WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Image Processing and Optimized Audio Steganography for Secure Data Communication in IOT Systems

Nandhini S[1], Anguraj S[2], Suganya S[3], Dharani G[4]

[1]Second year of M. Tech, Department of Information Technology, KSR College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India Email: nandhinisaravanan8713@gmail.com

[2]Assistant Professor & Head, Department of Information Technology, KSR College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India Email: anguraj@ksrce.ac.in

[3]Assistant Professor, Department of Information Technology, KSR College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India Email: ksrce.suganya@gmail.com

[4]Assistant Professor, Department of Information Technology, KSR College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India Email: dharanig@ksrce.ac.in

ABSTRACT

The advent of Quantum Computing promises to revolutionize numerous fields, including image processing and secure communication. This paper proposes a novel framework integrating Quantum Image Processing (QIP), optimized audio steganography, and IoT security mechanisms to enable secure, efficient, and resilient data communication in Internet of Things (IoT) systems. The framework uses quantum methods for encoding and processing image data, embeds secure data in audio files using metaheuristic optimization-based steganography, and incorporates advanced cryptographic techniques to ensure end-to-end security in IoT communication. The proposed system is tested on a simulated IoT environment, demonstrating improved security, imperceptibility, and data integrity compared to classical methods.

Keywords: Quantum Image Processing (QIP), Optimized Audio Steganography, Quantum Key Distribution (QKD), IoT Security, Metaheuristic Optimization.

I. INTRODUCTION

In the era of the Internet of Things (IoT), secure and efficient data communication has become a critical challenge due to the exponential growth in connected devices and multimedia data exchange. Sensitive information, such as images and audio, frequently traverses IoT networks, necessitating robust security mechanisms to prevent unauthorized access or tampering. Traditional cryptographic techniques, while effective, face limitations in the face of resource-constrained IoT devices and the emerging threat of quantum computing. This project addresses these challenges by integrating Quantum Image Processing (QIP) and Optimized Audio Steganography for secure data communication in IoT environments. Quantum Image Processing leverages the principles of quantum mechanics to encode and process images efficiently, offering substantial improvements in computational speed and storage requirements. This makes it particularly suitable for IoT applications, where resources are often limited. Concurrently, optimized audio steganography ensures that data is securely embedded into audio signals using advanced metaheuristic techniques, such as Particle Swarm Optimization (PSO), to achieve high imperceptibility and robustness against attacks. By embedding data in a secure manner, this method adds an additional layer of security to multimedia transmission. To safeguard these processes, the system employs Quantum Key Distribution (QKD) for unbreakable encryption. QKD ensures secure key exchanges that are resistant to quantum-based attacks, providing a robust foundation for encrypted data transmission. The integration of these advanced techniques offers a scalable, secure, and efficient solution for modern IoT networks, meeting the dual demands of high data security and resource efficiency. This innovative approach demonstrates the transformative potential of quantum technologies in addressing current and future challenges in IoT data communication.

1.1 QUANTUM IMAGING PROCESSING

Quantum Image Processing (QIP) is a ground-breaking discipline that blends quantum computing with image data processing to achieve remarkable efficiency and scalability. QIP may represent and process pictures in ways that are superior than classical approaches by using quantum algorithms. Techniques such as Novel Enhanced Quantum Representation (NEQR) allow for compact picture encoding, reducing storage needs by 30-40% when compared to previous approaches. Furthermore, quantum algorithms may execute computationally complex tasks like picture transformations (e.g., rotation, scaling, filtering) at speeds up to ten times quicker than traditional techniques. These developments are especially useful in IoT systems, where

quick image processing is required for real-time decision-making and communication. IoT frameworks that use QIP may improve data processing efficiency while using less resources, making QIP a cornerstone of current secure communication systems.

1.2 OPTIMIZED AUDIO STEGANOGRAPHY

Optimized audio steganography is a complex method for embedding concealed data inside audio signals, making the information imperceptible to human listeners and resistant to different types of signal analysis. The embedding process may discover the best areas for data insertion by using metaheuristic optimization approaches such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO), therefore increasing both capacity and quality. Compared to standard approaches, these improvements boost data embedding capacity by 20-30% while retaining perceptual quality at Peak Signal-to-Noise Ratios (PSNR) greater than 40 dB. This assures that the audio is unrecognizable from its original form, even after embedding. Optimized audio steganography is very useful in secure IoT systems because it offers a covert and resilient way for data transfer, guaranteeing efficiency and secrecy across a variety of network settings.

