A Framework for Secure Sharing of Medical Images Based on Visual Cryptography

A Framework for Secure Sharing of Medical Images Based on Visual Cryptography

Christian Coduri
Department of Control and Computer Engineering
Politecnico di Torino
Turin, Italy
christian.coduri@studenti.polito.it

Stelvio Cimato
Department of Computer Science
Università degli Studi di Milano
Milan, Italy
stelvio.cimato@unimi.it

***Abstract*—In the domain of medical data security, the confidentiality and integrity of diagnostic exam results is crucial. However, the use of DICOM files, the standard format for storing and sharing medical images like X-rays and MRIs, can pose security risks because they are not subject to encryption requirements. As a result, these files rely heavily on the security measures implemented within the healthcare institution's networks and databases, which are often inadequate in preventing unauthorized access, data tampering, or malicious injections.**

The goal of this paper is to propose a secure method for sharing and storing diagnostic exam results, ensuring the confidentiality of the information while safeguarding patient privacy. The proposed solution operates directly on DICOM files, utilizing steganography and visual secret sharing to protect and maintain the security of both metadata and pixel data.

***Index Terms*—E-Health, Visual Cryptography, Steganography, DICOM File, Secure Image Sharing**

I. Introduction

The protection of personal data and privacy has become increasingly critical, particularly in the healthcare sector, where hospitals, clinics, and other healthcare organizations are frequent targets of cybercriminals, due to the high value of medical data. This underscores the urgent need for robust security measures to safeguard sensitive patient information.

In this paper we present an innovative security mechanism that combines visual secret sharing and steganography to protect DICOM medical images. The primary contributions of this work are twofold. First, the system extracts pixel values from the DICOM image to generate a cover image in which all metadata are embedded, a process that can be performed in either a reversible or non-reversible manner, depending on the need to fully recover the original pixel values. Secondly, an additive secret sharing scheme called Random Grid Perfect Reconstruction Algorithm (RG-PRA) is introduced as an effective technique for generating two random grids. When combined, these grids enable precise, error-free reconstruction of the cover image, resulting in two distinct share images, each containing part of the medical image data.

The overall architecture involves starting with a DICOM file and generating two shared images: one containing part of the report data, stored at the healthcare facility, and the other provided to the patient. Full reconstruction of the original DICOM file, and thus access to the complete report, is only possible when both shares are available, ensuring that patient consent is required and unauthorized access is prevented.

In this way, the proposed method provides comprehensive protection: metadata is secured through steganography, while the pixel values of the medical image and any personally identifiable information (PHI) that may be directly embedded in the image during certain examinations are safeguarded by the RG-PRA.

II. Related work

Medical images contain highly sensitive patient information, underscoring the need for strong security measures. Various methods have been proposed to enhance their protection, with conventional cryptographic approaches among the most common. These methods rely on a secure key to encrypt and decrypt the images; however, the security of the system is at risk if the key is compromised. Furthermore, traditional cryptographic systems often store encrypted images in a single database, which presents a single-point vulnerability as any breach could expose all stored data. Although various encryption and cryptographic techniques have been proposed to secure medical data (such as [Pra18], [KHE+21], [MBPKS21], [ABS21] and [YLT20]), they commonly face challenges related to key dependency, secrecy, or computational complexity. In [Pra18], two chaotic-based encryption methods for DICOM images are explored. Kamal et al. [KHE+21] proposed a scheme combining block-based segmentation, block scrambling, and chaotic diffusion for both grayscale and color images, with an emphasis on secure key management. Mishra et al. [MBPKS21] introduced a DNA cryptography-based encryption method using confusion and diffusion to enhance randomness. Aouissaoui et al. [ABS21] presented another DNA-based approach that incorporates SHA-256 and MD5 for key generation, while Yin et al. [YLT20] proposed a method based on modified Elliptic Curve Cryptography (ECC) combined with homomorphic encryption for added key sensitivity.

