Measuring Fidelity of Steganography Approach in Securing Clinical Data Sharing Platform using Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM)

A.M. Adeshina, Siti Fatimah Abdul Razak, Sumendra Yogarayan, Md Shohel Sayeed
Faculty of Information Science & Technology, Multimedia University, Malaysia
Email: am.adeshina@mmu.edu.my, codedengineer@yahoo.com, fatimah.razak@mmu.edu.my, sumendra@mmu.edu.my, shohel.sayeed@mmu.edu.my

Keywords: steganography, cryptography, steganalysis, peak signal to noise ratio, structural similarity index measure

Received: January 23, 2024

In the vast digital landscape, the practice of data hiding finds multifaceted applications, ranging from simple hobbyist endeavors to critical tasks like safeguarding user privacy and ensuring covert data transmission. One of the gaping vulnerabilities in many contemporary systems is the transparency with which information is stored, making it easily interpretable. Such clear visibility can be a gateway for potential leaks, false portrayals, or even be manipulated for various malevolent intents. Consequently, as a countermeasure, steganography emerges at the forefront, extensively being resourceful in the revolutionized data storage concept, the cloud technology. Unfortunately, most earlier image steganography methods could only conceal one type of file, audio, text, image within an image, rendering them monodynamic. This study focuses on the novel application of steganography towards embedding information across multiple images to facilitate security of clinical data sharing platform as opposed to traditional single-image methods. The implementation was carried out using Ruby on Rails architecture, leveraging the ChunkyPNG library. With the analyses of image texture features, adaptive payload distribution strategies were devised and compared with the established single-image steganographic techniques. Interestingly, our findings show employing strategies based on texture complexity and distortion distribution greatly enhances security, making it more resilient to modern pooled steganalysis. The exceptionally high PSNR values consistently above 90dB, coupled with SSIM values nearing 1, collectively underscore the near-identical nature of our original and stego images. This convergence of both metrics emphasizes the effectiveness of our steganographic methods, suggesting minimal distortions and high fidelity. Such compelling outcomes not only validate the methodology employed but also accentuate its potential for applications demanding subtle data concealment. In essence, the combined insights from PSNR and SSIM robustly affirm the project's success in achieving high-quality steganographic results.

Povzetek: Študija uporablja steganografijo za izboljšanje varnosti platforme za izmenjavo kliničnih podatkov. Predlaga se nova metoda vdelave informacij v več slik (namesto tradicionalne v eno) z uporabo arhitekture Ruby on Rails in knjižnice ChunkyPNG. Razvite so prilagodljive strategije porazdelitve koristnega tovora na podlagi kompleksnosti teksture in porazdelitve popačenj.

1 Introduction

Steganography, being defined as both an art and a science, is all about concealed communication, aiming to embed written content within other unassuming data. This technique ensures that the actual embedded information remains inconspicuous. In the modern age, as information storage transitions to being predominantly digital due to the surge in ICT advancements, the importance and utility of such covert communication methods have witnessed a meteoric rise.

The beauty of steganography lies in its subtlety, it can seamlessly embed either a straightforward message or an encrypted one within a digital host file. This ensures the encoded message remains discreet, especially during transmission across digital networks. While cryptography stands as the age-old bulwark of information security, steganography introduces an added layer, bringing more depth to the protection, especially in the realms of digital media copyrights. The field of information hiding, ever-evolving, casts a wide net over a myriad of applications, be it watermarking, fingerprinting, or the discreet art of steganography. Watermarking, for instance, leans more toward embedding pertinent data such as owner credentials or specific timestamps to thwart potential copyright infringements. Conversely, fingerprinting is all about integrating a unique serial identifier into a dataset, helping monitor and curb unauthorized exploitation of the same. The digital age, characterized by its unbridled communication channels, has underscored the criticality of enhanced security protocols, particularly within interconnected networks. With the world increasingly becoming interconnected and the volume of data exchanges skyrocketing, the imperative of ensuring confidentiality and maintaining data integrity has never been higher. This escalating concern has been a driving force behind the robust evolution and development of intricate information-hiding methodologies.

Steganography, at its core, is the subtle art of concealing information within digital media. On the other hand, cryptography delves deep into the complex realm of encoding information, employing an array of intricate techniques to ensure it remains inaccessible to unauthorized users. While cryptography shoulders the responsibility of preserving communication confidentiality, steganography thrives on maintaining the secrecy surrounding the very existence of concealed information. As our world increasingly embraces electronic communication and relies heavily on the vast infrastructure of the internet, the imperative for robust information security escalates. Traditional cryptography, though a stalwart in its domain, focuses predominantly on safeguarding content. However, in certain situations, the need transcends mere content protection; sometimes, the very revelation that a hidden message exists can be detrimental. Here, steganography fills the void, it masterfully embeds information within everyday digital media, be it images, videos, or audio files, thereby evading undue attention or suspicion. Given its multifaceted applications, ranging from digital media copyright protection to watermarking and fingerprinting, steganography's importance is undeniable. Its relevance only grows in our digital age, where network security emerges as a paramount concern, leading to the rapid evolution of the broader field of information hiding, encompassing both cryptography and steganography.

In contemporary society, steganography's identity is deeply intertwined with digital data carriers and the pulsating rhythm of high-speed network communications. Drawing a comparison with cryptography, the distinction becomes clear: while cryptography aims to shield the content of a message, steganography thrives on obscuring the message's very existence. Both technologies, with their unique strengths, have carved out essential roles in the overarching goal of data protection. However, like all technologies, neither steganography nor cryptography is a silver bullet; each has its vulnerabilities and can potentially be compromised under specific scenarios. A significant challenge for steganography is that once the clandestine nature of the embedded information is suspected or, worse, unearthed, its primary objective is immediately jeopardized. Yet, the dynamic interplay between steganography and cryptography offers a promising avenue. By synergistically combining these two methods, one can amplify the effectiveness of steganographic techniques, ensuring a more robust and layered approach to securing sensitive information.

