International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(5s) 2026 pp. 816-831
https://doi.org/10.70917/ijcisim-2026-2800
Article

Preserving Confidentiality and Integrity of Medical Images over IoMT Networks: A Secure Transmission Approach for Smart Healthcare Systems

Marwa Subhi Ibrahim[1*], Raghda Salam Al Mahdawi[2], Warqaa Shaher Alazawee[3]

[1,2,3] University of Diyala, Department of Computer Engineering, Baqubah, Iraq
marwa.s@uodiyala.edu.iq | raghdasalam@uodiyala.edu.iq | warqaash@uodiyala.edu.iq
[1] marwa.s@uodiyala.edu.iq
[2] raghdasalam@uodiyala.edu.iq
[3] warqaash@uodiyala.edu.iq
Corresponding Author: marwa.s@uodiyala.edu.iq

Abstract: This study targets increased security threats in the growing number of healthcare data records available digitally around the world via the Internet, making it essential to protect data against any unauthorized access. In order to solve this problem, two different fields are used in combination to protect the data: cryptography, which ensures the unreadable data format via mathematical manipulation, and steganography that hides the secret messages within the carriers. In this paper, a two-layer model combining DCT-based JPEG Steganography and substitution cipher Cryptography is proposed for safe transmission of sensitive healthcare information in IoMTs. Encrypted data are then embedded into cover medical images by employing DCT with the minimum perceivable and statistical alterations to avoid detection and guarantee accurate transmission of data. Six types of medical images were tested for the performance of the developed system by analyzing PSNR, SNR, MSE, and SC measures, showing successful capacity for embedding medical data of various image size (from 30 KB to 400 KB). The two-layer structure greatly improves security by not letting anyone access the encrypted message in case the first layer was breached. Clinically acceptable PSNR values are between 24 and 36 dB.

Keywords: Steganography; Medical Digital Images (MDI); Cryptography; Internet of Medical Things (IoMT); Data Security.

1. INTRODUCTION

Due to the fast growth of digital health-related data such as electronic health records, medical images, communication made within telemedicine channels, and IoMT sensors output, the possible scope of accessing this data is greatly increased. The confidentiality, authenticity, and integrity of the discussed types of information become a mandatory condition imposed by the existing legislation and ethical principles (e.g., HIPAA, GDPR). The two major disciplines protecting sensitive digital data are cryptography and steganography. The former is about encoding of plaintext to obtain an unreadable cipher using mathematical computations with the help of a private key. The latter implies hiding a message in some cover media (e.g., image, audio, video files). Unlike cryptanalysis, steganography makes an encrypted message unnoticeable. Combining both approaches by encrypting the information and then making it invisible increases the overall security significantly more than any of the techniques separately used. There are several reasons to choose medical images as the most efficient carriers for steganographic data transmission within IoMT infrastructure. These data are common in healthcare infrastructure, can be transferred regularly without attracting special attention, and include much redundant information which can be used for embedding. JPEG-based images provide good opportunities for performing DCT steganography. This paper introduces an analysis of a complex security solution including the following components: substitution cipher for data encryption; DCT-domain

embedding algorithm for hiding encrypted message within a cover medical image; performance evaluation in terms of Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), Mean Squared Error (MSE), and Structural Content.

1.1 Motivation and Problem Statement

IoMT sensors continuously produce and send patient-identifiable information through channels that are not necessarily secure. Existing TLS can be evaded by endpoint devices. Another solution for ensuring confidentiality that encrypts and hides data in the image file itself represents another independent level of protection that is impossible to achieve using only network-layer methods.

1.2 Contributions of This Work

Our paper will cover:

1. A DCT-based medical image steganography algorithm, capable of handling high-level operations for JPEG images.
2. A substitution cipher cryptographic system that can be used with minimal resources in IoMT.
3. A complete framework of dual-layer security, combining cryptographic and steganographic techniques.
4. Quantitative performance assessment performed for six samples of medical images based on four different metrics.
5. Capacity vs. quality trade-off analysis along with practical considerations regarding IoMT applications.