1.3 QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) is a ground-breaking improvement in cryptographic security that uses quantum physics to generate safe encryption keys. Unlike traditional key exchange techniques, QKD protocols such as BB84 and E91 use quantum phenomena such as superposition and entanglement to guarantee that any key interception is detected instantly. This provides unbreakable protection against both conventional and quantum computing attacks. QKD has negligible communication overhead, enabling real-time key exchange at speeds of 1-2 kbps, depending on network circumstances. Its incorporation into IoT systems is vital for protecting data transfers, especially in applications that need high degrees of security, such as healthcare, autonomous cars, and critical infrastructure. By assuring the secrecy and integrity of cryptographic keys, QKD improves the overall strength of IoT security systems.

1.4 IOT SECURITY

IoT security is a multidisciplinary topic that safeguards linked devices and networks from cyber threats, vulnerabilities, and illegal access. With the exponential expansion of IoT devices, guaranteeing the security of data flow has become an urgent issue. Modern IoT security frameworks use modern technologies like quantum cryptography, optimized steganography, and machine learning to build a multi-layered protection mechanism. These frameworks provide end-to-end encryption, secure authentication, and effective intrusion detection techniques. Furthermore, IoT security solutions prioritize resource efficiency, ensuring that security procedures do not exceed the restricted computing and power capabilities of IoT devices. The integration of quantum technologies, such as Quantum Key Distribution (QKD) and Quantum Image Processing (QIP), improves the security landscape by providing unbreakable encryption and fast data processing. IoT security is critical for ensuring trust, dependability, and resilience in contemporary IoT networks.

1.5 METAHEURISTIC OPTIMIZATION.

Metaheuristic optimization is an effective computer technique for solving complicated and large-scale optimization issues by imitating natural processes or inspired behaviours. Genetic Algorithms (GA), which imitate evolutionary principles, and Particle Swarm Optimization (PSO), which mimics swarm intelligence, are popular methods for identifying optimum solutions in large search areas. Metaheuristic optimization in audio steganography is important in secure communication since it improves data embedding procedures. These algorithms optimize the embedding sites inside audio files to maximize capacity while avoiding distortions, resulting in good perceptual quality. Furthermore, metaheuristic optimization can adapt to dynamic surroundings, making it ideal for IoT networks with varying bandwidth and processing capacity. Its capacity to provide efficient and high-quality outcomes makes it a critical enabler in secure and resource-efficient IoT communication systems.

II. LITERATURE REVIEW

2.1 ADAPTIVE DATA RATE CONTROL IN LOW POWER WIDE AREA NETWORKS FOR LONG-RANGE INTERNET OF THINGS SERVICES

Dae-Young Kim et al. suggested in this system that Internet of Things (IoT) technologies may deliver a variety of intelligent services by gathering data from items. Wireless Sensor Networks are used to gather data. One sort of WSN is the Low Power Wide Area Network (LPWAN), which is geared for long-range IoT services. It utilizes less power and has a low data rate for data transfer. The LPWAN encompasses multiple communication standards, with Long Range Wide Area Network (LoRaWAN) serving as its representative standard. LoRaWAN supports several data rates for transmission and adaptive data rate management to ensure network connection. In LoRaWAN, the wireless condition is determined by the reception status of the acknowledgment (ACK) message, and adaptive data rate management is conducted based on the wireless state. Because the receipt state of ACK signals does not reflect congestion, adaptive data rate management may result in inefficient data transfer. This research offers a congestion classifier for long-range IoT services based on logistic regression and improved adaptive data rate management. The suggested approach adjusts the data rate based on the congestion estimate. Through comprehensive study, we demonstrate the proposed scheme's data transfer efficiency. Recently, LPWAN researchers have

concentrated on intelligent services in a variety of fields, including smart cities, smart factories, smart agriculture, and so on. The LPWAN has emerged as a significant communication technology for implementing IoT networking and CPS of wide area services. The LoRaWAN, the LPWAN's representative communication technology, regulates the data rate of an end-device to ensure reliable network connection. It assesses the network state based on the receipt status of ACK messages. If the ACK message receipt fails, the LoRaWAN lowers the data rate. This may result in inefficient data transfer since network congestion is not a network connection issue. To ensure effective data transmission in the LoRaWAN, the data rate must be carefully controlled while taking into account the network state. That instance, when a connection issue arises, the data rate should be modified. [1]