Several efforts were frequently into tackling secure transmission of images containing embedded data over a network by image steganography. More attention was recently on further resolving challenges of earlier image steganography methods on only able to conceal one type of file (e.g., audio, text, image, etc.) within an image. As a result, recent studies aim to create an image steganography system capable of concealing text and image within an image. The aim of this study is to develop an image steganography system that hides either text or image files within an image by proposing a framework for an image steganography model, design and implement the framework proposed and evaluate the designed and implemented framework using PSNR (Peak Signal-to-noise Ratio) and Structural Similarity Index Measure (SSIM).

2 Related works

2.1 Data sharing platform

A data sharing platform is a vital technological system that underpins the seamless exchange, collaboration, and dissemination of data among diverse entities, from organizations to individual researchers. Such platforms are pivotal in converting expansive data into actionable insights, particularly in the era of Industry 4.0. Karabacak et al. (2022) shed light on this notion by proposing a unique document-based data-sharing platform software architecture. This architecture is meticulously designed to address the intricate challenges tied to the analysis of vast data sets, with a particular focus on metadata management, which serves to thwart data complexity while elevating its usability. Concepts of connected networks (Adeshina & Hashim, 2017), which have now being seen quite resourceful very recently will immensely benefit from improved data architecture.

At the heart of this architecture lies a sophisticated metadata store, equipped with a suite of tools tailored for data owner identification, intricate versioning processes, and thorough lineage tracking. The architecture doesn't just stop there; it prioritizes data accessibility by presenting detailed illustrations that pinpoint critical data locations. This emphasis on accessibility is seamlessly complemented by robust mechanisms to uphold data quality, encompassing user-centric data preprocessing techniques. Furthermore, to fortify the system against potential security vulnerabilities, the architecture integrates rigorous operational security controls and an astute user group management framework.

Delving deeper into the functionalities, the software architecture refines data management by classifying information into stochastic data sets, thereby offering role-tailored suggestions to its users. It adopts a dynamic version and rule adaptation methodology, ensuring the platform remains resilient to evolving data landscapes. Moreover, a bespoke rule customization mechanism stands ready to cater to specific user-driven requirements. In their comprehensive exploration, Karabacak et al. (2022) elucidates the nuances of this document-based data-sharing platform, accentuating its pivotal role in championing efficient data management and fostering collaboration.

Research data sharing platforms, as detailed by Hahnel (2023), represent pivotal online systems developed to bolster the storage, management, and dissemination of research data among the global scientific fraternity. These digital infrastructures serve as linchpins, championing the virtues of transparency, seamless collaboration, and reproducibility of pivotal research findings. As such, researchers are endowed with a unified, secure sanctuary, allowing them to store and propagate their research data. This centralized approach not only amplifies access but also paves the way for potential data reuse by the broader research community.

In the intricate landscape of clinical cohort studies, researchers delve into the life histories of population groups, seeking understanding of disease progression Vilaza et al. (2020). Newly minted health research data platforms have revolutionized this process, granting unprecedented access to cohorts' non-identifiable health details, with cutting-edge initiatives even assimilating mobile-generated data.

In the vast digital ecosystem, certain platforms are tailor-made to address the unique needs and nuances of specific industries, be it healthcare, finance, or the multifaceted world of agriculture (Yoon et al., 2018). Rather than adopting a one-size-fits-all approach, these specialized platforms zero in on the intricate challenges and opportunities inherent to their respective sectors. Through that, they become invaluable conduits, seamlessly facilitating data sharing among myriad organizations nestled within a particular industry. The ripple effect of such targeted data exchange is profound. Not only does it foster an environment conducive to collaboration, but it also paves the way for robust benchmarking exercises.

2.2 Steganographic procedures

Steganography stands as a nuanced technique, meticulously designed to clandestinely embed secret information within digital media, predominantly images, ensuring such embeddings fly under the radar of unintended observers. The advent and meteoric rise of cloud technology have significantly transformed the digital storage landscape, with cloud storage platforms becoming the de facto choice for housing vast repositories of digital images. This proliferation of cloud-based image storage has inadvertently spawned an exciting avenue for steganography. Now, instead of being confined to embedding information in a solitary image, the technique can be scaled to span multiple images, marking a paradigm shift from traditional single-image steganographic methods.

In this evolving context, Liao et al. (2022), through an insightful publication in the IEEE Transactions on Dependable and Secure Computing, delve deep into the intricacies of optimally allocating embedding payload across a sequence of images, all with an overarching goal to bolster security efficacy in this new era of multiple image steganography.

Two distinct payload distribution blueprints emerge from Liao's research. The inaugural strategy is anchored in image texture complexity, wherein the embedding payload distribution is meticulously choreographed in sync with the image's unique texture attributes. In contrast, the secondary strategy pivots towards distortion distribution, keenly focusing on distributing the payload in alignment with the distortions birthed during the embedding phase. Such strategies, as proposed, don't exist in isolation; they are adeptly designed to coalesce with cutting-edge single image steganographic algorithms, thereby amplifying their inherent security attribute.

Image Steganography stands as an artful technique of discreetly embedding information-be it text, image, or video-within a primary or cover image. Executed with finesse, this embedded information remains invisible to the naked eye, ensuring the secrecy of the data. With technological advancements, particularly the emergence of deep learning technology, steganography has undergone significant evolution. Deep learning, having etched its mark in diverse applications, is now making inroads into the domain of image steganography, attracting a surge of research interest Subramanian et al. (2021). The crux of Subramanian's exploration lies in dissecting and elucidating the myriad deep learning methods prevalent in the field of image steganography.

In the realm of secure communication, various methods are employed to ensure the confidentiality of information exchanged through different channels such as phones, faxes, computer communications, and radio. Steganography offers three primary types which are Pure Steganography, Private Key Steganography, and Public Key Steganography.

Pure steganography emerges as a distinctive approach, concentrating on the concealment of information within digital media, devoid of any reliance on cryptographic techniques or password defenses. Sharma (2017) delves deep into this concept, advocating for its potential as a singular strategy to bolster information security amidst the plethora of existing mechanisms. In today's digital epoch, myriad security protocols and algorithms are enlisted to shield data from unauthorized access and potential cyber threats. Cryptography, with its robust frameworks, often stands at the forefront of such defenses, recognized widely for its efficacy. Yet, pure steganography diverges, aspiring for stealth without leaning on the cryptographic pillar.