These methods contribute to the field by addressing different aspects of encryption, yet they still depend on key management or involve substantial computational demands. To address these limitations, Visual Secret Sharing (VSS) schemes could be used, offering an alternative by distributing

image shares across multiple locations, thereby improving security and resilience. One such method is the Random Grid-based VSS (RGVSS) proposed by Yan et al. [YLY18], which avoids pixel expansion by encrypting the secret image into n random grids with no discernible meaning. Although RGVSS improves security, the quality of the reconstructed image is relatively low. To enhance this, Mhala et al. [MP19] introduced a contrast-improved VSS scheme for medical images. While the scheme achieves 70% similarity to the original image, sufficient for visual evaluation by medical professionals, it does not enable full reconstruction of the original DICOM file. Another approach that use visual secret sharing for medical images is presented in [MKR20], where the secret medical image is encrypted using a Circular Shift Encryption (CSE) algorithm, and the encrypted image is embedded into three cover images to generate three shares. While this method increases security, it introduces the complexity of managing multiple shares.

III. Preliminaries

A. Visual Cryptography

Visual Cryptography (VC) is a powerful technique that combines the principles of perfect security, secret sharing, and raster graphics. The concept of VC is rooted in Visual Secret Sharing, where an image representing the secret is divided into multiple pieces, known as shares. Individually, these shares reveal no information about the original secret. Reconstructing the secret requires the collaboration of a predetermined number of parties who possess the necessary shares [WY10].

In 1995, Naor and Shamir extended this concept by introducing Visual Cryptography. Formally, VC is defined as a (k, n)-Visual Secret Sharing ((k, n)-VSS) scheme. In this framework, a secret is divided into n shares, and any group of k shares can reveal the secret when combined. Conversely, any group of fewer than k shares reveals no information about the secret [NS95].

Two matrices are defined to determine the color of the subpixels in the shares based on the original pixel's color. Specifically, matrix W is used when the original pixel is white, while matrix B is used when it is black. In a $(2, 2)$-VC scheme, the procedure utilizes the first row of one of the matrices to determine the color of the subpixels in the first share, while the second row is used for the second share. During the share generation phase, a random permutation of the columns of matrices W and B is applied for each pixel of the secret image. It can be observed that, regardless of the column permutation, the following properties hold:

- In the case of a white source pixel, the two rows of matrix W will have the same values, implying that the subpixels in both shares will have the same pattern.
- Conversely, if the source pixel is black, the two rows of matrix B will be complementary to each other, resulting in the subpixels of the two shares having inverted patterns.

After the share generation process, the secret image can be obtained by applying the logical OR operation between the two shares, while for physical prints, the two transparencies can simply be superimposed. Figure 1 shows all possible combinations of shares and their corresponding results.

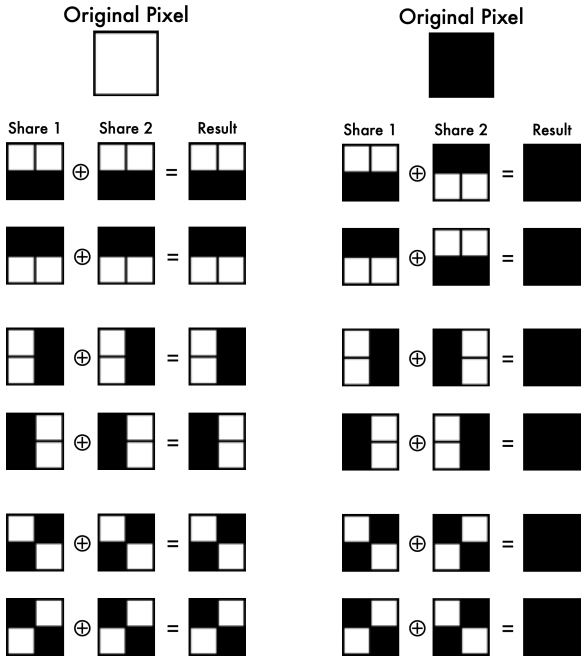


Fig. 1: Basic Visual Cryptography

Due to pixel expansion, the generated shares are twice the size of the original image. Consequently, the reconstructed image will also be twice the size of the original image.

