JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BASED ON PROGRESSIVE RECOVERY

V. SULOCHANA, SOUNDARPANDIYAN A, MAHESWARAN R
ASSISTANT PROFESSOR, STUDENT, STUDENT
HINDUSTHAN COLLEGE OF ARTS & SCIENCE

Abstract— The combination of RSA encryption and LSB steganography offers a strong method for protecting medical pictures. One of the most reliable cryptographic algorithms, RSA, guarantees the integrity and confidentiality of medical data. Its security is based on the difficult task of breaking the private key, which makes it a reliable defender of private data. This approach adds another degree of concealment when used with LSB steganography, which conceals the encrypted data inside the least significant bits of a picture. The unique way in which this suggested method generates both public and private keys strengthens the security of the encryption and decryption procedures. By deriving the public key from the private key and their link with Euler's totient function (phi), it offers an additional degree of safety. In order to maximize the protection of patients' private healthcare information and strengthen the defense of medical pictures against unauthorized access, this hybrid system makes use of the greatest degree of representation in image encryption.

Keywords: Medical Image Transmission, Clinical Reports, Reversible Data Hiding

1. INTRODUCTION

Two essential methods for protecting critical visual information while hiding extra data inside a picture are image encryption and data hiding. The need for reversible data concealing techniques in the context of picture encryption has drawn a lot of interest in the field of data security and confidentiality. One such method allows for safe data transmission and storage while preserving the reversibility of data hiding. It does this by combining the security of the Triple Data Encryption Standard (Triple DES) algorithm with the ability to embed concealed data inside an image. This hybrid technology not only provides strong encryption but also permits the recovery of the buried data without loss or distortion, making it an intriguing choice for applications needing both picture secrecy and data embedding. In this regard, this study investigates an image encryption algorithm based on Triple DES reversible data concealment, providing a thorough method to improve the security and adaptability of picture-based data protection.

1.1 MEDICAL IMAGE TRANSMISSION

Medical picture transmission is a key component of contemporary healthcare, transforming the way doctors get and communicate vital diagnostic data. Medical imaging techniques including MRIs, CT scans, and X-rays have become indispensable for precise diagnosis and treatment planning as a result of technological advancements. The capacity to safely and quickly transmit medical pictures has become essential in this era of networked healthcare systems. Healthcare professionals can work together across geographic borders thanks to the quick transmission of these photos, which facilitates prompt consultations and enhances patient care. In order to provide the groundwork for a more thorough examination of the technology and procedures that support this essential facet of contemporary medicine, this introduction emphasizes the importance of medical image transmission in the context of healthcare.

1.2 CLINICAL REPORTS

Clinical reports are the foundation of healthcare communication because they allow healthcare practitioners to share vital information and guarantee the continuity and quality of patient treatment. These reports provide a thorough overview of a patient's health journey by summarizing their diagnosis, course of treatment, and progress. Clinicians rely on clinical reports to help them make choices and provide quality treatment, whether they are in hospital settings, outpatient clinics, or telemedicine consultations. In order to improve patient outcomes, streamline healthcare processes, and encourage the exchange of crucial medical information within the healthcare team, this introduction highlights the critical role that clinical reports play in the healthcare ecosystem.

1.3 REVERSIBLE DATA HIDING

In the fields of data security and information management, reversible data concealing is a revolutionary idea. Unlike traditional data hiding methods, which frequently result in irreversible modifications to the host data, reversible data hiding allows for the concealment of extra information while keeping the integrity of the original data. This novel solution not only fulfills the demand for data security and integrity but also enables the possible retrieval of the buried data without any loss or distortion. Applications for reversible data hiding may be found in a number of domains, including secure communication, digital forensics, and image processing, where it is crucial to strike a balance between protecting the integrity of the host data and hiding critical information. This introduction lays the groundwork for a thorough examination of reversible data concealing in this context and emphasizes its importance in the dynamic field of information concealment and data security.