Private key steganography emerges as a transformative approach, amplifying data steganography's security threshold by integrating a private key, serving as an auxiliary encryption stratum. Alqadi's exploration (Alqadi, 2020) unveiled in the International Journal of Engineering Technologies and Management Research, charts a course towards enhancing the security matrix of the well-trodden LSB2 (Least Significant Bit 2) method - esteemed for its capacity to cloak secret dispatches in digital color canvases. While LSB2 has carved its niche for preserving the host image's pristine quality even as it harbors clandestine messages, its inherent simplicity has left it vulnerable, often placing it in the crosshairs of hacking endeavors. Alqadi charts a pioneering pathway, offering a remedy in the form of a private key mechanism to galvanize the security bastion of the LSB2 methodology. At the heart of this proposition lies the extraction of a bespoke key from the host image, functioning as the linchpin for secret message encryption.

Public key steganography (PKS) is an intricate merger of steganography with the tenets of public key cryptography. Casting a spotlight on this evolving intersection is the review contributions of Abdul-Razak et al. (2018) which meticulously curated to furnish readers with a holistic perspective, spanning the characteristic features, rich content, and evaluation matrices intrinsic to PKS. Central to the discourse are three pillars: the multifaceted domains where PKS finds application, the diverse schemes championing its cause, and the critical yardsticks employed to gauge the efficiency of PKS infrastructures. Through this tri-pronged lens, Abdul-Razak et al. (2018) dissects and compartmentalizes findings, bequeathing a structured, panoramic view of the PKS landscape. This methodical exploration is not just a mere documentation; it emerges as a treasure trove, brimming with insights, primed to enrich researchers and aficionados venturing into the PKS domain.

2.3 Steganographic filing methods

Text steganography, Protocol steganography, Audio steganography, Image steganography, and video steganography, are the primary categories of file formats commonly used in steganography.

Text steganography has risen as a key technique for discreetly embedding messages within textual documents. Majeed and the team (Majeed et al., 2021) emphasize in their insightful analysis featured in the journal of Mathematics. The technique provides an overview of the intricate methodologies, a litany of challenges faced, and potential future trajectories in this unique field of study. While encryption methods, like cryptography, often shoulder the brunt of data protection efforts, Majeed et al. (2021) contend that steganography presents an unparalleled approach, deftly interweaving hidden messages within overt narratives or other cover media.

The data Protocol steganography has emerged as an innovative mechanism, intricately crafting covert channels within the lattice of network protocols, offering a secure conduit for the surreptitious transmission of privileged information. Alishavandi & Fakhredanesh (2021) pave the way for an avant-garde approach, christened as Master Key Identifier based Protocol Steganography (MKIPS). This groundbreaking methodology is intricately tailored for the Secure Real-time Transfer Protocol (SRTP), a cornerstone in the realm of Voice-over-Internet Protocol (VoIP) communications.

Venturing into the mechanics of MKIPS, it brilliantly harnesses the sender's prerogative to cherry-pick a master key from a meticulously curated reservoir of cryptographic keys. These keys are gracefully presented by an external key management protocol during the crucial phase of session initiation. Through astute manipulation of the master key identifier field as part of the SRTP packet orchestration, Alishavandi & Fakhredanesh (2021) delineate the establishment of a covert channel. Impressively, this clandestine conduit seamlessly operates beneath the canopy of the SRTP channel, showcasing an admirable bandwidth, its prowess dictated by the inherent characteristics of the SRTP channel in operation.

Audio steganography, at its core, intricately embeds covert messages within the vast expanse of audio data, thus offering a fortified layer of security during data transmission (Abdulkadhim & Shehab, 2022). As featured in the International Journal of Electrical and Computer Engineering (IJECE), meticulously sketches out a crypto-steganographic blueprint tailored to surreptitiously nestle an audio or voice message within two distinct cover media forms, specifically audio and video. The ingenuity of this method stems from its harmonious melding of the least significant bits (LSB) algorithm and the intricate 4D grid multi-wing hyper-chaotic (GMWH) system. Initially, an audio undergoes a transformative shuffle orchestrated by a key birthed from the GMWH system. This meticulous shuffle not only introduces a layer of intricate complexity but also fortifies the audio against the prying eyes of hackers, making the extraction of the original composition a daunting task. The empirical results underscore the method's superiority, showcasing its enhanced security pedigree in juxtaposition to its contemporaries.

Image steganography has transformed from a mere technique into a crucial facet of data security, significantly bolstered by the proliferation of cloud technology and its expansive cloud storage possibilities. This progression enables a shift from the conventional single-image steganography to an innovative approach where skilled steganographers judiciously embed covert information across a multitude of digital images. Consequently, these adapted payloads, spread across images, culminate in a cryptic array of concealed data, primed for cloud-based transmission to the intended audience.

Video steganography, a pivotal instrument in the cybersecurity toolkit, ensures that confidential information remains clandestinely embedded within video files, thereby bolstering data transmission security. A major caveat, however, is the discernible limitations of conventional algorithms, which grapple with sluggish convergence rates, illuminating the pressing need for a more adept algorithmic framework. In response to this exigency, Salunkhe & Bhosale (2022) unveils an innovative algorithm coined as the Water-Earth Worm Optimization (WEWO) in a seminal paper published in the International Journal of Engineering Science and Technology. This avant-garde algorithm, the product of an intricate amalgamation of the Water wave optimization (WWO) and Earth worm optimization (EWO) model algorithms, emerges as a potential game-changer in the realm of video steganography. As part of its modus operandi, the video frames are subjected to rigorous preprocessing and extraction processes, leveraging the capabilities of Discrete Cosine Transform (DCT) and Structured Similarity Index (SSIM) techniques.

For the pivotal task of pixel prediction, an astutely designed fitness function-birthed from neighborhood entropies-becomes the cornerstone of the proposed algorithm. Herein, the surreptitious embedding of the covert message is accomplished via a meticulous two-tier decomposition process hinged on Wavelet Transform (WT). To critically evaluate the WEWO-Deep RNN algorithm's mettle, comprehensive experiments were orchestrated utilizing the 'CAVIAR' dataset. Rigorous tests assessing the algorithm's resilience against modular perturbations such as salt, pepper, and combined noises were conducted. Drawing from quantifiable metrics like Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Correlation Coefficient (CC), which are indispensable for gauging image quality, the results gleaned from Salunkhe & Bhosale research emphatically spotlight the WEWO algorithm's superior prowess in seamlessly embedding encrypted messages without compromising the overarching video quality.