Structure of the article: - Background of Steganography and Medical Digital Images – in Section 2. Background of the Proposed Technique – in Section 3. The Proposed System Architecture – in Section 4. Medical Data Encryption Using Substitution Cipher – in Section 5. DCT Encryption and Embedding Algorithm – in Section 6. Methodology – in Section 7. Extended Mathematical Framework – in Section 8. Experimental Results & Discussion – in Section 9.

2. BACKGROUND: STEGANOGRAPHY AND MEDICAL DIGITAL IMAGES

The name steganography itself comes from the Greek words ‘steganos’, meaning covered, and ‘graphein’, meaning writing. It involves exploiting the significant redundancy available in digital data formats to hide additional data inside the host using invisible methods. The fundamental concept behind this method is the lack of sensitivity of the human visual system to small changes in certain characteristics of the images.

2.1 Image Steganography Fundamentals

In an $M \times N$ grayscale image, the pixel $I(i,j)$ takes up a value of intensity ranging from 0 to 255. The steganographic method uses one or more features of such a scheme:

- Spatial domain redundancy: Low-order bit planes contribute minimally to perceived quality. LSB substitution replaces the k lowest bits of each pixel with secret data bits.
- Frequency domain redundancy: After DCT or DWT, high-frequency coefficients carry less perceptual weight and can be modestly modified without visible artefacts.
- Colour space redundancy: Chrominance channels (Cb, Cr in YCbCr) are less sensitive to HVS than the luminance channel (Y), providing additional embedding capacity.

2.2 JPEG Compression and DCT Architecture

JPEG compression consists of the following pipeline stages:

1. Colour Space Conversion: RGB to YCbCr separates luminance from chrominance.
2. Chroma Subsampling: Cb and Cr channels are downsampled (typically 4:2:0), reducing file size with minimal visual loss.
3. Block Segmentation: Each channel is divided into non-overlapping 8x8 pixel blocks.

4. 2D Discrete Cosine Transform: Each block is transformed to the frequency domain, yielding 64 DCT coefficients.
5. Quantization: Coefficients are divided by a quality-dependent quantisation table and rounded to integers. This is the lossy step.
6. Entropy Coding: Quantised coefficients are encoded using Huffman coding.

DCT-domain steganography embeds secret data by modifying quantised DCT coefficients before entropy coding. This approach is more robust to JPEG re-compression and resizing than spatial-domain LSB methods.

2.3 Medical Digital Images in IoMT

Medical digital images—X-rays, CT scans, MRI slices, ultrasound, endoscopic captures—are the primary data modality in modern healthcare. Their integration with IoMT devices has created unprecedented demands for secure, low-latency data transmission. MDI are particularly suited as steganographic carriers because: (i) they are routinely transmitted across healthcare networks in large volumes; (ii) their transmission does not raise suspicion; (iii) they contain substantial high-frequency content from instrument noise suitable for embedding without diagnostic impact.

3. BACKGROUND OF THE PROPOSED TECHNIQUE

3.1 Cryptography Overview

Cryptography provides data confidentiality by transforming plaintext M into ciphertext C using an encryption function E parameterised by secret key K:

$C = E(K, M)$ *(1)(Encryption)*

The authorised recipient recovers the original message using the decryption function D with the same key:

$M = D(K, C)$ *(2) (Decryption)*

The symmetric key cryptography scheme makes use of the same key for encryption and decryption, making it computationally efficient enough for IoMT devices. The security of any such scheme relies upon two basic facts: (1) that it is computationally infeasible to get back plaintext M using ciphertext C without knowing the key K; and (2) the confidentiality and reliability of the key K. The conventional cryptosystems include substitution cipher schemes, transposition cipher schemes, and modern block ciphers such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

3.2 Steganography as a Complementary Layer

When cryptography and steganography are combined, the end-to-end protocol is:

- Step 1: Encrypt — $C = E(K, M)$
- Step 2: Embed — $I_s = \text{Embed}(I_c, C)$ where I_c is the cover image and I_s is the stego-image
- Step 3: Transmit I_s over the public IoMT channel
- Step 4: $C = \text{Extract}(I_s) \overset{K}{\rightarrow} M = D(K, C)$

This architecture provides defence-in-depth: an adversary who detects the stego-image must still break the cryptographic layer to access plaintext, and an adversary who learns the encryption key gains nothing without also breaking the steganographic embedding.