Moreover, when the original pixel is white, a 50% increase in contrast occurs because half of the sub-pixels inserted into both shares are black.

Despite progress in visual cryptography, three major challenges persist: pixel expansion, which doubles the size of the image; degradation of image quality due to contrast issues during reconstruction; and the requirement for different codebooks based on parameters k and n.

B. Visual Secret Sharing with Random Grid

In 1987, Kafri and Keren developed a Visual Secret Sharing (VSS) scheme based on Random Grid (RG), which differs from the Visual Cryptography scheme as it avoids the previously discussed issues of VC [KK87].

Consider a binary image A of size $h \times w$. Two random grids R_1 and R_2 of the same size as A are generated. One of the algorithms proposed by Kafri and Keren for implementing this scheme is as follows:

1) The random grid R_1 of size $h \times w$ is generated by randomly selecting a value of 0 or 1 (white or black) for each pixel;
2) Next, based on the value of the pixel $A[i, j]$ and the corresponding pixel $R_1[i, j]$, the value of the pixel $R_2[i, j]$ is determined as:

$$R_2[i,j] = \begin{cases} R_1[i,j], & \text{if } A[i,j] = 0 \\ \overline{R_1[i,j]}, & \text{otherwise} \end{cases} \tag{1}$$

where $[i, j]$ denotes the position of the pixel in the image ($i = 1, 2, ...h$ and $j = 1, 2, ...w$), and $\overline{R_1[i, j]}$ denotes the complement of $R_1[i, j]$;

3) Repeat Step 2 until all pixels of A have been processed;

If a pixel in A has a value of 1, the corresponding pixels in R_1 and R_2 will be complements of each other. Conversely, if the pixel value is 0, the values of the pixels in R_1 and R_2 will be the same.

Decryption is performed by overlapping the grids. From a computational perspective, this corresponds to an OR operation, which is also used in Visual Cryptography.

Alternatively, the XOR operation enables both VC and RG to accurately reconstruct the secret. However, it requires computations to retrieve the secret and does not permit the random grids (or shares) to be printed on transparent paper, thus preventing the secret from being revealed through grid overlay [KS12].

C. Image Steganography

Steganography is the practice of concealing information within another non-secret medium, such as an image, audio, or text file, so that the existence of the hidden message is not apparent. Unlike cryptography, which aims to obscure the content of a message, steganography hides the presence of the communication [KR16].

A steganographic system is composed of three elements:

- **Cover-image**: the cover object used to conceal the secret message within it;
- **Secret message**: the message that is intended to be hidden and kept secret;
- **Stego-image**: the cover object with the secret message embedded inside.

These methods are typically evaluated based on three main criteria: hiding capacity (the amount of data that can be embedded), image quality (the visual fidelity of the stego-image), and security (the ability to prevent unauthorized access to the hidden data).

Steganography embedding generally degrades image quality, making it impossible to fully recover the original. Reversible steganography, however, allows for the exact recovery of the cover object without any loss of information [LV20].

D. DICOM Standard

In the 1990s, a consortium was formed by NEMA (National Electrical Manufacturers Association) and ACR (American College of Radiology) with the aim of creating a standard communication format for the medical field. This resulted in the development of the non-proprietary DICOM (Digital Imaging and Communications in Medicine) standard for the storage, visualization, and exchange of medical images. DICOM consists of a set of layers and protocols designed to standardize [MDG08]:

- The transmission and storage of medical files;
- The querying and retrieval of such objects;
- The execution of specific actions on these objects;
- Workflow management.