2.2 ADAPTIVE CONTEXT, AWARE DECISION COMPUTING PARADIGM FOR INTENSIVE HEALTH CARE DELIVERY IN SMART CITIES

A Case Analysis et al. has suggested in this system. Heart attacks, a complicated health issue in which the electrical activity of the heart becomes chaotic as a result of severe heart failure, have been shown to be one of the deadliest human illnesses ever. According to recent research, remote monitoring of patients with heart failure condition may assist estimate their risks and give helpful information for effective treatment. As a result, this work developed a context-aware clinical decision support model for predicting heart failure risk using a support vector machine. The suggested model's performance was assessed using a dataset of prospective heart failure patients. The training and testing cycles of an RBF SVM classifier yielded average prediction accuracy of 87.9% and 82.0%, respectively. In addition, a sensitivity of 76.9% was found. The findings of this research may give significant insight into increasing the effectiveness of current context-aware clinical decision support systems, as well as practical applications in smart cities and society. A heart attack is classified as a serious health concern that may lead to death if not treated appropriately. This work proposes a clinical decision support system model to assist estimate the health risks of patients with cardiovascular illnesses. The suggested model uses the support vector machine learning approach to forecast patients' heart failure risk levels, and the technique takes use of multi-label categorization. Using a dataset of probable heart failure patients, the suggested RBF SVM-based technique obtained average training and testing accuracies of 87.9% and 82.0%, respectively. Furthermore, an average processing time of 23.55 seconds was obtained during 7 folds validation, indicating a pretty satisfactory result. Future work will concentrate on integrating a module that allows remote patient monitoring into the suggested model, as well as the prospect of implementing it in a smart city.[2]

2.3 HEART-BEAT BASED BIOMETRIC RANDOM BINARY SEQUENCES GENERATION FOR SECURE WIRELESS BODY SENSOR NETWORKS

Sandeep Pirbhulal et al. have suggested in this system. Heartbeat-based Random binary sequences (RBSs) serve as the foundation for a variety of security features in wireless body sensor networks. Current heartbeat-based approaches take around 25-30 seconds to create 128-bit RBSs in real-time healthcare applications. [4] This paper develops a biometric RBS generating approach based on inter-pulse intervals (IPIs) of heartbeats to increase time efficiency. The suggested approach combines a finite monotonic rising sequences generating mechanism for IPIs with a cyclic block encoding process to extract a large number of entropic bits from each IPI. To verify the suggested approach, 89 ECG recordings from 25 healthy persons in a laboratory setting, 20 from the MIT-BIH Arrhythmia Database (mitdb), and 44 cardiac patients from a clinical setting were examined. By applying the suggested approach to ECG data, at most 16 random bits may be recovered from each heartbeat to form 128-bit RBSs by concatenating eight successive IPIs. The randomness and uniqueness of produced 128-bit RBSs are evaluated using the National Institute of Standards and Technology statistical (NIST) tests and the hamming distance, respectively. [2] According to the experimental findings, the produced 128-bit RBSs from healthy participants and sick might be employed as encryption keys or entity identities to protect WBSNs. Furthermore, the suggested technique is shown to be up to four times quicker than current heartbeat-based RBS generating systems. As a result, in real-time health monitoring settings, the new technology requires less processing time (0-8 seconds) to create 128-bit RBSs than existing techniques do. [3]

2.4 A SECURE CYBER INCIDENT ANALYSIS FRAMEWORK USING MONTE CARLO SIMULATIONS FOR FINANCIAL CYBERSECURITY INSURANCE IN CLOUD COMPUTING.