2.4 Watermarking and fingerprint

Watermarking and Fingerprinting are two related steganographic technologies that are often used in the protection of intellectual property.

The heatmap function watermarking, as a technique, embeds imperceptible yet robust data within digital media, be it images, audio, or videos. Its primary function serves as a mechanism for copyright protection, authentication, and ownership verification, ensuring media content is traceable even if illicitly altered or redistributed. A significant stride in this domain has been the amalgamation of deep learning into watermarking methods. With the submission of Li (2021), deep learning-based watermarking techniques are explored at length, elucidating their strengths and potential constraints. The study espouse the potential of these techniques, particularly emphasizing how deep neural networks amplify the robustness and security of the embedded watermarks. The efficacy of deep learning in this domain suggests its pivotal role in ensuring watermarks remain undisturbed, even when the media is subjected to modifications. This innovation not only ensures the robustness of watermarking but also sets new paradigms for securing digital media.

Shah & Prakash (2020) delves into the intricacies of watermarking algorithms tailored explicitly for images. Recognizing the limitations of traditional LSB-based watermarking techniques, The researchers propose an enhanced method, intertwining Discrete wavelet Transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) to bolster the protection of copyrighted images. The novelty of the proposed technique lies in its remarkable robustness, ensuring that watermarks remain resilient against potential alterations. Furthermore, they prioritize the aesthetic aspect, ensuring minimal perceptual distortion while maintaining a robust security shield for the images. This dual emphasis on both security and image quality underscores the importance of their research, making the findings indispensable for those looking to strike a balance between protection and presentation.

Given the critical nature of medical data, watermarking in the realm of medical imaging demands specialized attention. Chugh & Vashishth (2020) undertake this responsibility, offering a comprehensive examination of digital watermarking techniques custom-built for medical images. The discourse spans across the multifaceted dimensions of watermarking, be it security, tamper detection, or authentication. The research accentuates the bespoke challenges posed by the medical sector, underscoring the need for watermarking methods that cater to the specific requirements and nuances of medical images.

3D watermarking, given its unique challenges and potentials, stands apart in the vast panorama of watermarking research. Cao et al. (2019) explores this niche by introducing an adaptive watermarking blueprint crafted for 3D point clouds. Their approach, tailored to resonate with the distinct attributes of point cloud data, ensures the watermark's seamless embedding and extraction. By integrating an understanding of 3D data's specificities into the watermarking methodology, they have carved out a pioneering path, bridging the chasm between 3D data's potential and the imperatives of robust watermarking.

Dwelling on the foundational aspect of watermarking, Meng & Huang (2018) proffer a blind watermarking blueprint hinging on block Discrete Cosine Transform (DCT) specifically designed for images. The innovation, however, doesn't just rest with the embedding. The true novelty of their method is its recovery capability, ensuring watermarks remain extractable even in the absence of the original host image.

Digital fingerprinting, known as content-based fingerprinting, is a crucial technique used to trace specific digital media instances. By creating a unique "fingerprint" based on inherent features within media, such as images, distinct audio patterns, or video sequences, it offers a novel way to identify and track content (Suhail & Abhayaratne, 2018). This method extends its utility beyond mere identification, proving instrumental in tracing unauthorized copies and managing media distribution. The entire fingerprinting process is methodical.

Shifting focus to image fingerprinting, visual cues like color histograms and intricate texture patterns become pivotal (Casey & Veltkamp, 2019). Such markers form the essence of the extraction process, is consistent with, the metodologies of Suhail & Abhayaratne (2018), they are molded into fingerprints. These fingerprints are then archived for future reference and juxtaposed against new media fingerprints for identification. With fingerprinting techniques extending their influence to areas like digital rights management and plagiarism detection, the digital domain has acquired a structured mechanism to manage and protect its vast media assets.

2.5 Applications of steganography

Steganography plays a pivotal role in the domain of covert communication, acting as a safeguard for sensitive data. By embedding classified information within seemingly benign cover media like images, audio, or text, it offers a camouflage that's nearly undetectable for unintended observers. As a discipline, steganography has evolved dramatically, adapting to the digital age with finesse. Modern challenges in data breaches and information warfare necessitate robust steganographic techniques that can withstand sophisticated scrutiny. One such technique that's risen to prominence due to its simplicity and efficiency is the Least Significant Bit (LSB) embedding. By replacing the least significant bits of cover media with covert data, it seamlessly merges the secret with the innocuous. Renowned for its ease of implementation and impressive imperceptibility, LSB-based steganography has been recognized as an ideal choice for certain secretive communication applications (Sakshi et al., 2022).

Expanding on the realm of steganographic techniques, spatial domain methods have gained traction. Techniques like pixel intensity modifications alter pixel values strategically, thereby embedding classified data. These modifications are meticulously done, ensuring that to the naked eye, the cover media remains unchanged. The genius behind these methods is the exploitation of intrinsic properties of the cover media, leveraging nuances such as color variations or intensity gradients. By making minuscule changes, which often escape detection, these methods can achieve a high degree of secrecy. Such spatial domain techniques offer another layer of versatility to the world of steganography, presenting a formidable challenge to those attempting unauthorized decryptions (Liao, 2022).

Branching further into the multifaceted realm of steganography, frequency domain techniques offer a sophisticated approach. Instead of operating solely on the spatial properties of the cover media, these techniques dive deep into the frequency components. Using transformations such as the Discrete Cosine Transform (DCT) or the Discrete Fourier Transform (DFT), secret data is embedded in the frequency spectrum of the cover. This approach offers a higher degree of camouflage, often eluding traditional detection methods. The strength of frequency domain methods lies in their ability to harness the intricate frequency patterns, embedding information in a way that's both secure and imperceptible (Salunkhe & Bhosale, 2022).