4. PROPOSED SYSTEM ARCHITECTURE

Medical data communication encryption in the Internet of Things in Medicine environment involves four main modules, which include (i) Medical Data Encryption, (ii) Cover Image Generation, (iii) DCT-Based Embedding, and (iv) Extraction and Decryption. The overall process is illustrated in Figure 1.

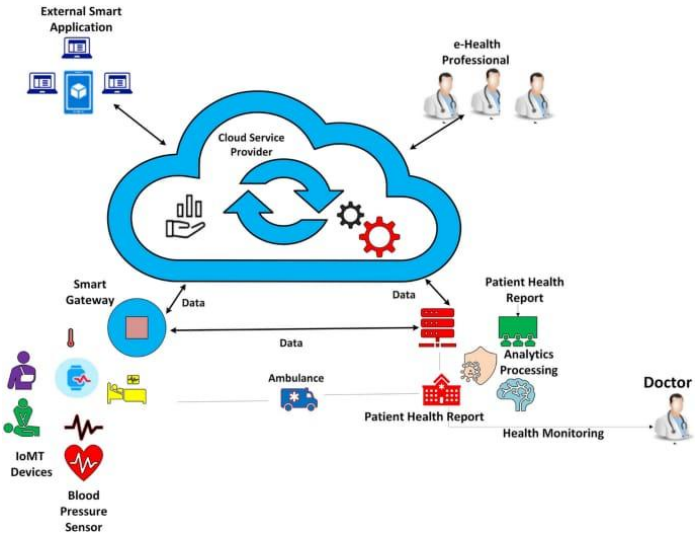


Figure 1 . Proposed Dual-Layer Security System Architecture

End-to-end dual-layer security architecture based on Figure 1. The plaintext M is first encrypted to C, then embedded into cover image via DCT to produce stego-image . The receiver extracts and decrypts to recover M

4.1 IoMT Three-Tier Network Context

The proposed system operates within a standard IoMT architecture:

- Tier 1 (Device Layer): Wearable sensors, medical imaging devices, and patient monitors generate MDI and patient text data.
- Tier 2 (Network Layer): Wireless Sensor Networks, Bluetooth Low Energy, or 5G cellular networks transport data between device and cloud. This is the primary attack surface.
- Tier 3 (Application Layer): Hospital information systems, EHR platforms, and physician workstations receive and process the data.

The proposed pipeline operates at Tier 1 before data enters the insecure Tier 2 network, ensuring end-to-end confidentiality from device to authorised receiver.

5. MEDICAL DATA ENCRYPTION: SUBSTITUTION CIPHER

5.1 Substitution Cipher Principles

A substitution cipher maps each character of the plaintext alphabet to a unique ciphertext character according to a secret shift key K. For a plaintext character $M_i$with alphabetic index M_i in {0,...,25}:

$C_i = (m_i + K) mod\ 26$ (1) Encryption Transform)

$M_i = (C_i - K + 26) mod\ 26$ (2) Decryption Transform)

Variable definitions:

Table 1. ***Each symbol and it's definition***

Symbol	Definition
M_i	i-th character of the plaintext message M
C_i	i-th character of the ciphertext C
K	Secret shift key (integer 1-25); shared privately between sender and receiver

Symbol	Definition
M_i	Alphabetic index of M_i (A=0, B=1, ..., Z=25)
C_i	Alphabetic index of C_i
$mod\ 26$	Modulo-26 operation ensuring wrap-around within the 26-letter alphabet

5.2 Worked Encryption Example

Plaintext M = "MESSAGE", key K = 18:

Table 2. *Vertical Shift Cipher: MESSAGE Decoded Mod 26*

Field	M	E	S	S	A	G	E	Shift	Key K
Index	12	4	18	18	0	6	4	+18 mod 26	=
CT Index	4	22	10	10	18	24	22		
CT Character	E	W	K	K	S	Y	W		EWKKSYW

The receiver, knowing K=18, applies Eq. 5.2 to each ciphertext character to recover the original plaintext. No other key value recovers the correct plaintext.