1) Life cycle of a DICOM File: The process of report handling from acquisition to delivery, employed in most healthcare facilities, is schematically illustrated in Figure 2.

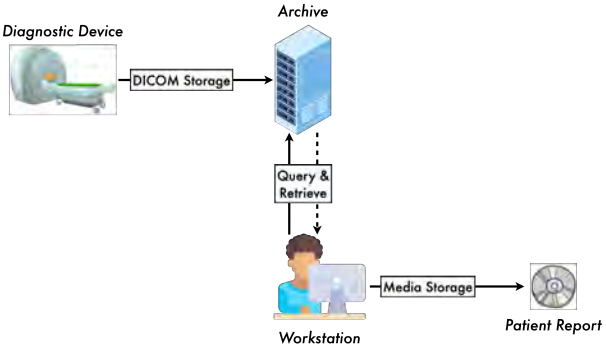


Fig. 2: Life cycle of a DICOM File

Initially, the diagnostic device performs the acquisition and generates one or more DICOM files, which are then stored in a dedicated repository. At a later stage, a designated operator is responsible for retrieving these files and copying them onto a medium intended for the patient. The most commonly used medium is the CD, although reports can also be delivered via alternative methods such as USB drives or email.

It should be noted that the exchange of reports via email can occur not only between the doctor and the patient but also between different healthcare institutions or among doctors requiring access to examination results. Therefore, ensuring security is crucial not only for the DICOM files stored or directly provided to the patient but also for those exchanged through alternative channels.

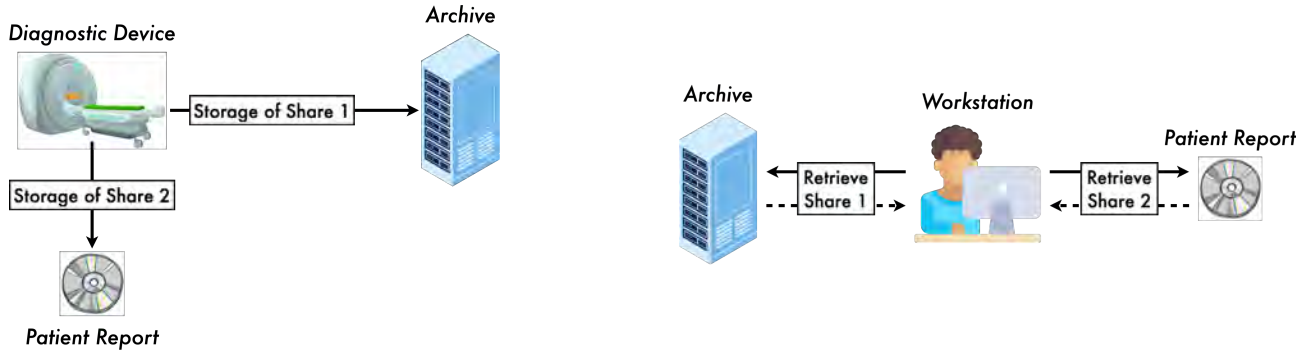
In addition to the actual image, a DICOM file includes various supporting information, known as metadata. These metadata provide details related to the patient, clinical staff, referring hospital, the device used for acquisition, the conditions under which the exam was performed, and other relevant clinical information. A file can contain a variable number of elements depending on the type of examination performed.

IV. Secure Framework for DICOM Image Sharing and Storage

The objective of this work is to propose a framework that enables the secure sharing and storage of diagnostic exam results, ensuring the integrity and confidentiality of information while preserving patient privacy. This framework is designed to operate directly on DICOM files, employing steganography to protect sensitive metadata (PHI) and visual secret sharing to secure pixel data.

A. Proposed Architecture

The proposed secure architecture (Fig. 3) differs from the one currently used in healthcare institutions (Fig. 2). The new architecture divides the diagnostic report into two distinct parts: one stored in the institution's archive and the other delivered directly to the patient.