2.6 Least significant bit (LSB) insertion

In the multifaceted domain of steganography, the Least Significant Bit (LSB) technique stands out, especially when it comes to hiding text and images within digital media. Operating in the spatial domain, its simplicity in terms of implementation is noteworthy. The method modifies the least significant bits of a host image's pixels. This involves substituting some parts of the pixel's initial component with the secret data's most significant bits. This very simplicity is something that Liao (2022) has discussed in depth. Despite the approach's simplicity, Sakshi et al. (2022) highlight its challenges, particularly in the realm of image hiding. Here, despite the method's promise, there is an observable degradation in image quality, characterized by an elevated mean square error and a diminished peak signal-to-noise ratio.

Exploring further, the frequency domain techniques in steganography offer a complex and layered approach to data hiding. Moving beyond the spatial characteristics of the cover media, these techniques delve deep into its frequency components. They utilize transformative tools like the Discrete Cosine Transform (DCT) or the Discrete Fourier Transform (DFT) to embed secretive data into the cover media's frequency spectrum. Such methods, due to their intricacy, often dodge conventional detection mechanisms, a point of discussion in the works of Liao (2022). Furthermore, Sakshi et al. (2022) focus on the method's potential, emphasizing its unique ability to manipulate intricate frequency patterns, which makes the embedded data almost imperceptible and thus enhancing the security of the concealed information.

Usually, the least significant bits in each byte group will often results in such minor significance compared to the overall data to the extent that modifying these bits would have absolutely minimal impact on the final result. Indeed, even changing only half of the least significant bits is significantly sufficient to discreetly embed the character 'A' (01000001) into the sequence. This demonstrates how much-hidden data can be concealed using the least significant bit substitution technique. It is a common and straightforward method for message hiding. In this technique, the message is hidden in the least significant bits of image pixels. Modifying the LSB of the pixels has minimal impact on the overall image, resulting in the stego-image closely resembling the original image. In the case of 24-bit images, three bits of each pixel can be used for LSB substitution since each pixel has separate components for red, green, and blue.

2.6.1 Masking and filtering

In steganography, masking and filtering techniques offer robust means of concealing secret messages within digital images without compromising their natural appearance (Purba et al., 2021). These methods manipulate the image's luminance values to seamlessly embed the hidden information. Specifically, the masking step delineates a specific region in the image to insert the message, whereas filtering assigns specific values to this marked section, resulting in a stego image that integrates the secret message without detection. Contrasting this with the least significant bit (LSB) technique, another spatial domain method, masking and filtering display superior resilience against various image manipulations like compression or rotation. This ensures the hidden message's security and retrievability, even if the container image undergoes alterations.

2.6.2 Parity checker method

In the evolving domain of CryptoSteganography, the Parity Checker method stands out for its fusion of cryptography and steganography to bolster the confidentiality of concealed messages (Abdelmged et al., 2016). The technique, detailed by Abdelmged (2016), utilizes a three-pronged approach: Huffman coding, the RC4 encryption algorithm, and the Parity Checker algorithm. Initially, the secret message undergoes compression via Huffman coding, which trims its size. This condensed message is then encrypted with the RC4 algorithm, imbuing it with an additional protective layer. Subsequently, this encrypted cipher text is embedded into the blue layer of a cover image using the Parity Checker algorithm. Critical to this process is the algorithm's ability to maintain the image's visual consistency, ensuring the message's covert nature. Experimental results from Abdelmged's study reveal the superiority of this method, as showcased by a higher Peak Signal-to-Noise Ratio (PSNR) and a diminished Mean Squared Error (MSE), both indicative of superior image quality and the preserved integrity of the embedded message.

2.6.3 Line shift coding

Text steganography presents unique challenges and opportunities, with line shift coding emerging as an effective technique for safeguarding embedded messages within cover texts. A fundamental aspect of this technique is ensuring the concealed information remains undisturbed, while preserving the original text's meaning. Interestingly, the Sundanese script, an official Unicode font, provides a potential medium for such covert embedding. In pivotal research by Ciptaningtyas et al. (2018), an enhanced version of line shift coding was proposed, aimed at augmenting the capacity of the concealed message. Unlike traditional methods that employ the odd row as a pivotal anchor, this revamped approach harnesses both the first and fifth rows as pivot lines. This innovative alteration not only amplifies the capacity for message storage but also fortifies the stego text's resilience against the rigors of processes like printing and copying. Impressively, even after two reprints, the method upholds the sanctity and confidentiality of the embedded messages.

2.6.4 Feature coding

Feature coding is pivotal in music genre recognition (MGR) as it encapsulates the unique nuances and intricacies of various music genres, thus enhancing indexing and retrieval processes. Most traditional representation techniques in MGR emphasize global features, often making determinations based on singular-level attributes. This strategy unfortunately glosses over the significance of granular data and the intricate dependencies present between different abstraction tiers (Ng et al., 2020), which introduces an innovative approach by harmoniously melding a convolutional neural network (CNN) with the likes of NetVLAD and self-attention mechanisms.

Weaving these tools together, the methodology is fine-tuned to capture localized information across multiple levels while also grasping the intertwined, long-term dependencies they share. NetVLAD steps in to code these local features into comprehensive representations, and the self-attention mechanism deftly models the underlying relationships amidst these features. Adding another layer of sophistication, Ng's strategy deploys a meta classifier, designed to learn and adapt from the aggregated, high-tier features sourced from various local feature coding networks. This meta entity shoulders the responsibility of making the conclusive MGR classifications. Experimental trials of this approach have been illuminating, with results showing marked improvements in accuracy over leading models on benchmark MGR datasets such as GTZAN, ISMIR2004, and Extended Ballroom. Through this fusion of feature, coding mechanisms focused on local detail and long-term interdependencies, the MGR field takes a significant leap forward.

2.6.5 Peak Signal-To-Noise ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) is an engineering term used to measure the ratio between the maximum power of a signal and the power of noise that can distort its fidelity. This metric is particularly valuable for assessing the quality of signal representations given their wide dynamic range. In practice, PSNR is often expressed logarithmically in decibels (dB).

Audio steganography aims to achieve capacity, robustness, and imperceptibility simultaneously, but it remains a challenge to effectively implement all three features together. The Least Significant Bit (LSB) embedding method is commonly used in audio steganography due to its high capacity and imperceptibility. However, it lacks robustness compared to other methods. To address this issue, researchers have increased the embedding depth to the fourth, sixth, and eighth LSB levels to enhance robustness. However, this trade-off between robustness and imperceptibility leads to a reduction in the imperceptibility feature, as measured by Peak Signal to Noise Ratio (PSNR) (Azam et al., 2022).