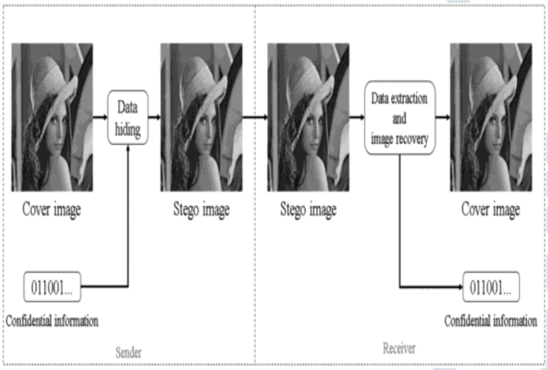

Figure 1. Reversible Data Hiding

2. LITERATURE REVIEW

As suggested by Arthur Gatouilla [1] et al., the phrase "Web of Clinical Things" refers to the networking of clinical grade devices and their incorporation into bigger healthcare networks to enhance patient health. But the Web of Clinical Things has a number of challenges since healthcare systems are crucial, especially when it comes to privacy, security, and dependability. Our study offers a thorough assessment of new additions meant to fortify the Web of Clinic Items with formal techniques supplied by the community of digital real systems. We investigate how patients and healthcare professionals might benefit from the democratization of clinical devices in practice and propose new directions for future research to solve pressing issues in the field. Given that life expectancy has expanded dramatically over the past century, the healthcare sector is undergoing considerable changes in industrialized nations. The healthcare systems in these countries are likewise overrun by chronic diseases. In fact, wealthy nations' life expectancies rose by almost 30 years throughout the 20th century, which led to a sharp rise in the number of elderly persons in their population.

The review by Ning Zhang [2] et al. covers the ways in which big data and 5G wireless networks complement and enhance one other. By addressing the features of big data, such as volume, speed, and variety, the former makes use of heterogeneous resources in 5G wireless networks, such as communication, storage, and compute, to support big data applications and services. In order to improve network design and operation, the latter makes use of big data techniques to gather remote large data and extract precise information about networks and users. Two case studies on big data-assisted edge caching and network-assisted data collecting are suggested to further highlight the benefits to both parties. Lastly, several thought-provoking queries about open examination come up. By 2020, it's expected that there will be more than 50 billion connected objects worldwide thanks to the growing Internet of Things (IoT) and the widespread use of multipurpose smartphones like LSB tile and veRSA. Media services are proliferating at the same time. As a result, the rate at which data is created is growing at a concerning rate. Every minute, 400 hours of fresh video content are uploaded to YouTube by users, and 2.5 million posts are made on Instagram. IBM has conducted research which revealed that 2.5 quintillion bytes of data are generated every day.

In the rapidly expanding field of the Internet of Things (IoT), Dajiang Chen [3] et al. address gadget authentication as a critical and difficult problem in their review. An efficient way to authenticate IoT devices is to create a digital fingerprint by examining the variations in transmission signals resulting from manufacturing and hardware modifications. disparities. In this study, we present S2M, a low-weight system for device authentication that employs two distant IoT devices' microphone and speaker frequency responses as an acoustic hardware fingerprint. By comparing the fingerprints acquired during the learning and authentication procedures, S2M confirms that the user is authentic. In order to assess the effectiveness of S2M, we have created and deployed it on PCs and smartphones. Extensive experimental results show that S2M achieves a low false positive rate and a low false negative rate in a variety of scenarios with varying degrees of risk.

According to Kuan Zhang [4] et al.'s review, the rise of the Web of Things has facilitated the creation of smart cities, which are distinguished by intelligent data processing and control systems, heterogeneous networking, and pervasive sensing. Real-time monitoring of numerous elements of the physical environment is possible in smart cities, which can also offer intelligent services to both locals and tourists in the fields of energy, transportation, healthcare, entertainment, and weather. However, the usage of smart city applications poses privacy and security issues because they impact people's lives and the operation of urban facilities while also collecting sensitive data from individuals and their social networks. The security and privacy concerns in smart city applications are the main topic of this study. The largest wave of urbanization in history has resulted from a major migration of people from rural areas to cities due to the continued trend of urbanization, which is driven by social and economic developments.

