteristic of 5G networks. Their findings highlight advancements in audio steganography methodologies that can be employed to safeguard confidential information in the evolving landscape of IoT security.

Amjath and Senthooran (2020) focused on steganographic techniques to be employed to obscure sensitive data within IoT communications, thereby improving data confidentiality and integrity. They evaluated various methods of embedding secret information in different types of digital media, such as images and audio, to prevent unauthorized access and eavesdropping. The study highlighted the importance of integrating steganography with IoT systems to address security challenges and ensure secure data transmission in a networked environment with numerous interconnected devices. Bachrach and Shih (2012) provided a comprehensive survey of image steganography and steganalysis within the context of multimedia security. They reviewed various techniques used for embedding secret information within digital images (steganography) and methods for detecting and analyzing such hidden data (steganalysis). The study covered a range of steganographic approaches, including spatial domain methods like Least Significant Bit (LSB) insertion and transform domain techniques such as Discrete Cosine Transform (DCT). They discussed the challenges and advancements in steganalysis, which aims to identify and extract hidden information, thus highlighting the ongoing efforts to enhance both the robustness of steganographic techniques and the effectiveness of detection methods.

Bairagi et al. (2016) presented an efficient steganographic method designed to enhance communication security within critical infrastructures of IoT. They introduced a novel approach for embedding secret information into digital media, specifically targeting the challenges posed by the high-stakes nature of IoT environments. Their approach highlighted the steganographic technique's ability to securely conceal data while maintaining the integrity and performance of IoT systems. Their study emphasized the importance of this method in safeguarding sensitive communications against unauthorized access and attacks, thus contributing to the overall security and resilience of IoT networks. (Das & Das, 2016) explored the integration of cryptography and steganography techniques to enhance secure data transfer in IoT environments. They proposed a hybrid approach that combines cryptographic methods for encrypting data with steganographic techniques for hiding the encrypted information within digital media. This dual-layered security strategy aimed to address the vulnerabilities of IoT systems by ensuring that data is both encrypted and concealed, thereby improving confidentiality and reducing the risk of unauthorized access or interception. They discussed the effectiveness of this combined approach in securing data transmission across IoT networks.

Djebbar (2021) presented a practical framework for enhancing the security of IoT data through the application of steganography. They discussed how steganographic techniques can be employed to conceal sensitive information within IoT communications, thereby providing an additional layer of security against potential cyber threats. They detailed a practical implementation approach, including methods for embedding data within various types of media and data streams used in IoT systems. The study highlighted the advantages of using steganography to obscure the presence of sensitive information, complementing traditional security measures like encryption. Khari et al. (2020) explored advanced methods for enhancing data security within IoT environments. They presented a comprehensive approach that integrates both cryptographic and steganographic techniques to protect sensitive data transmitted across IoT networks. The study emphasized the importance of using elliptic curve cryptography for robust public key authentication and confidentiality, alongside steganography to obscure data within otherwise benign communication channels.

Hassaballah et al. (2021) introduced a novel image steganography method on embedding sensitive data within digital images to enhance the security of IoT communications. By leveraging advanced steganographic techniques, the approach aimed to provide an additional layer of security against unauthorized access and data breaches in industrial environments. Their study demonstrated how the method effectively conceals information within image files while maintaining data integrity and operational efficiency. Jia-jia et al. (2018) explored bio-inspired steganography techniques designed to enhance the security of underwater acoustic communications. They proposed innovative steganographic methods inspired by biological systems to embed secret information within acoustic signals used in underwater communication. These bio-inspired techniques aimed to improve the robustness and stealth of data concealment, making it more difficult for potential eavesdroppers to detect hidden messages. Their study highlighted the advantages of using nature-inspired approaches to achieve secure and efficient underwater communication, addressing the unique challenges of the aquatic environment, such as signal degradation and noise. Pradhan et al. (2016) provided an in-depth evaluation of performance parameters for various image steganography techniques. They analyzed different steganographic methods by assessing key performance indicators such as embedding capacity, image quality, and robustness against detection and attacks. They emphasized the importance of these parameters in determining the effectiveness of steganographic techniques for securely hiding data within images while maintaining visual fidelity.

3. Material and Methods

The study starts with the acquisition of visual data. The underwater data steganographic encoding and decoding consists of two layers of image and audio signal processing as introduced in Figure 2 where the flowchart illustrates the proposed mechanism. The chaotic map is generated through Arnold’s cat algorithm. Thus, the image steganography step is achieved to generate relevant sound data. However, the media is not suitable for underwater communication since it is not an acoustic wave. Inverse MEL transformation is applied to generate sound file from encoded image file. The encoded data is sent to the receiver. When the receiver gets the message, the sound is transformed to shuffled

image. Finally, the original image is reconstructed with the inverse Arnold's cat algorithm. The flowchart of the study is given in Figure 2.