The estimation of PSNR is crucial in assessing the imperceptibility-robustness trade-off in audio steganography. However, there is a lack of studies on PSNR estimation specifically for audio steganography, making early assessment challenging. To overcome this, a PSNR Estimator (PE) method is proposed to estimate the PSNR for each stego-file generated by audio steganography. The PE method utilizes patterns extracted from the embedding process at different levels to estimate the PSNR. The proposed method achieves a high accuracy of 99.9% in estimating PSNR values at various levels. Comparative evaluation with the Mazdak Method demonstrates the superior performance of the proposed PE method in all scenarios (Azam et al., 2022).

3 Methodology

An Image Sharing Platform using Steganography refers to an online platform or service that allows users to share and distribute images while incorporating steganographic techniques for added security and privacy. Steganography involves the concealment of confidential data within the shared images, making it an effective method to protect sensitive information from unauthorized access or detection. With such a platform, users can securely transmit images containing hidden messages or encrypted data, ensuring that the concealed information remains intact and undetectable to outsiders. By leveraging steganography in image sharing platforms, users can maintain the privacy and confidentiality of their shared visual content while benefiting from the convenience and accessibility of online image sharing services.

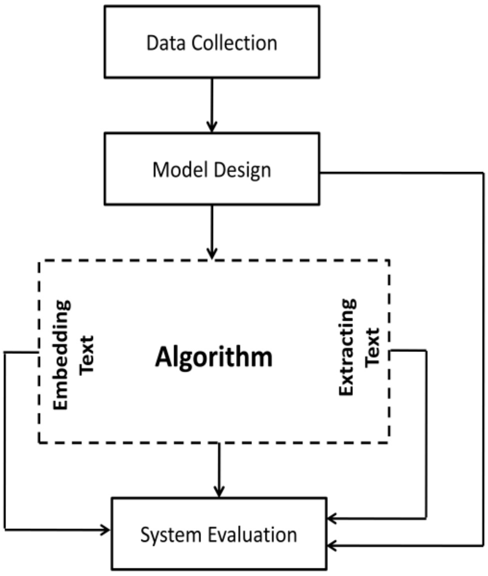

Figure 1: The proposed framework

3.1 Data collection

In order to utilize the proposed application for hiding files, the following data elements such as Cover Image, Message, and Steganographed Image (Stego-Image) were prepared.

3.2 Cover image

The image that serves as the container for the hidden message or data. The cover image can be in any form, such as JPG, PNG, AVIF.

3.3 Message

This represents the file, data, or message that was intended to be concealed within the cover image. The framework accepts text and image.

3.4 Steganographed image

This is the resulting file that is obtained after embedding the hidden data or message into the cover image. The stego-image is essentially a replica of the cover image, typically saved in PNG format.

3.5 Model design

A model is a conceptual representation of a system that simplifies and abstracts the system by disregarding certain details. Developing complementary system models can provide a holistic view of the system, including its context and interactions with other components.

Designing a model for our system involves creating an algorithmic description of the system or process. This theoretical description helps in understanding the inner workings and mechanisms of the system. By utilizing an algorithm, we can outline the step-by-step procedures and logic that govern the functioning of the system.

Creating a model through algorithmic design enables us to analyze and evaluate the system's behavior, identify potential issues or optimizations, and gain insights into its overall functionality.

4 Algorithm

Algorithms are finite sequences of well-defined instructions that are used to solve specific problems or perform computations. They provide unambiguous specifications for tasks such as calculations, data processing, and automated reasoning. Algorithms are expressed in a formal language and can be executed within a finite amount of space and time.

Algorithm 1: describes the processes of how the system embeds text in an image.

Algorithm 2 gives a description of how the system extracts the text from the image.

Algorithm 1

Embedding Text/Image Algorithm (Encoding)

```
STEP 1: Initialize the required modules.
STEP 2: Capture the message input.
STEP 3: Capture the cover image input.
STEP 4: Identify if the message is text or an image.
STEP 5: If text, encode message using Base64.
STEP 6: If text, convert the Base64-encoded message to binary.
STEP 7: If an image, extract its RGB pixel values.
STEP 8: Convert message/image RGB values to binary.
STEP 9: Extract the pixel map of the cover image.
STEP 10: Calculate the cover image's capacity.
STEP 11: Confirm if the message fits in the cover image.
STEP 12: Traverse the cover image pixel by pixel.
STEP 13: Replace LSB of each pixel's RGB with the message's bit.
STEP 14: Continue until all message bits are embedded.
STEP 15: Convert modified binary back to image format.
STEP 16: Save the stego-image.
STEP 17: Provide the output to the user.
```

Algorithm 2

Extracting Text/ Image Algorithm

```
STEP 1: Initialize necessary tools.
STEP 2: Capture the stego-image.
STEP 3: Extract its pixel map.
STEP 4: Traverse each pixel in the stego-image.
STEP 5: Extract the LSB from each RGB component.
STEP 6: Concatenate LSBs to form the binary message.
STEP 7: Identify the end of the message.
STEP 8: Determine if binary represents image or text.
STEP 9: If image, restore binary to image format.
STEP 10: If text, convert binary to Base64.
STEP 11: Decode Base64 to original text.
STEP 12: Present the decoded message to the user.
STEP 13: Conclude the decoding process.
```

4.1 Implementation

The implementation was carried out using the Ruby on Rails framework, leveraging the ChunkyPNG library. Ruby is an interpreted high-level general-purpose programming language. Ruby's design philosophy emphasizes code readability and productivity with its elegant syntax and focus on simplicity. Similar to Python, Ruby also uses significant indentation to enhance code clarity. Ruby on Rails is a framework for web development that is built on the Ruby programming language following the Model-View-Controller (MVC) architectural pattern, which promotes the separation of concerns and facilitates modular development. With analyses of image texture features, adaptive payload distribution strategies were devised and compared with established single-image steganographic techniques.