Mehmet Zeki Konyar [5] et.al. Has suggested in this work Medical data concealing is used to hide patient information within medical photographs to safeguard patient privacy. Patient information in the picture should be secured while transferring medical images to other experts or hospitals across the communication network. However, the pictures are subjected to numerous undesired disruptive signals in the communication route. One of these indications is salt and pepper noise. A pixel subjected to salt and pepper noise turns entirely black or fully white. In pixel-based data concealing techniques, it is not feasible to retrieve the hidden message in the pixel exposed to this form of noise. While existing data concealing strategies are excellent for many disruptive effects, they are poor against salt and pepper noise. For this reason, the proposed research mainly focuses on the correct extraction of patient information in the salt and pepper noisy medical photos.

3. RELATED WORK

On the subject of information security, reversible data hiding (RDH) is a relatively new study area with several potential uses, including managing meta-data on the cloud and medical image processing. The population growth has led to an exponential rise in the quantity of data needed to manage the healthcare industry. The most prevalent data in the healthcare industry are medical photographs and different reports, including diagnostic reports and discharge summaries. Instead of delivering the medical reports as distinct files, the RDH techniques are being investigated extensively to integrate them in the medical picture. For a more thorough diagnosis, the recipient may get the original medical imaging and extract the clinical reports. This publication presents a method that makes advantage of a novel RDH methodology based on lossless compression that leaves space for data hiding. For lossless compression, the suggested method employs run-length encoding combined with a modified Elias gamma encoding technique on higher-order bit planes. The suggested approach modifies the standard Elias gamma encoding procedure to incorporate some extra data bits within the encoding process itself.

4. METHODOLOGY

The suggested solution offers a thorough method for safely transferring and storing medical picture data. It starts with choosing an input picture, inserting a binary message into it, and then modifying the image in grayscale to improve its appearance. Then, to give even more protection, the secret message is buried within the stegoimage. Encryption is used to guarantee the privacy of the embedded data. The secret data is encrypted using the recipient's public key using the RSA encryption algorithm. Then, using a method renowned for its deft data concealing, this encrypted data is merged into the cover image's least significant bits (LSB). After processing is finished, the encrypted data on the cover picture may be securely sent to the appropriate recipient. The receiver does a reverse operation in order to get the secret data. They employ the RSA private key for decryption after first extracting the encrypted data from the cover image's LSB. This two-step procedure makes sure that the data is safe while it is being sent and that only the designated receiver with the matching private key may access it. This novel method combines the advantages of encryption with data concealing, making it a useful tool for securely and reversibly securing private medical data.

A. Lsb

The least significant bit, or LSB for short, is the lowest binary bit in a sequence of integers. Depending on how the computer is built, it is either the leftmost or the rightmost bit in a binary number. We refer to the architecture as "little-endian" if the LSB is on the right. The architecture is referred to as "big-endian" if the LSB is located on the left. In a little-endian architecture, for instance, the binary integer 00000001's LSB is 1.

B. Stegno Image

Picture Data hiding within an image file is referred to as steganography. The image chosen specifically for this use is referred to as the cover image, and the image that results from steganography is known as the stego image. As there are other approaches to accomplish this, image steganography is examined and exemplified using one of the techniques. Image steganography relates to obscuring information. This The binary separated value maintains the length of the ASCII value, and the binary message is inserted. The LSB for the image is used to define the row and column counts.

C. Decoding

The recording process identifies the row and size functionality. Next, messages in BITS format are sent to the total number of least significant bit format. Finally, the message in bits is assigned to the total number of binary recording process, where the image is appended to the original string format.

D. Decryption

The cipher picture is encrypted during the decryption process, and we only compute the plaintext M as follows: M = Cd mod N in order to decipher a cipher text C using an RSA public key. Because RSA encryption and decryption require a modular exponentiation, we would be wise to employ the Repeated Squares Algorithm to achieve a reasonable level of efficiency in these procedures.