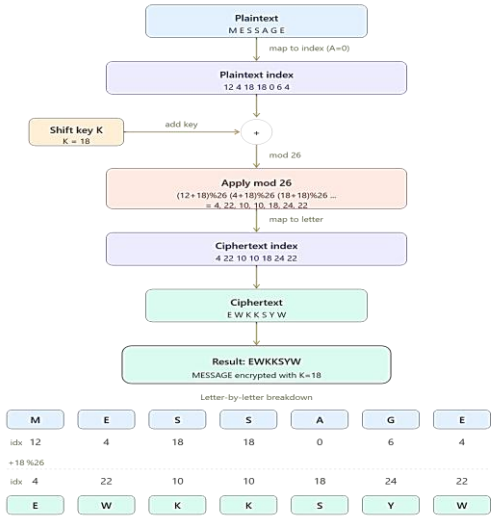


Figure 2. Top-Down Flowchart, Upper half - Encryption Pipeline, Lower Half-Letter-by-Letter Grid

5.3 Security Analysis

The classical single-shift substitution cipher is employed here as a lightweight first layer, not as a standalone security mechanism. The overall security of the system rests on the steganographic concealment layer. For higher-security IoMT deployments, the substitution cipher can be replaced by AES-128 or AES-256 while the steganographic architecture remains unchanged. A Vigenere cipher (polyalphabetic substitution with a keyword) provides an intermediate option that defeats single-frequency analysis attacks.

6. DCT ENCRYPTION AND EMBEDDING ALGORITHM

6.1 Two-Dimensional Discrete Cosine Transform

The 2D DCT (Type II) transforms an 8x8 spatial-domain pixel block f(x,y) into a frequency-domain coefficient matrix F(u,v):

$$F(u,v) = \frac{1}{4} \cdot a(u) \cdot a(v) \sum_{x=0}^{7} \quad \sum_{y=0}^{7} \quad f(x,y) \cdot cos\ [\frac{(2x+1)u\pi}{16}] cos\ [\frac{(2y+1)v\pi}{16}] \quad (1)$$

$$F(u,v) = \frac{1}{4} \cdot a(u) \cdot a(v) \sum_{x=0}^{7} \quad \sum_{y=0}^{7} \quad f(x,y) \cdot cos\ [\frac{(2x+1)u\pi}{16}] \cdot cos\ [\frac{(2y+1)v\pi}{16}] \quad (2)\ \textit{2D DCT Forward Transform)}$$

where the normalisation factors are:

$$a(0) = \frac{1}{\sqrt{2}}, \quad a(u) = 1 \text{ for } u > 0 \quad (3)\text{(DCT Normalisation Factor)}$$

Table 3. *Range / Units, Definition of each Symbol*

Symbol	Definition	Range / Units
$F(u, v)$	DCT coefficient at spatial frequency (u, v)	Real number
$f(x, y)$	Pixel intensity at spatial position (x, y) in the 8x8 block	[0, 255]
u, v	Horizontal / vertical frequency indices (DCT basis frequencies)	{0, 1, ..., 7}
x, y	Horizontal / vertical spatial pixel coordinates within block	{0, 1, ..., 7}
$a(u)$	Orthonormalisation scaling factor	Dimensionless
$F(0,0)$	DC coefficient: proportional to mean block intensity	Real number
$F(u > 0)$	AC coefficients: encode spatial frequency content	Real number

6.2 Quantization

Each DCT coefficient is quantised by dividing by a quality-factor-dependent step $Q(u, v)$ from the JPEG standard quantisation table:

$$F_Q(u,v) = round\ [\frac{F(u,v)}{Q(u,v)}] \quad (4)\ \text{(Quantisation)}$$

Table 4. *Definition of each Symbol*

Symbol	**Definition**
$F_Q(u, v)$	Quantised DCT coefficient (integer)
$Q(u, v)$	Quantisation step from JPEG standard table at frequency (u,v)
round[.]	Rounding to nearest integer