5 Evaluation

5.1 Testing

Upon entering the required images and text into the designated input fields and initiating the functions to embed or extract files, the program produces specific outputs based on the given inputs. Ten (10) selected Image Sets were prepared for the evaluations.

Primary cover images destined to act as vessels for concealed data and the discrete messages intended for embedding within the cover images were prepared as inputs. Similarly, the stego-images that have gone through the steganography processes were obtained, and the discrete messages were extracted from the images at the output phases.

Image Set	PSNR Value (dB)
Image Set 1	96.52
Image Set 2	102.18
Image Set 3	101.13
Image Set 4	97.39
Image Set 5	101.24
Image Set 6	101.02
Image Set 7	101.37
Image Set 8	101.19
Image Set 9	101.64
Image Set 10	99.96

Table 4.1: Evaluation of Image Sets using PSNR

5.2 Peak Signal-to-Noise Ratio (PSNR)

In the realm of image processing, assessing the quality of images is of paramount importance, especially when comparing an original image to a processed one. One of the widely accepted metrics to measure this quality is the Peak Signal-to-Noise Ratio (PSNR). PSNR is a logarithmic measure that quantifies the difference between the original and the processed images. A higher PSNR indicates better quality, as it suggests a smaller difference between the two images.

For PNG images, the formula to calculate PSNR is:

$\mathrm{PSNR}=20\times\log_{10}(\mathrm{MAXI} / (\sqrt{\mathrm{MSE}}))$

Where,

MAX_I is the maximum possible pixel value of the image. For standard PNG images,

MAX_I is 255.

MSE is the Mean Squared Error between the original and the processed image.

PSNR Values of Image Sets

The Table 4.1 presents the PSNR values for ten different image sets.

5 Discussion

However, analyzing the table, it is evident that all image sets have PSNR values well above 40dB, indicating a very high degree of similarity between the original and processed images in each set. Such high PSNR values, especially those above 100dB, suggest an almost imperceptible difference to the human eye, which denotes outstanding performance in the image processing method employed in this project.

The PSNR value is an indicator of similarity between the two images:

i. Above 40dB: The images are very similar.

ii. Between 30dB to 40dB: Acceptable similarity, but there might be some noticeable differences.

iii. Below 30dB: Significant differences exist between the images.

6.1 SSIM (Structural Similarity Index Measure)

Structural Similarity Index Measure (SSIM) is another critical metric used to assess the quality of images, particularly in the domain of steganography.

Image Set	SSIM Value
Image Set 1	0.9952
Image Set 2	0.9978
Image Set 3	0.9973
Image Set 4	0.9955
Image Set 5	0.9974
Image Set 6	0.9972
Image Set 7	0.9975
Image Set 8	0.9971
Image Set 9	0.9980
Image Set 10	0.9962

Table 4.2: Evaluation of Image Sets using SSIM

Unlike PSNR, which quantifies the difference in pixel values, SSIM evaluates the structural changes between two images, making it a more perceptually relevant metric.

The SSIM index is calculated as:

$\mathrm{SSIM}\ (x, y) = (2\mu_x\mu_y + C_1)\ (2\sigma_{xy} + C_2)/\ ((\mu^2_x + \mu^2_y + C_1)\ (\sigma^2_x + \sigma^2_y + C_2)$

Where:

μ_x and μ_y are the average values of x and y respectively,

σ^2_x and σ^2_y are the variances of images x and y respectively,

σ_{xy} is the covariance of images x and y

C_1 and C_2 are constants to avoid division by 0

A higher SSIM value suggests that the structure, luminance, and contrast of the two images are very similar, if not identical. The resulting value lies between -1 (completely different images) and 1 (identical images).

The Table 4.2 showcases the SSIM values for ten different image sets, reflecting the high similarity between the original and stego images. Observing the table, it's evident that all SSIM values are remarkably close to 1, reinforcing the inference that the stego images are almost indistinguishable from the original ones in terms of structural and perceptual similarity. This high degree of similarity further underscores the efficacy of the steganographic techniques used in this project.

In the implementation phase, the Ruby programming language was chosen for its versatility and adaptability. The Ruby on Rails framework, known for its robustness and streamlined development capabilities, was utilized to create the backend of the platform. The ChunkyPNG library played a pivotal role in implementing steganographic techniques, allowing for the secure embedding of data within image files. Furthermore, Visual Studio Code was used as the primary editor, offering advanced code editing and debugging functionalities, which accelerated the development process.

In the testing phase, the platform was subjected to an exhaustive evaluation. Rigorous unit tests were initially conducted to assess its individual components. This was followed by comprehensive integration tests, which focused on how different parts interacted. Additionally, end-to-end tests were performed to ensure the system functioned as a whole. To evaluate its core features, test cases were specifically designed for both the steganography and encryption functionalities. During this thorough testing process, any discrepancies that arose were immediately identified. Potential vulnerabilities were also spotted and swiftly addressed. As a result of these measures, the system emerged significantly more resilient and secure.

In the evaluation phase, we extensively evaluated our steganographic techniques using two paramount metrics: PSNR and SSIM. While PSNR offered insights into pixel-level differences, SSIM sheds light on perceptual and structural similarities. The PSNR values obtained from the experiments are considered exceptionally high consistently above 90dB. Moreover, the SSIM values were nearing 1. The PSNR and SSIM results collectively underscore the near-identical nature of our original and stego images. Interestingly, the convergence of both metrics emphasizes the effectiveness of the proposed steganographic methods, suggesting minimal distortions and high fidelity. Without mincing words, such compelling outcomes not only validate the methodology employed but also accentuate its potential for applications demanding subtle data concealment. We therefore confirm that the combined insights from PSNR and SSIM robustly affirm the project's success in achieving high-quality steganographic results.

6 Conclusion and future work

The journey of crafting an effective steganography system, underpinned by the Ruby on Rails framework coupled with the ChunkyPNG library, has culminated successfully, fulfilling its envisioned objectives. The primary intent, embedding text within cover images and extracting concealed content from stego-images, was executed with precision. Ruby on Rails, renowned for its robustness in web development, was harnessed to weave a desktop application that married efficiency with user-friendliness. Every user interaction was seamlessly facilitated through an intuitive graphical user interface (GUI), which epitomized simplistic design while not compromising on functionality. This effective synergy between design and backend processing paved the way for an enhanced user experience.