(a) Storaging — Encryption

(b) Reconstruction — Decryption

Fig. 3: Proposed Architecture

When a doctor wishes to consult the exam results, they cannot simply access the archive and use a key to decrypt the image, as the archive contains only part of the diagnosis. Instead, the physician must obtain the patient's approval, represented by the request and receipt of their share of the report. With both shares available, the doctor can view the complete outcome.

Such authorization will also be required when sharing half of the report between two different doctors or healthcare institutions. In this scenario, the first party can only share the part in their possession. The second party, however, must request the other half from the patient to access the complete exam results.

While this mechanism eliminates the possibility of unauthorized consultations and/or manipulations of reports, it places responsibility on both involved parties. They must carefully safeguard their respective share, as losing one of the two parts will make it impossible to reconstruct the full report.

B. Random Grid Perfect Reconstruction Algorithm (RG-PRA)

To implement such an architecture, a Random Grid algorithm capable of generating two shares from a grayscale image, such that their overlap perfectly reconstructs the original image, is required. To this end, the Random Grid Perfect Reconstruction Algorithm (RG-PRA) has been developed, which implements additive secret sharing and relies on pixel-level subtraction and addition operations.

Consider an image I of size $h \times w$. The first grid R_1, of dimensions $h \times w$, is generated with pixel values ranging from 0 to 255, selected randomly. The second grid R_2, of the same dimensions, is then created using the following formula:

$$R_2[i,j] = I[i,j] - R_1[i,j] \tag{2}$$

Through these two fundamental steps, a pair of random grids is generated: the first grid is produced entirely at random, while the second is obtained by subtracting the pixel values of the random grid from those of the secret image.

To reconstruct the original image, once the two shares are obtained, the following algebraic operation is performed:

$$I[i,j] = R_1[i,j] + R_2[i,j] \tag{3}$$

C. Encryption

The process begins by using the `Pydicom`[1] library to read the DICOM file and retrieve the dataset containing all necessary data for subsequent processing.

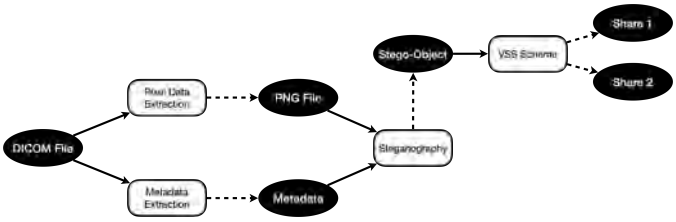


Fig. 4: Encryption Schema

Next, the tool utilizes a specialized library designed for DICOM file interaction, implementing functions to extract pixel values from the DICOM file. The extracted pixel values are then used to create an image in PNG format, which serves as the cover object in the steganography process. To complete the first phase of encryption, the Pixel Data field is removed from the DICOM dataset, while the remaining metadata are extracted and organized into a JSON object.

To ensure accurate decryption and proper reconstruction of the DICOM file, both the essential DICOM metadata and the File Meta Information, which contains critical data related to the file's structure, standard, and compatibility, must be preserved. As such, the JSON object used as the secret in the steganographic process incorporates both components. Its structure is illustrated as follows:

```
{
    "dataset_json": ds.to_json(),
    "metafile_json": ds.file_meta.to_json()
}
```

Once all necessary elements for steganography are prepared, the framework embeds the JSON object into the previously created PNG image, using either a standard or reversible steganography algorithm, depending on the selected algorithm.

[1]https://pydicom.github.io/

The final stage of the encryption process involves applying the RG-PRA algorithm to the resulting stego-object, generating two random grids that securely encapsulate both the pixel data and the metadata extracted from the original DICOM file.

D. Decryption

The decryption process (Figure 5) involves a series of operations that reverse the encryption: starting from two shares, the aim is to reconstruct the DICOM file.