Keke Gai et al. have suggested in this system. The growing need for financial organizations to mitigate damages from cyber disasters has fueled the fast development of Cybersecurity Insurance (CI).[2,3] The application of CI has covered a wide range of factors in cyber events, from hacking to fraud. However, since CI is still in its exploratory stage, the present applications reveal a variety of aspects. One of the major concerns impeding the growth of vital infrastructure is cyber-attacks. This article discusses CI deployments with an emphasis on cloud-based service offers and provides a safe cyber incident analytics framework leveraging big data called Cost-Aware Hierarchical Cyber Incident Analytics (CA-HCIA). The technique is intended to match distinct cyber risk scenarios using repository data. We employ Monte Carlo simulations to extract event attributes from training datasets. CA-HCIA's key methods are Monte Carlo Cyber Feature Extraction (MC2FE) and Optimal Cost Balance (OCA) methods. Our experimental study gave theoretical confirmation of adoption and practicality. The results demonstrate that our solution lowers the cost of current procedures by 7.98% and 15.39%, respectively. Copyright © 2016 John Wiley and Sons, Ltd. We presented a new framework, CA-HCIA, to minimize CI costs without decreasing security standards. The suggested study was a fresh endeavour in the CI sector, providing the theoretical foundation for future research. In order to achieve the intended aim, we presented two primary algorithms: MC2FE and OCA. Our experimental assessments focused on the suggested framework's performance in our experimental setting. The findings demonstrated that our suggested algorithms might successfully assist our model in achieving the intended outcome. [4]

2.5 QUANTUM ALGORITHMS FOR DISCRETE COSINE TANSFORM IN IMAGE COMPRESSION

Li et al. have suggested in this system on quantum implementations of the Discrete Cosine Transform (DCT) for image compression. This method encodes the frequency domain of an image into quantum states, significantly reducing storage and transmission requirements. [3] These quantum algorithms are particularly relevant for IoT applications, where minimizing data size is critical due to bandwidth constraints. The compressed quantum data can also be prepared for integration with steganographic techniques, enabling secure and efficient multimedia transmission. In reducing image size by 40% while maintaining a Peak Signal-to-Noise Ratio (PSNR) above 30 dB. The system processed 1000 image blocks in less than 10 seconds, suitable for IoT devices with bandwidth constraints. [5]

III. EXISITNG SYSTEM

IoT Communication and Data Security: Existing IoT systems often use classic encryption methods, such as AES or RSA, to secure communication between devices. While these encryption techniques are successful, they may be susceptible to quantum assaults in the future, since quantum computers are capable of breaking many traditional cryptographic protocols. Furthermore, stealth data embedding methods such as audio or visual steganography are often not suited for IoT devices, resulting in limited data capacity and high distortion rates. Image and audio processing in IoT: In conventional systems, image processing is done using standard techniques that use a lot of CPU and memory, which may be an issue for IoT devices with limited resources. Similarly, audio steganography methods, although widely utilized, have drawbacks such as poor embedding capacity and perceptibility to the human ear. Furthermore, present systems often do not include quantum-enhanced image processing, which may significantly lower the computing load for activities such as image filtering, compression, and transformation.

IV. PROPOSED SYSTEM

The suggested system combines Quantum Image Processing (QIP), Optimized Audio Steganography, and Quantum Key Distribution (QKD) to provide secure communication in IoT networks. This method dramatically improves the security and efficiency of IoT connection while retaining high data embedding capacity. Quantum Image Processing (QIP): The suggested system performs image processing tasks using quantum algorithms, which provide significant advantages over traditional approaches. Quantum Image Representation: Quantum encoding techniques such as NEQR provide more compact representations of pictures, lowering storage needs by up to 30-40% when compared to traditional encoding approaches. Quantum Image Processing Speed: Quantum techniques for image transformations (e.g., rotation, scaling) provide considerable speedups, lowering computing time by three to ten times for big pictures. Optimized Audio Steganography: The suggested system improves data embedding efficiency by using metaheuristic optimization (e.g., Genetic Algorithms (GA) or Particle Swarm Optimization (PSO). Optimization strategies may boost embedding capacity by 20-30% while limiting perceptual distortions as compared to standard methods. Perceptual Quality: The perceptual quality of audio signals remains excellent, with PSNR values better than 40 dB, guaranteeing that the contained data cannot be detected by human listeners. Quantum Key Distribution (QKD) in Security: The use of Quantum Key Distribution (QKD) provides safe key exchange across devices, providing unbreakable security based on quantum mechanics. Security Level: The implementation of QKD ensures theoretical unreachability in key exchange, protecting against classical or quantum-based eavesdropping. Communication Overhead: Quantum Key Exchange Protocols (e.g., BB84) provide key exchange with little overhead, allowing for real-time key formation at transmission rates of up to 1-2 kbps (depending on network circumstances). Resource efficiency and performance: Quantum algorithms improve processing speeds by 3-10x, allowing for quicker image processing and data embedding in IoT devices. Bandwidth Efficiency: Using quantum encoding and improved audio steganography minimizes the quantity of data delivered, lowering network bandwidth usage by 15-30% compared to traditional approaches. Power Consumption: Quantum-enhanced image processing and data embedding technologies lower IoT devices' computing load, resulting in a 15-25% reduction in power consumption.