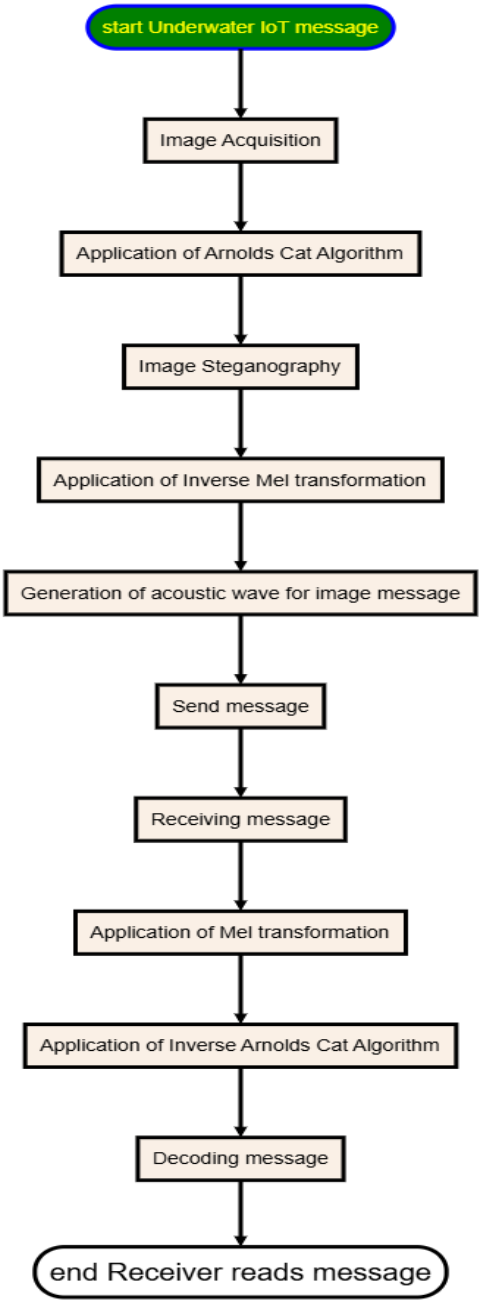

Figure 2. Flowchart of the proposed approach.

In this study, two different image datasets were chosen to perform image to acoustic wave transformation using steganography. The EUVP (Enhancing Underwater Visual Perception) dataset is a specialized collection of underwater imagery designed to advance research and development in underwater visual perception and computer vision (Islam et al., 2020). The dataset includes high-resolution underwater images captured in various environments and conditions, such as natural marine settings and artificial underwater structures. Images are annotated with labels for various objects and features, including marine life, coral reefs, and underwater equipment. The dataset covers a wide range of underwater conditions, including different lighting scenarios and depths. This variety helps in developing robust algorithms that can handle diverse real-world scenarios. It encompasses various types of underwater scenes, from shallow coastal waters to the deep-sea environments, providing a broad

spectrum of visual contexts. The dataset is used for developing and evaluating algorithms related to object detection, segmentation, and tracking in underwater environments. It focused on improving image quality and visibility in challenging underwater conditions, such as addressing issues with color distortion and low contrast. The underwater_imagenet dataset, introduced by Fabbri et al. (2018) is a specialized dataset designed to address challenges in underwater imagery enhancement. The dataset comprises a large collection of underwater images, which are derived from the ImageNet dataset but adapted to underwater conditions. This includes a variety of underwater scenes featuring marine life, objects, and environments. The dataset is specifically created to train and evaluate Generative Adversarial Networks (GANs) for improving underwater image quality. It focuses on enhancing features such as color correction, contrast, and overall clarity, which are often degraded due to the underwater environment. The images in the dataset are processed to simulate realistic underwater distortions, such as color fading and blur, which allows GAN models to learn how to generate high-quality images from degraded inputs. In a nutshell, the underwater_imagenet dataset provides a crucial resource for advancing underwater image processing through GANs, addressing specific challenges related to image quality and visual clarity in aquatic settings. 100 color JPEG images from each dataset were chosen as input messages in this study. 200 images have a spatial resolution of 256 x 256 pixels. The experiments were evaluated through mean images.

Arnold's cat map is a chaotic transformation used to scramble images, enhancing data security through mathematical manipulation. The process begins by representing an image as a matrix I with pixel values, where each pixel's position is denoted by coordinates (x, y) in the matrix. The Arnold's cat map applies the transformation defined by the matrix multiplication as follows;

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{1}$$

(x', y') are the new coordinates of the pixel after transformation, and N is the size of the image matrix. This matrix multiplication results in a chaotic reorganization of the pixel positions. By repeatedly applying the transformation, the image undergoes multiple iterations, with each application scrambling the pixel positions further. The image then appears as random noise due to the chaotic nature of the transformation. In order to recover the original image, the inverse of Arnold's cat map is applied, given by;

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{2}$$

This reverse procedure reconstructs the original image from the scrambled image, revealing the original content. Arnold's cat map's chaotic transformation effectively transforms the original image into a chaotic map, making it secure against unauthorized access.