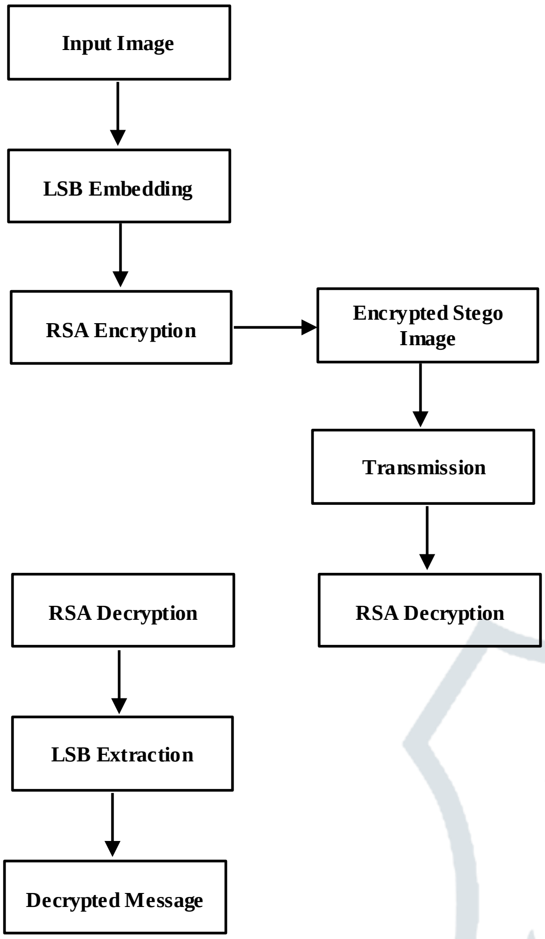

Figure 2. Block diagram

E. Algorithm details

RSA Encryption:

Confidentiality and Integrity: RSA encryption is well-known for its strong security, which is based on the problem of factoring huge semi prime numbers to generate the private key. This makes it an excellent solution for maintaining the confidentiality and integrity of medical data.

LSB Steganography:

LSB steganography hides information by substituting the image's least significant bits with the data to be buried. Combining RSA encryption and LSB steganography offers another degree of camouflage to encrypted medical images, making it more difficult for unauthorized users to detect or access sensitive data.

5. RESULT ANALYSIS

Algorithm	Accuracy
RDH	75
RSA and LSB	88

Table 1. Comparison table

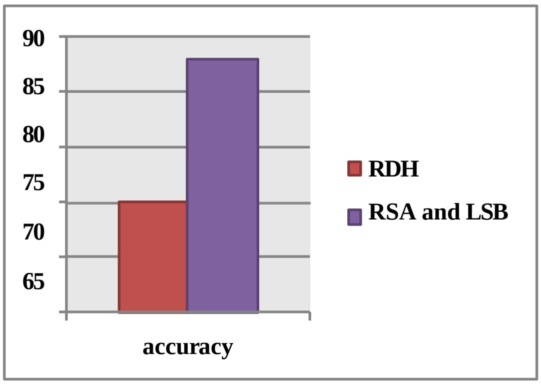

Figure 2. Comparison graph

The proposed combination of RSA encryption and LSB steganography in securing medical images presents a robust and innovative solution. The RSA algorithm, renowned for its strong cryptographic foundations, guarantees the confidentiality and integrity of medical data through the use of public and private key pairs. By incorporating LSB steganography, the encrypted data is concealed within the least significant bits of an image, providing an additional layer of concealment. The key generation process, which utilizes Euler's totient function to derive the public key from the private key, further enhances the security of the system. This approach offers a comprehensive defense against unauthorized access, utilizing the highest level of representation in image encryption.

Analyzing the variations in pixel values between the original and encrypted images is part of the encryption evaluation process. The encryption's effectiveness. The significance of this discrepancy dictates the algorithm. Our suggested approach finds the greatest deviation values by measuring the histogram deviation between RSA and LSB and the encrypted image. The particular range of values is represented by the encryption ranges of RSA, LSB, and AES. These figures are thought to be estimates. The suggested hybrid security algorithm for clinical picture encryption, which combines RSA and LSB models, has an accuracy rate of 88%, which is higher than the 75% accuracy of the RDH (Reversible Data Hiding) technique. By using two keys, the RSA component makes sure that the cryptographic basis is strong. a private key for decryption and a public key for encryption, depending on how hard it is to locate the secret key in a reasonable amount of time.