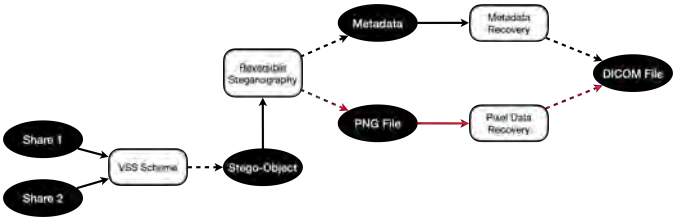


Fig. 5: Decryption Schema

By applying RG-PRA decryption, the stego-object is recovered, enabling the extraction of metadata. If reversible steganography is employed, the original pixel data can also be fully restored; otherwise, depending on the algorithm used, the recovered pixel data may exhibit slight differences. Once these components are retrieved, all necessary elements are available to reconstruct the DICOM file.

V. Evaluation

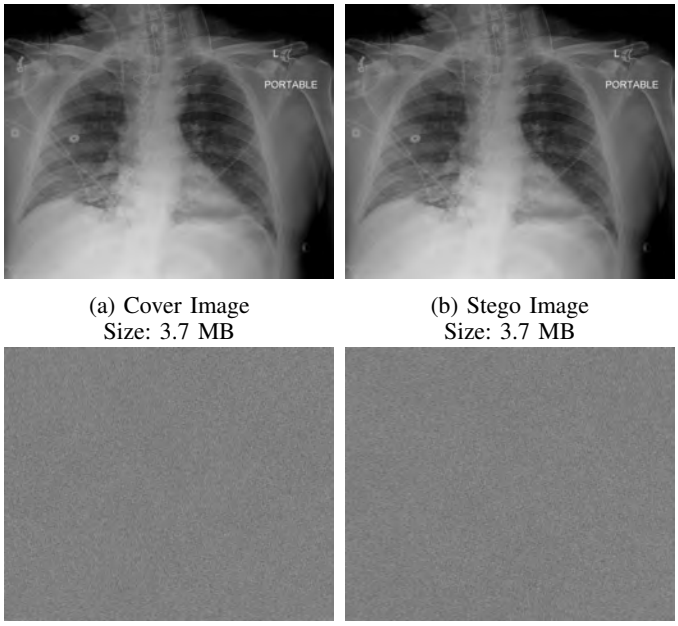
This section presents the evaluation of the proposed framework. Hereafter, Visual Mode denotes the use of a non-reversible steganography algorithm, while Standard Mode refers to the reversible variant.

The DICOM images used for evaluating this framework were sourced from *The Cancer Imaging Archive (TCIA)* [CVS+13], an open-access repository that provides a vast collection of de-identified medical images for cancer research.

In Visual Mode, the Least Significant Bit (LSB) steganography technique is employed, as it provides a simple and efficient method for embedding data into an image with minimal distortion. The data embedding capacity refers to the ability to hide secret data, and in the case of LSB steganography, this capacity is determined by the number of pixels in the DICOM's Pixel Data field, with each pixel capable of embedding a single bit. Similarly, the size of the secret, which includes both the metadata and meta file (expressed in bits), directly dictates the number of pixels required for embedding.

In Standard Mode, reversible steganography based on Histogram Shifting is used, ensuring that the exact same original image can be fully recovered during decryption. The algorithm, developed based on [NSAS06], employs a single pair of zero and peak points. As a result, the embedding capacity is determined by the number of pixels corresponding to the grayscale value at the peak point, making it inherently dependent on the content of the image.