In audio processing, a Mel spectrogram is a powerful tool for analyzing and visualizing the frequency content of an audio signal, particularly for tasks like speech recognition and audio classification. It provides a time-frequency representation of the signal, but with a frequency scale that is more aligned with human auditory perception. The first step in generating a Mel spectrogram is to compute the Short-Time Fourier Transform (STFT) of the audio signal. This involves dividing the signal into overlapping frames and applying a Fourier Transform to each frame. For an audio signal x(t), the STFT is given by;

$$X(t,f) = \int_{-\infty}^{\infty} x(\tau)\omega(\tau - t)e^{-j2\pi f\tau}d\tau \tag{3}$$

where $\omega(\tau - t)$ is a window function centered at time t, and f is the frequency variable. The magnitude spectrogram is obtained by taking the magnitude of the STFT result:

$$|X(t,f)| = \sqrt{Re[X(t,f)]^2 + Im[X(t,f]^2} \tag{4}$$

This gives us a time-frequency representation where each point indicates the amplitude of a particular frequency at a given time. The Mel scale is a perceptual scale of pitches that approximates human hearing. The Mel filter bank is used to map the frequency axis of the magnitude spectrogram to the Mel scale. The Mel scale is defined as follows;

$$Mel(f) = 2595log_{10}(1 + \frac{f}{700}) \quad (5)$$

where f is the frequency in Hertz.

In order to convert the frequency axis to the Mel scale, the magnitude spectrogram is multiplied by a set of triangular filters that cover the Mel frequency bands. The Mel-filtered spectrogram can be computed as:

$$S_m(t,m) = \sum_f |X(t,f)| \,.\, H_m(f) \quad (6)$$

where Hm(f) represents the Mel filter bank, which is a set of triangular filters spaced according to the Mel scale. The Mel spectrogram is converted to a logarithmic scale to better represent the perceptual differences in loudness. This is done by applying a logarithmic function;

$$LogMel(t,m) = \log\,(1 + S_m(t,m)) \quad (7)$$

This step compresses the dynamic range of the spectrogram, making it more suitable for machine learning applications. A Mel spectrogram thus combines the STFT for time-frequency analysis with the Mel scale for frequency scaling and optional logarithmic compression. The result is a time-frequency representation that better matches human auditory perception, making it an effective feature for various speech processing tasks.

Finally, Chroma feature extraction was integrated to our method to compare acoustic performance between pitch classes in acoustic wave transmission. Chroma computation using is a powerful tool in the analysis of speech processing, offering valuable insights into the harmonic structure of audio signals. This technique enables the extraction of tonal characteristics from speech by analyzing the chroma features. Briefly, it captures the intensity distribution across the twelve pitch classes of the chromatic scale. This is particularly useful in tasks such as pitch tracking, speaker identification, and emotion recognition, where understanding the underlying musicality or tonal variations in speech can enhance the accuracy of these processes.

During the design and the implementation, Python 3.11 programming language was used with OpenCV, Librosa, NumPy and Matplotlib libraries.

4. Results

Arnold's cat map takes a structured initial image and, after several iterations, transforms it into a highly scrambled form. An underwater image with a clear pattern becomes increasingly distorted with each application of the map. This behavior demonstrates the concept of chaos, where even simple deterministic rules can lead to highly unpredictable results. The transformation effectively randomizes the image, which is a key characteristic of chaotic systems.

Figure 3 presents the preprocessed images where 200 images were normalized in RGB channels and grayscale images were created. Even if RGB steganography are in use for IoT systems, grayscale images were preferred due to image to sound conversion to decrease data loss and bandwidth capacity in underwater environments. Figure 4 shows the histogram distribution for grayscale images. Histograms become important to ensure high quality data transmission and measure data loss during image-audio encoding. Three different experiments were evaluated to compare the efficiency of the proposed setup. Figure 5 illustrates the application of 10 times, 50 times and 500 times Arnold cat mapping on mean images. The map's periodicity is crucial for applications like image encryption. It means that the scrambling is not permanent; the original image can be recovered by applying the inverse

transformation. This feature is valuable in scenarios given in Figure 5 where reversible scrambling is required. The chaotic map essentially performs a shearing and stretching transformation on the image. Over iterations, this transformation can cause the image to stretch and fold in complex ways, leading to its eventual scrambling. The nature of the transformation reveals how spatial structures can evolve under linear mappings, giving insight into how complex patterns and textures can emerge from simple rules. When Arnold's cat map is applied to the image, the histogram distribution undergoes significant changes. After several iterations, the histogram of the scrambled image often becomes approximately uniform. This uniformity indicates that the pixel values are spread more evenly across the entire range of possible intensities. The map effectively redistributes pixel values, leading to a more uniform histogram. This characteristic is consistent with the behavior of chaotic systems, where initial structures become mixed and spread out over time.