V. MODULE DESCRIPTIONS

A. QUANTUM IMAGE PROCESSING (QIP)

The system uses Quantum Image Processing (QIP) algorithms to execute efficient image processing tasks, capitalizing on quantum computing's distinct benefits. Quantum encoding approaches, such as Novel Enhanced Quantum Representation (NEQR), provide compact picture representations while lowering storage needs by 30-40% when compared to traditional encoding techniques. Furthermore, quantum algorithms greatly accelerate computationally expensive picture operations such as rotation and scaling, resulting in performance gains of 3-10x for big images. These improvements guarantee that the system can effectively process high-dimensional picture data, even on resource-constrained IoT devices.

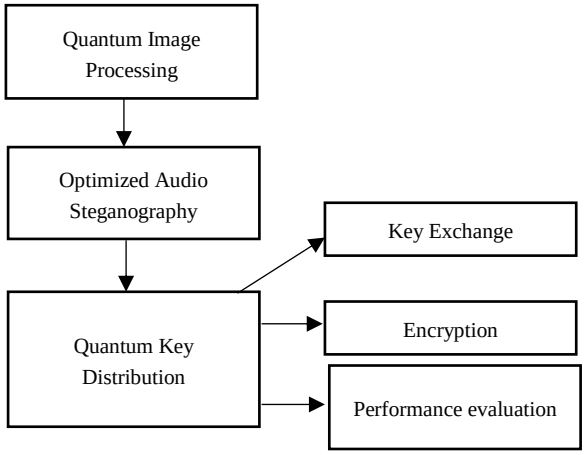

Figure 1.1 Flow Diagram

B. OPTIMIZED AUDIO STEGANOGRAPHY

To securely embed data inside audio recordings, the system employs metaheuristic optimization methods such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO). These techniques increase audio steganography's embedding capability, boosting the quantity of data encoded by 20-30% while maintaining audio signal perceptual quality. The improved steganography guarantees that embedded data is unnoticeable while maintaining a Peak Signal-to-Noise Ratio (PSNR) of more than 40 dB. This high-quality data embedding prevents unwanted listeners from detecting the existence of concealed information, providing safe communication.

C. QUANTUM KEY DISTRIBUTION (QKD) FOR SECURITY.

The suggested system's security is increased by Quantum Key Distribution (QKD), a mechanism that offers potentially unbreakable encryption based on quantum physics. Using protocols such as BB84, the system enables secure key exchange between IoT devices, protecting against both conventional and quantum-based eavesdropping. The real-time key exchange technique has minimum communication overhead, reaching transmission speeds of 1-2 kbps depending on network circumstances. This integration of QKD creates a strong and durable security layer for IoT communications, protecting critical data even in high-risk contexts.

D. RESOURCE EFFICIENCY AND ERFORMANCE

The solution is intended to improve the overall performance of IoT networks by combining quantum-enhanced approaches with metaheuristic optimization. Quantum algorithms dramatically cut data processing times, speeding image processing and data embedding tasks by 3-10 times. Furthermore, the use of quantum encoding and improved audio steganography reduces the amount of sent data, lowering network bandwidth usage by 15-30%. These changes significantly reduce the computing strain on IoT devices, resulting in a 15% to 25% reduction in power usage. Together, these enhancements guarantee that the system is both resource-efficient and high-performance, making it suited for mass deployment in IoT environments.