The ChunkyPNG library emerged as an invaluable asset in this endeavor. Its tailored features and modules, meticulously designed for image manipulation, enabled vital processes like RGB template splitting and binary conversion of RGB values. Additionally, its capabilities in merging templates and extracting concealed text were instrumental in breathing life into the core steganography techniques. To gauge the system's efficacy, the Peak Signal-to-Noise Ratio (PSNR) was deployed, offering an objective lens to assess image fidelity. Such a holistic assessment validated the system's prowess in ensuring data security. In essence, this project not only fortified the domain of information security with a robust tool but also sowed the seeds for future innovations, expanding the horizons of steganography research.

Steganography, as a field, is in a constant state of evolution. Each introduction of a cutting-edge steganographic method necessitates the creation of fresh applications, adapting to the innovations. This journey of continuous enhancement has led to contemporary techniques that facilitate data insertion into varied mediums, including images, documents, and audio recordings.

However, a significant constraint of the current application is its exclusive focus on image-based cover files, only allowing images to serve as the carrier. To further elevate the application's utility and reach, it could be adapted to encompass diverse multimedia file types. As our security requirements become increasingly intricate, the scope and applications of steganography are poised for expansive growth.

References

[1] Karabacak, A., Okay, E., & Aktas, M. S. (2022). Document Based Data Sharing Platform Architecture. *2nd International Conference on Design, Research and Development (RDCONF 2022)*, *1*(1), 339–348.

[2] Adeshina, A.M., Hashim, R. (2017) Computational Approach for Securing Radiology-Diagnostic Data in Connected Health Network using High-Performance GPU-Accelerated AES. *Interdiscip Sci Comput Life Sci* 9, 140–152. https://doi.org/10.1007/s12539-015-0140-9.

[3] Liao, X., Yin, J., Chen, M., & Qin, Z. (2021). Adaptive payload distribution in multiple images steganography based on image texture features. *IEEE Transactions on Dependable and Secure Computing*, 1.

[4] Hahnel, M. (2023). Figshare. Retrieved June 5, 2023, from https://figshare.com/. Online Platform for sharing reasearch data.

[5] Vilaza, G. N., Maharjan, R., Coyle, D., &Bardram, J. E. (2020). Futures for Health Research Data Platforms from the Participants' Perspectives. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*.

[6] Yoon, H., Yen, C. W., Tian, F., & Zhang, Z. (2018). Healthcare data sharing in cloud computing environment. Computers, Materials & Continua, 56(1), 145-159

[7] Subramanian, N., Elharrouss, O., Al-Maadeed, S., &Bouridane, A. (2021). Image Steganography: A review of the recent advances. *IEEE Access*, *9*, 23409–23423.

[8] Alqadi, M. A. (2020). Data Steganography Using Embedded Private Key. International Journal of Engineering Technologies and Management Research.

[9] Abdul-Razak, N. H., Din, R., & Ahmad, M. (2018). Comparative review on feature-content based of public key steganography trends. *International Journal of Engineering & Technology*.

[10] Majeed, M., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.

[11] Alishavandi, A. M., &Fakhredanesh, M. (2021). MKIPS: MKI-based protocol steganography method in SRTP. *Etri Journal*, *43*(3), 561–570.

[12] Abdulkadhim, H. A., &Shehab, J. N. (2022). Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system. *International Journal of Power Electronics and Drive Systems*, *12*(1), 320.

[13] Salunkhe, S., &Bhosale, S. (2022). Nature inspired algorithm for pixel location optimization in video steganography using deep RNN. *International Journal on Engineering, Science and Technology*, *3*(2), 146–154.

[14] Sakshi, S., Verma, S., Chaturvedi, P., & Yadav, S. A. (2022). Least Significant Bit Steganography for Text and Image hiding. *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*.

[15] Ng, W. W. Y., Zeng, W., & Wang, T. (2020). Multi-Level local feature coding fusion for music genre recognition. *IEEE Access*, *8*, 152713–152727. https://doi.org/10.1109/access.2020.3017661

[16] Li, S. (2021). Deep Learning-Based Watermarking: A Comprehensive Review and Future Perspectives. IEEE Access, 9, 30552-30571.

[17] Shah, A., & Prakash, O. (2020). An Improved LSB-Based Watermarking Technique Using Hybrid DWT-DCT-SVD for Copyright Protection. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.

[18] Chugh, T., &Vashishth, S. (2020). Digital Watermarking in Medical Images: A Review. Journal of King Saud University-Computer and Information Sciences, 32(8), 1056-1066.

[19] Cao, Y., Huang, J., Yang, L., & Zhang, C. (2019). A Robust and Adaptive Watermarking Scheme for 3D Point Clouds. IEEE Access, 7, 168100-168113.

[20] Meng, H., & Huang, J. (2018). Blind watermarking scheme with recovery capability based on block-DCT for images. Signal Processing, 147, 115-123.

[21] Casey, M. A., &Veltkamp, R. C. (Eds.). (2019). Content-based audio and image retrieval. John Wiley & Sons.

[22] Purba, D. E. R., &Purba, D. (2021). Text Insertion by Utilizing Masking-Filtering Algorithms As Part of Text Message Security. *Jurnal Info Dan Sains: Informatika Dan Sains*, *11*(1), 1–4.

[23] Abdelmged, A. A., Saad, A. S., &Hussien, N. (2016). A Combined Approach of Steganography and Cryptography Technique based on Parity Checker and Huffman Encoding. *International Journal of Computer Applications*, *148*(2), 26–32.

[24] Ciptaningtyas, H. T., Anggoro, R., &Fadhillah, M. B. A. (2018). Text Steganography on Sundanese Script using Improved Line Shift Coding. *Text Steganography on Sundanese Script Using Improved Line Shift Coding*.

[25] Suhail, A., &Abhayaratne, C. (2018). Image and video fingerprinting: Concepts, algorithms, and applications. IET Image Processing, 12(11), 1957-1973.

[26] Azam, M. H. N., Ridzuan, F., &Sayuti, M. N. S. M. (2022). A new method to estimate peak signal to noise ratio for least significant bit modification audio steganography. *Pertanika Journal of Science and Technology*, *30*(1), 497–511.