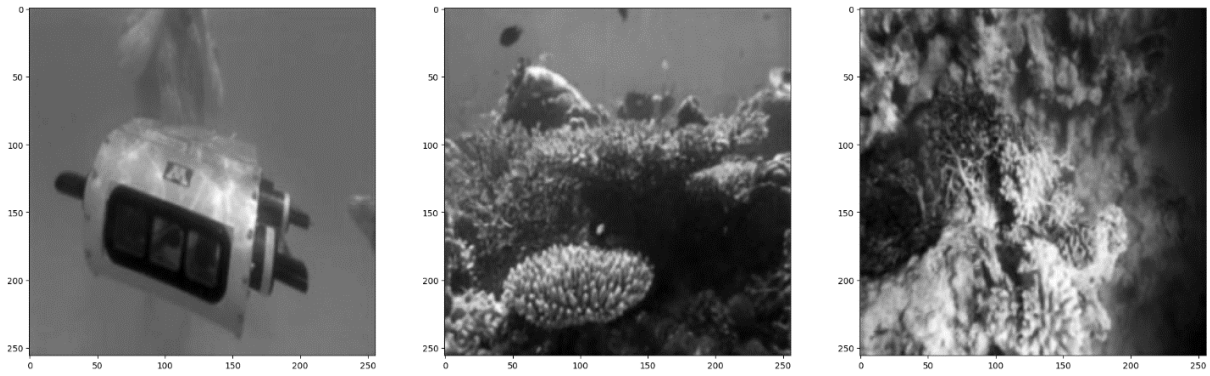

Figure 3. Preprocessed images.

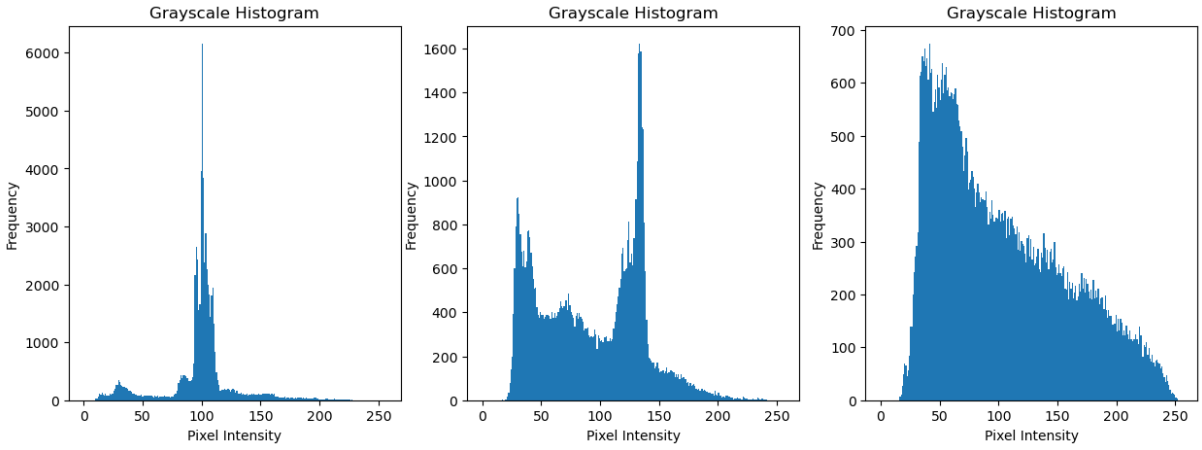

Figure 4. Histograms of preprocessed images.

The inverse Mel transformation provides an approximation of the original STFT magnitude spectrum from Mel features. While it can effectively reconstruct many aspects of the signal, there may be some loss of detail due to the compression and scaling performed by the Mel filter bank. The reconstruction quality depends on the accuracy of the inverse transformation and how well the Mel features capture the original frequency content. Some high-frequency details may be lost or approximated, especially if the Mel filters are coarse. The Mel transformation is inherently lossy because it maps the frequency spectrum to a lower-dimensional Mel scale. This process reduces the resolution of frequency information, which can impact the accuracy of the inverse Mel transformation. As a result, the reconstructed spectrum from Mel features may not perfectly match the original STFT magnitude spectrum, and some fine-grained frequency details may be lost. The inverse Mel transformation is useful in applications where approximate reconstruction of the audio signal is acceptable. This includes tasks such as speech synthesis, where the Mel features are used to generate new audio signals, and audio

enhancement, where the goal is to improve the quality of audio based on Mel features. Figure 6 presents the comparison of three scenarios and the loss of reconstructed mean images with STFT as residual errors in dB.

In underwater communication, the inverse Mel transformation can be used to create synthetic or enhanced audio signals that approximate the characteristics of the original signal. However, it is important to consider the trade-offs between reconstruction quality and the level of detail retained. The inverse Mel transformation involves mapping Mel-scaled features back to the original frequency domain using a procedure that approximates the inverse of the Mel filter bank. This often requires careful handling of the Mel scale and its associated parameters. The mathematical relationship between the Mel and frequency domains is complex, and the inverse transformation must account for the non-linear mapping between these domains to achieve accurate reconstruction.