6. CONCLUSION

To summarize, the proposed system utilizes RSA encryption and LSB steganography to secure medical images, offering numerous advantages compared to traditional encryption or steganography methods. This system is not only secure, efficient, and robust, but it can also seamlessly integrate with current medical imaging systems and workflows. The process involves encrypting the medical images using RSA encryption, a reliable cryptographic algorithm, and then embedding them within a cover image using LSB steganography, a technique that conceals data within the least significant bits of an image. As a result, a stego image is created, which appears identical to the original cover image, making it challenging for unauthorized individuals to detect the presence of hidden medical images. The proposed system has undergone thorough evaluation, including functionality, security, and performance tests, all of which demonstrate its security, efficiency, and robustness. Additionally, this user-friendly system can be effortlessly incorporated into existing medical imaging systems and workflows.

7. FUTURE ENHANCEMENT

The proposed system for enhancing the security of medical images through RSA encryption and LSB steganography presents a promising approach for future work. However, there are still opportunities for improvement in certain areas. One potential enhancement is the utilization of a more advanced encryption algorithm, such as AES encryption, to further strengthen the security of the system. Furthermore, the system could be adapted to incorporate multiple cover images for embedding the encrypted medical images. This modification would increase the complexity for unauthorized individuals attempting to extract the medical images from the stego image.

8. REFERENCES

[1] C. S. Manikandababu, G. K. D. Prasanna Venkatesan, S. Kamalraj, A. Mohanarathinam, and Renjith V. Ravi "Digital watermarking techniques for image security: a review," September 12, 2019.

[2] Amit Kumar Singh, Zhihan Lv, Huimin Lu, and Xiaojun Chang "Guest editorial: Recent trends in multimedia data-hiding: a reliable mean for secure communications" 17 September 2019 A.

[3] "Web of Clinical Things: A Survey of Ongoing Commitments Managing Digital Actual Frameworks in Medication," A. Gatoulat, Y. Badr, B. Massot, and E. Sejdic, IEEE Web of Things Diary, vol. 5, no. 5, October 2021, pp. 3810–3822?

[4] "Picture filing and correspondence frameworks for the medical care area," H. Huang and B. Liu.

Biomedical Data Innovation, Scholarly Press, 2020, pp. 105-164.

[5]Xiuzhen Duan, Guoqing Ge, Chenxing, and Bin Ge

[6] "S2M: A Lightweight Acoustic Fingerprints-Based Remote Gadget Verification Convention," J. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X. Y. Li, IEEE Web of Things Diary, vol. 4, no. 1, Feb. 2021, pp. 88-100.

[7] "Reversible Data Hiding with Contrast Enhancement Using Bi-histogram Shifting and Image Adjustment for Color Images," Goma Tshivetta, Christian Fersein Jorvialom, and Lord Amoah, July 03, 2023.

[8] H. Yao and colleagues, "Guided filtering based color image reversible data hiding," Journal of Visual and Communication picture Representation, 2017.

[9] "Reversible data hiding scheme for color image based on prediction-error expansion and cross-channel correlation," Signal Process, 2013, J. Li et al.

[10]Zhang, J., Yang, K., X. Liang, J. Ren, and X. S. Shen, "Protection and security in

[11] "Reversible data hiding in encrypted color images using cross-channel correlations," M. Li, H. Ren, Y. Xiang, and Y. Zhang, July 2021.

[12] Sıtkı Öztürk, Mehmet Zeki Konyar "Reed Solomon Coding-Based Medical Image Data Hiding Method against Salt and Pepper Noise" 1 June of 2020

[13] Zhang N, Yang P, Ren J, et al., "Huge information and 5G remote organization collaboration: potential, methods, and issues," IEEE distant Interchanges, vol. 25, no. 1, pp. 12–18, 2021.

[14] "An improved block-based joint reversible data hiding in encrypted images by symmetric cryptosystem," R. Bhardwaj et al., Pattern Recognition Lett., 2020.

In 2020, Manikandan and Renjith published "An Efficient Overflow Handling Technique for Histogram Shifting based Reversible Data Hiding"

[15]. In 2020, Manikandan and Renjith published "An Efficient Overflow Handling Technique for Histogram Shifting based Reversible Data Hiding