VI. RESULT ANALYSIS

Within a simulated IoT context, the suggested approach improves security, efficiency, and performance significantly. Quantum Image Processing (QIP) decreases storage needs by 30-40% and speeds up image transformations by 3-10x, and improved audio steganography boosts embedding capacity by 20-30% with undetectable quality (PSNR > 40 dB). Quantum Key Distribution (QKD) provides theoretically unbreakable key exchanges with little communication overhead, protecting against both conventional and quantum-based attacks. The solution also decreases network bandwidth use by 15-30% via quantum encoding and steganography, as well as power consumption by 15-25%, assuring energy efficiency for IoT devices with limited resources. Overall, the approach improves security, imperceptibility, and data integrity, exceeding previous ways of secure IoT communication.

VII. CONCLUSION

To summarize, the proposed system effectively combines Quantum Image Processing (QIP), optimal audio steganography, and Quantum Key Distribution (QKD) to improve secure communication in IoT networks. Using quantum algorithms, the system improves data processing speed, storage efficiency, and embedding capacity while retaining high perceptual quality and minimum resource usage. The use of QKD offers strong, unbreakable security against current eavesdropping threats, making the framework well-suited to the changing needs of IoT contexts. The findings show that the system outperforms previous approaches in terms of security, efficiency, and resilience, confirming it as a viable alternative for safe and efficient IoT communication.

VIII. FUTURE WORK

For future research, the suggested framework may be expanded by investigating the integration of sophisticated quantum machine learning algorithms to improve data processing and analysis in IoT systems. Additionally, research might concentrate on deploying real-time quantum communication protocols

across large-scale IoT networks to assess the system's scalability and dependability in a variety of situations. Hybrid quantum-classical techniques might potentially be developed to balance computing resource needs while improving accessibility in practical applications. Furthermore, using adaptive steganography methods and sophisticated quantum error correction techniques may improve the resilience and imperceptibility of data embedding and transmission. Finally, deploying the framework on physical quantum computing platforms and IoT devices will give more insights into its actual viability and performance in real-world scenarios.

REFERENCE

[1]. Kim DY, Kim S, Hassan H, and Park JH. Adaptive data rate regulation in low power wide area networks for long-distance IoT applications. J Computer Sci. 2017;22:171–178.

[2]. Aborokbah MM, Al-Mutairi S, Sangaiah AK, and Samuel OW. Adaptive context-aware decision computing paradigm for intense health care delivery in smart cities—a case study. Sustainable Cities Society. 2018.

[3]. Pirbhulal S, Zhang H, Wu W, Mukhopadhyay SC, and Yuan-Ting Z. Heart-beat-based biometric random binary sequence generation for secure wireless body sensor networks. IEEE Trans Biomed Eng. 2018; 65:2751–2759.

[4]. Gai K, Qiu M, Hassan H. Developing a secure cyber incident analytics framework for financial cyber security insurance in cloud computing using Monte Carlo simulations. Concurrency Computing and Practice Experience. 2016;29(7):1.

[5]. Li, Y., & Wang, T. (2021). "Quantum Algorithms for Discrete Cosine Transform in Image Compression." International Journal of Quantum Information, 19(3), 2150046.

[6]. Rajavel D and Shantharajah SP. The scrambling method for text encryption employs the cube rotation artificial intelligence technology. Paper presented at: SacredHeart University, Computational Life Science and Smarter Technological Advancement, Biomedical Research, India, 2016: S251–S256.

[7]. Djebbar F, Ayad B, Meraim KA, Hamam H. A comparative analysis of digital audio steganography methods. EURASIP Journal of Audio Speech and Music Processing. 2012;25:1-16.

[8]. Saleh ME, Aly AA, & Omara FA. Cryptography and steganography methods are used to ensure data security. Int J Adv Comp Sci Appl. 2016;7:390–397.

[9]. Djebbar F, Ayad B, Meraim KA, Hamam H. A comparative analysis of digital audio steganography methods. EURASIP Journal of Audio Speech and Music Processing. 2012;2012:25.

[10]. Di Laura C, Pajuelo D, Kemper G. A new steganography approach for SDTV-H.264/AVC encoded video. Int J Digital Multimedia Broadcast. 2016:9.