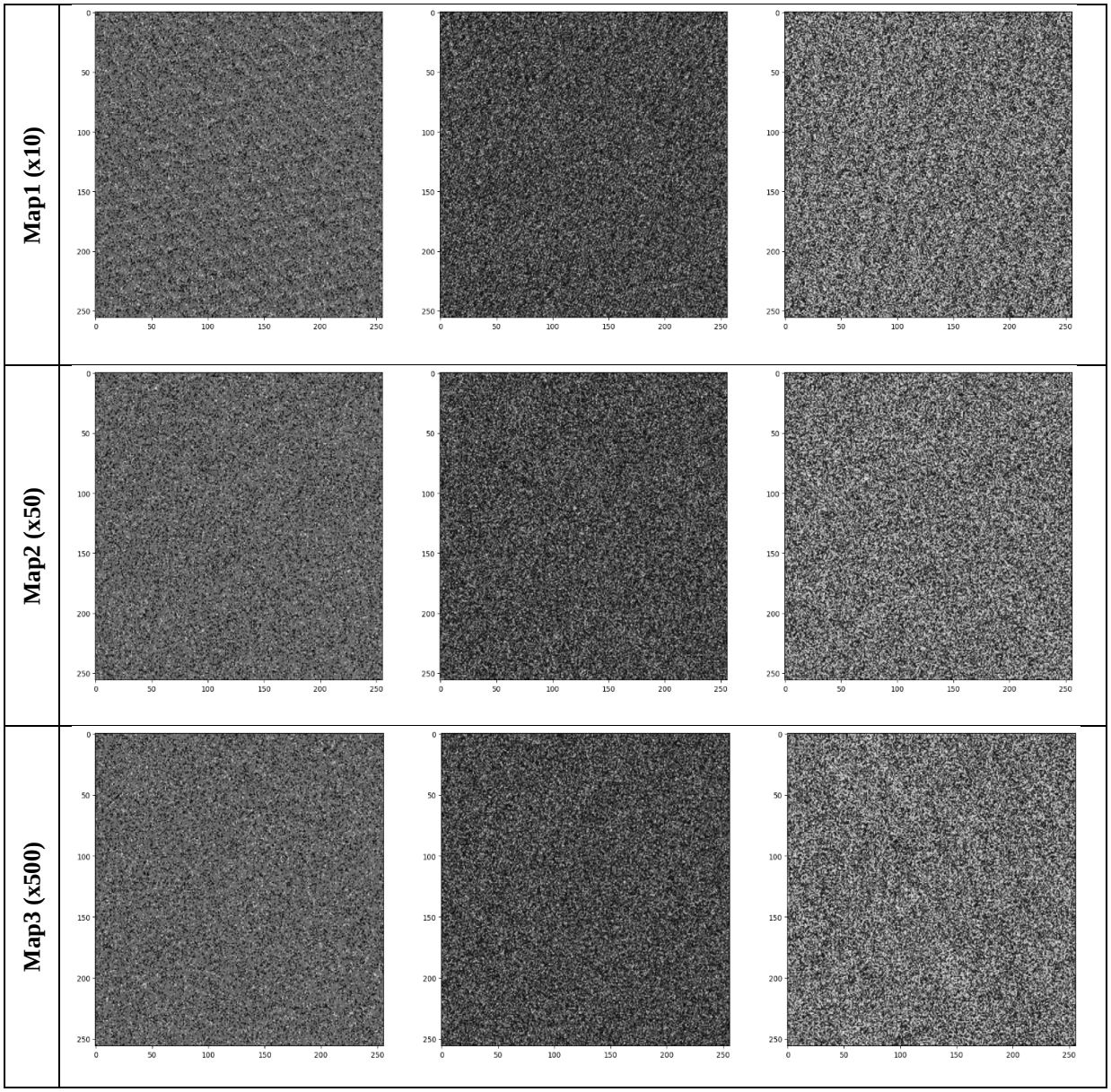

Figure 5. Application of three different Arnold cat maps on preprocessed images.