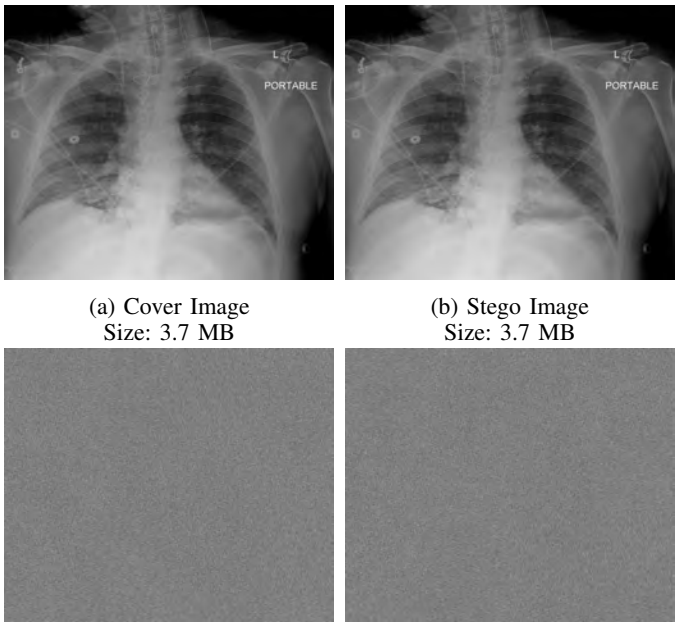
The framework has been tested on DX and MRI images. Figures 6, 7, and Table I present the results of one of our case studies.



(a) Cover Image Size: 3.7 MB (b) Stego Image Size: 3.7 MB

(c) Random Grid 1 Size: 7.6 MB (d) Random Grid 2 Size: 7.6 MB

Fig. 6: Visual Mode Encryption (LSB) – Chest X-ray Image



(a) Cover Image Size: 3.7 MB (b) Stego Image Size: 3.7 MB

(c) Random Grid 1 Size: 7.6 MB (d) Random Grid 2 Size: 7.6 MB

Fig. 7: Standard Mode Encryption (HS) – Chest X-ray Image

In Visual Mode, the DICOM binaries are guaranteed to differ, as the least significant bits of some pixel values are modified. In contrast, Standard Mode always reconstructs high-fidelity images (infinite PSNR), but the resulting DICOM binaries may either perfectly match the original or exhibit slight differences due to bit-level variations introduced during the extraction process, as DICOM pixel encoding is modality-

Experiment	Original DICOM Size	Secret Size	Mode	Embedding Capacity	PSNR	SSIM
DX Chest	7.3 MB	7.28 KB	Visual (LSB)	951.99 KB	72.83 db	1.0
			Standard (HS)	61.73 KB	*inf*	1.0

TABLE I: Summary table presenting the results obtained from one of the case studies

dependent. Nevertheless, both outputs pass validation using the `dicom-validator`[2] tool, demonstrating that the encryption and decryption processes maintain standard integrity.

The table further demonstrates that non-reversible schemes, such as LSB, provide higher data embedding capacity compared to reversible algorithms like HS. However, implementing an HS-based steganography method that utilizes a greater number of zero-peak pairs can enhance capacity as well.

The encryption and decryption times are largely influenced by the specific algorithm used. In general, however, Standard Mode tends to require more time for both processes due to the increased complexity of the reversible steganography algorithms. Additionally, decryption in Standard Mode involves extra processing steps to reconstruct the original pixel values, further contributing to the longer processing time.

VI. Conclusions and Future Works

This project aimed to develop a secure framework for the sharing and storage of DICOM files, ensuring the protection of both image content and sensitive patient data. The results demonstrate that privacy threats, including the exposure of sensitive information through DICOM metadata or directly embedded in images, have been effectively mitigated. Additionally, by using our proposed architecture, security vulnerabilities, such as access attacks on servers storing patient data, have been effectively addressed.

The framework successfully meets its objectives by providing a flexible, dual-mode system that allows users to adjust security levels based on specific needs. This flexibility ensures a balance between computational efficiency and data integrity, meeting the unique demands of medical image management.