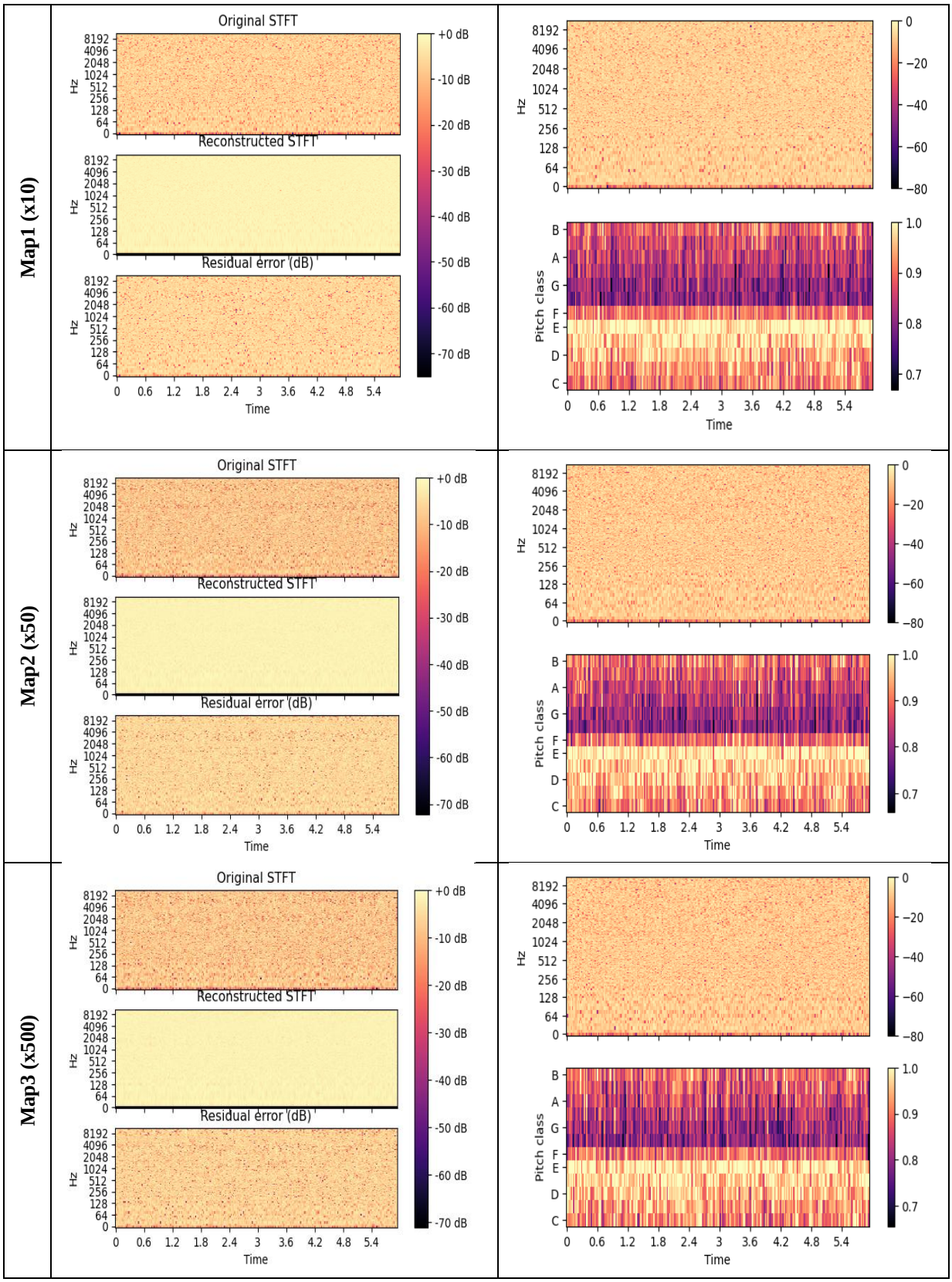

Figure 6. Comparison of three Arnold cat map techniques on reconstructed acoustic signals and chroma features through mean images.

5. Discussion and Conclusion

After a few iterations, the histogram of the scrambled image tends to approach a uniform distribution. This means that pixel values are distributed more evenly, as opposed to clustering around certain values. Uniform histograms are a sign that the map has successfully scrambled the image by removing any initial patterns or structures and achieving a high degree of randomness. This property is desirable in cryptographic applications where predictability needs to be minimized. The rate at which the histogram converges to uniformity depends on the number of iterations. Typically, after a sufficient number of iterations the histogram distribution of the scrambled image will closely approximate a uniform distribution. This convergence indicates that the map's effect on the pixel values is thorough, spreading out pixel intensities and reducing correlation between neighboring pixels. Given that Arnold's cat map is periodic, the histogram of the image will eventually return to its original distribution after a certain number of iterations. This periodicity implies that while the histogram becomes uniform during the scrambling process; it will revert to the initial histogram after completing one full cycle of iterations. This property is useful for applications where the ability to return to the original image is required.

The STFT provides a time-frequency representation of a signal by dividing it into overlapping segments, applying the Fourier transform to each segment, and then analyzing the resulting frequency components over time. The Mel transformation maps the frequency axis to the Mel scale, which is designed to approximate the frequency resolution of human hearing. This transformation is typically performed using a Mel filter bank applied to the magnitude spectrum obtained from the STFT. The inverse Mel transformation aims to approximate the original frequency-domain representation from Mel-scaled features. It involves mapping the Mel features back to the original frequency domain.