Further research may explore text compression techniques, such as eliminating redundant spaces and optimizing formatting, to reduce metadata size, allowing more images to be used with the framework. Expanding the system to handle multiple DICOM files simultaneously would also be valuable, enabling the management of entire DICOM studies and collections of related images from a single medical imaging session, such as a series of MRI slices or a full CT scan for a specific patient. This enhancement would streamline batch processing workflows, improving the framework's efficiency and making it more applicable to real-world clinical and research settings where multi-image studies are common.

VII. Acknowledgement

This work was supported in part by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the Italian MUR. Neither the European Union nor the Italian MUR can be held responsible for them.

[2]https://pydicom.github.io/dicom-validator/

References

[ABS21] Ichraf Aouissaoui, Toufik Bakir, and Anis Sakly. Robustly correlated key-medical image for dna-chaos based encryption. *IET Image Processing*, 15(12):2770–2786, 2021.

[CVS+13] Kenneth Clark, Brent Vendt, Kevin Smith, John Freymann, Justin Kirby, Patrick Koppel, Scott Moore, Susan Phillips, David Maffitt, Michael Pringle, et al. The cancer imaging archive (tcia): Maintaining and operating a public information repository. *Journal of Digital Imaging*, 26(6):1045–1057, 2013.

[KHE+21] Sara T. Kamal, Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, and Mostafa M. Fouda. A new image encryption algorithm for grey and color medical images. *IEEE Access*, 9:37855–37865, 2021.

[KK87] Oded Kafri and E Keren. Keren, e.: Encryption of pictures and shapes by random grids. opt. lett. 12, 377-379. *Optics letters*, 12:377–9, 07 1987.

[KR16] Harpreet Kaur and Jyoti Rani. A survey on different techniques of steganography. *MATEC Web of Conferences*, 57:02003, 05 2016.

[KS12] Sachin Kumar and RK Sharma. Improving contrast in random grids based visual secret sharing. *International Journal of Security and Its Applications*, 6(1):9–28, 2012.

[LV20] Tzu-Chuen Lu and Thanh Nhan Vo. 10 - reversible steganography techniques: A survey. In Mahmoud Hassaballah, editor, *Digital Media Steganography*, pages 189–213. Academic Press, 2020.

[MBPKS21] Pooja Mishra, Chiranjeev Bhaya, Arup Kumar Pal, and Abhay Kumar Singh. A medical image cryptosystem using bit-level diffusion with dna coding. *Journal of Ambient Intelligence and Humanized Computing*, 14, 08 2021.

[MDG08] Mario Mustra, Kresimir Delac, and M. Grgic. Overview of the dicom standard. volume 1, pages 39 – 44, 10 2008.

[MKR20] Richa Maurya, Ashwani Kumar Kannojiya, and B. Rajitha. An extended visual cryptography technique for medical image security. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pages 415–421, 2020.

[MP19] Nikhil C. Mhala and Alwyn R. Pais. An improved and secure visual secret sharing (vss) scheme for medical images. In *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*, pages 823–828, 2019.

[NS95] Moni Naor and Adi Shamir. Visual cryptography. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 1–12, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[NSAS06] Zhicheng Ni, Yun-Qing Shi, N. Ansari, and Wei Su. Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology*, 16(3):354–362, 2006.

[Pra18] Rengarajan Praveenkumar. Medical image encryption. In *Cryptographic and Information Security Approaches for Images and Videos*, pages 297–320. CRC Press, 2018.

[WY10] Jonathan Weir and WeiQi Yan. A comprehensive study of visual cryptography. *Trans. Data Hiding Multim. Secur.*, 5:70–105, 2010.

[YLT20] Shoulin Yin, Jie Liu, and Lin Teng. Improved elliptic curve cryptography with homomorphic encryption for medical image encryption. *Int. J. Netw. Secur.*, 22(3):419–424, 2020.

[YLY18] Xuehu Yan, Xin Liu, and Ching-Nung Yang. An enhanced threshold visual secret sharing based on random grids. *Journal of real-time image processing*, 14:61–73, 2018.