The Mel scale reduces frequency resolution, especially at higher frequencies. The Mel filter bank groups frequencies into broader bands, which means fine-grained frequency information is lost. When performing the inverse Mel transformation, the loss of detailed frequency information can result in discrepancies between the reconstructed spectrum and the original STFT magnitude spectrum. The Mel filter bank approximates the human auditory system’s frequency resolution and maps the continuous frequency spectrum to discrete Mel bands. This approximation introduces quantization errors. The inverse transformation must approximate the original frequency content based on these quantized Mel features, leading to errors in the reconstructed spectrum. The Mel scale involves a non-linear mapping of frequencies, which complicates the inverse transformation process. The inverse operation approximates the mapping rather than perfectly reversing it. The complexity of reversing a non-linear transformation can result in residual errors, as the process may not perfectly reconstruct the original frequency content. The design of the Mel filter bank, including the number and width of filters, affects the fidelity of the transformation. A limited number of filters or suboptimal filter design can introduce errors. The resolution and characteristics of the Mel filter bank influence the accuracy of the inverse transformation. If the filter bank does not capture the signal’s frequency content adequately, the reconstructed spectrum will be inaccurate. During the inverse Mel transformation, certain artifacts may appear due to the approximation process and the inherent limitations of the Mel scale.

Image steganography presents both significant opportunities and notable challenges in the context of IoT systems for underwater applications. This technique, which involves embedding secret data within digital images, offers a novel approach to securing communications in an environment where traditional methods face severe constraints. The primary advantage of using image steganography in underwater IoT is its ability to provide an additional layer of security by concealing sensitive information within seemingly safe images. This can greatly reduce the risk of interception and unauthorized access, which is particularly important in underwater environments where communication channels are vulnerable to eavesdropping and interference.

However, image steganography in underwater applications is not without its limitations. The constrained bandwidth and signal quality in underwater environments can restrict the amount of data that can be effectively hidden within images. Additionally, implementing robust steganographic techniques requires careful design to avoid detection by sophisticated steganalysis methods, which can undermine the security benefits. The complexity of integrating steganographic methods into existing underwater IoT systems also presents a challenge, as it demands a balance between security and system performance. As promising application areas in underwater IoT systems, image steganography can be used to secure the transmission of data collected by underwater sensors, ensuring that sensitive research

information in marine biology and environmental monitoring. Moreover it can enhance communication between underwater vehicles and surface stations, safeguarding mission-critical data in defense and security. For underwater exploration and navigation, steganography can facilitate secure data transfer between exploration robots and surface control stations. Furthermore, during emergency response and disaster management, steganographic techniques can ensure secure communication among rescue teams and underwater sensors, improving coordination and security.

References

Alhaddad, M. J., Alkinani, M. H., Atoum, M. S., & Alarood, A. A. (2020). Evolutionary detection accuracy of secret data in audio steganography for securing 5G-enabled internet of things. *Symmetry*, *12*(12), 2071. https://doi.org/10.3390/sym12122071

Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012, November). *An introduction to image steganography techniques*. 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 122-126. IEEE. https://doi.org/10.1109/ACSAT.2012.25

Amjath, M. I. M., & Senthooran, V. (2020, December). *Secure communication using steganography in IoT environment*. 2020 2nd International Conference on Advancements in Computing (ICAC), 114-119. IEEE. https://doi.org/10.1109/ICAC51239.2020.9357260

Bachrach, M., & Shih, F. Y. (2012). Survey of image steganography and steganalysis.In *Multimedia Security: Watermarking, Steganography, and Forensics* (pp. 201-214). CRC Press.

Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. *Information Security Journal: A Global Perspective*, *25*(4-6), 197-212. https://doi.org/10.1080/19393555.2016.1206640

Das, R., & Das, I. (2016, September). *Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques*. 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), 296-301. IEEE. https://doi.org/10.1109/ICRCICN.2016.7813674

Djebbar, F. (2021). Securing IoT data using steganography: A practical implementation approach. *Electronics*, *10*(21), 2707. https://doi.org/10.3390/electronics10212707

Fabbri, C., Islam, M. J., & Sattar, J. (2018, May). *Enhancing underwater imagery using generative adversarial networks*. 2018 IEEE International Conference on Robotics and Automation (ICRA), 7159-7165. IEEE. https://doi.org/10.1109/ICRA.2018.8460552

Ghoul, S., Sulaiman, R., & Shukur, Z. (2023). A review on security techniques in image steganography. *International Journal of Advanced Computer Science and Applications*, *14*(6). https://dx.doi.org/10.14569/IJACSA.2023.0140640

Goel, S., Rana, A., & Kaur, M. (2013). A review of comparison techniques of image steganography. *Global Journal of Computer Science and Technology*, *13*(4), 9-14.

Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, 6(3), 168-187.

Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A novel image steganography method for industrial internet of things security. *IEEE Transactions on Industrial Informatics*, *17*(11), 7743-7751. https://doi.org/10.1109/TII.2021.3053595

Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. *International Journal of Advanced Science and Technology*, *54*, 113-124.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66. https://doi.org/10.1016/j.image.2018.03.012

Islam, M. J., Xia, Y., & Sattar, J. (2020). Fast underwater image enhancement for improved visual perception. *IEEE Robotics and Automation Letters*, *5*(2), 3227-3234. https://doi.org/10.1109/LRA.2020.2974710

Jia-jia, J., Xian-quan, W., Fa-jie, D., Xiao, F., Han, Y., & Bo, H. (2018). Bio-inspired steganography for secure underwater acoustic communications. *IEEE Communications Magazine*, *56*(10), 156-162. https://doi.org/10.1109/MCOM.2018.1601228

Kaur, S., Singh, S., Kaur, M., & Lee, H. N. (2022). A systematic review of computational image steganography approaches. *Archives of Computational Methods in Engineering*, *29*(7), 4775-4797. https://doi.org/10.1007/s11831-022-09749-0

Khan, H. A., Abdulla, R., Selvaperumal, S. K., & Bathich, A. (2021). IoT based on secure personal healthcare using RFID technology and steganography. *International Journal of Electrical and Computer Engineering*, *11*(4), 3300. http://doi.org/10.11591/ijece.v11i4.pp3300-3309

Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2020). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 73-80. https://doi.org/10.1109/TSMC.2019.2903785

Koptyra, K., & Ogiela, M. R. (2023). Steganography in IoT: Information hiding with joystick and touch sensors. *Sensors*, *23*(6), 3288. https://doi.org/10.3390/s23063288

Kumar, A., Rani, R., & Singh, S. (2023). A survey of recent advances in image steganography. *Security and Privacy*, *6*(3), e281. https://doi.org/10.1002/spy2.281

Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. *Information Sciences*, *609*, 1451-1488. https://doi.org/10.1016/j.ins.2022.07.120

Mileva, A. (2018, August). *Steganography in the world of IoT*. IoT-SECFOR 2018, International Conference on Availability, Reliability and Security (ARES), Hamburg, Germany.

Mishra, R., & Bhanodiya, P. (2015, March). *A review on steganography and cryptography*. 2015 International Conference on Advances in Computer Engineering and Applications, 119-122. IEEE. https://doi.org/10.1109/ICACEA.2015.7164679

Mustafa, G., Ashraf, R., Mirza, M. A., Jamil, A., & Muhammad. (2018, June). *A review of data security and cryptographic techniques in IoT based devices*. Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, 1-9. https://doi.org/10.1145/3231053.3231100

Pradhan, A., Sahu, A. K., Swain, G., & Sekhar, K. R. (2016, May). *Performance evaluation parameters of image steganography techniques*. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), 1-8. IEEE. https://doi.org/10.1109/RAINS.2016.7764399

Qin, J., Luo, Y., Xiang, X., Tan, Y., & Huang, H. (2019). Coverless image steganography: a survey. *IEEE Access*, 7, 171372-171394. https://doi.org/10.1109/ACCESS.2019.2955452

Ray, A. M., Sarkar, A., Obaid, A. J., & Pandiaraj, S. (2021*)*. IoT security using steganography. In *Multidisciplinary approach to modern digital steganography* (pp. 191-210). IGI Global. https://doi.org/10.4018/978-1-7998-7160-6.ch009

Setiadi, D. R., Rustad, S., Andono, P. N., & Shidik, G. F. (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Processing*, *206*, 108908. https://doi.org/10.1016/j.sigpro.2022.108908

Sharda, S., & Budhiraja, S. (2013). Image steganography: A review. *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, *3*(1), 707-710.

Strelkoff, S. (2021). *Underwater communications with acoustic steganography: Recovery analysis and modeling*. (Doctoral dissertation), Monterey, CA; Naval Postgraduate School.

Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. *Computer Science Review*, *13-14*, 95-113. https://doi.org/10.1016/j.cosrev.2014.09.001

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. *IEEE Access*, *9*, 23409-23423. https://doi.org/10.1109/ACCESS.2021.3053998

Tao, J., Li, S., Zhang, X., & Wang, Z. (2018). Towards robust image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, *29*(2), 594-600. https://doi.org/10.1109/TCSVT.2018.2881118

Wang, W., & Li, Q. (2022). An image steganography algorithm based on PSO and IWT for underwater acoustic communication. *IEEE Access*, *10*, 107376-107385. https://doi.org/10.1109/ACCESS.2022.3212691

Wani, M. A., & Sultan, B. (2023). Deep learning based image steganography: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *13*(3), e1481. https://doi.org/10.1002/widm.1481

Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015, December). *Internet of Things: Securing data using image steganography*. 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS), 310-314. IEEE. https://doi.org/10.1109/AIMS.2015.56

Yu, J., Zhang, X., Xu, Y., & Zhang, J. (2024). *Cross: Diffusion model makes controllable, robust and secure image steganography*. Advances in Neural Information Processing Systems (NeurIPS) 36.