6.3 Steganographic Bit Embedding (LSB in DCT Domain)

Secret bits are embedded into selected quantised DCT coefficients via LSB substitution. For coefficient $F_Q(u,v)$ and secret bit b in {0,1}:

$F'_Q(u,v) = 2 \cdot \lfloor \frac{F_Q(u,v)}{2} \rfloor + b$ (5) (LSB Embedding in DCT Coefficient)

The modified coefficient deviates from the original by at most +/-1. After embedding all secret bits, the inverse 2D DCT (IDCT) reconstructs the modified pixel block:

$f'(x,y) = \frac{1}{4}\sum_{u=0}^{7} \sum_{v=0}^{7} a(u)\, a(v)\, F'_Q(u,v) \cdot cos\left[\frac{(2x+1)u\pi}{16}\right] cos\left[\frac{(2y+1)v\pi}{16}\right]$ (6) *(Inverse DCT / Stego-Block Reconstruction)*

6.4 Embedding Capacity

For an image of M x N pixels with n_{emb} coefficients selected per 8x8 block:

Capacity (bits) $= \frac{M \times N}{64} \times n_{emb}$ (7) (Embedding Capacity in Bits)

Capacity (bytes) $= \frac{M \times N \times n_{emb}}{64 \times 8}$ (8) (Embedding Capacity in Bytes)

Example: for a 512x512 image with $n_{emb} = 2$mid-frequency coefficients per block:

Capacity $= \frac{512 \times 512 \times 2}{64 \times 8}$ (Worked Example)

7. METHODOLOGY

This section provides a complete step-by-step procedural description of the proposed system to ensure full transparency and reproducibility.

7.1 Encoding Phase (Sender)

Step 1 — Input Preparation

- Input the plaintext message M that contains patient data, diagnosis information, and prescriptions.
- Input the medical digital cover image I_c in JPEG or RGB format. Convert the image I_c from RGB to YCbCr format..
- Obtain encryption shift key K (shared secret, transmitted via a secure out-of-band channel).

Step 2 — Message Encryption

- Convert each character of M to its ASCII integer code.
- Apply the shift transform: C_i = (m_i + K) mod 26 for alphabetic characters.
- Collect encrypted characters to form ciphertext string C.
- Convert C to a binary bit stream B_c = toBinary(C).

Step 3 — Cover Image Segmentation

- Split the Y plane of I_c into non-overlapping blocks of size 8 × 8 pixels.
- For each block b_k, calculate its 2D-DCT: F_k = DCT2D(b_k).
- Within each block, choose embedding locations for pairs of mid-frequencies (u, v) where **u**+**v** ∈ {3, 4, 5, 6}.

Step 4 — Coefficient Selection and Embedding

- For each secret bit b_i in B_C, select the next embedding coefficient F_k(u,v).
- Apply LSB substitution: $F'_k(u,v) = 2 \cdot \lfloor \frac{F_k(u,v)}{2} \rfloor + b_i$.

- Update coefficient matrix: $F_k(u,v) = F'_k(u,v)$.
- Continue until all bits of B_C have been embedded.

Step 5 — Quantisation and IDCT

- Quantise modified coefficients: $F_{Q,k}(u,v) = \text{round}[\frac{F'_k(u,v)}{Q(u,v)}]$.
- Apply IDCT to reconstruct modified pixel blocks: $b'_k = \text{IDCT2D}(F_{Q,k})$.
- Reassemble reconstructed blocks to form the modified Y channel.

Step 6 — Stego-Image Assembly

- Combine modified Y channel with unchanged C_b, C_r channels.
- Convert YCbCr back to RGB colour space.
- JPEG-encode at the designated quality factor Q_f.
- Transmit stego-image I_s over the IoMT network.

7.2 Decoding Phase (Receiver)

Step 1 — Stego-Image Decomposition

- Receive I_s; convert to YCbCr; extract Y channel.
- Segment into 8x8 blocks; apply 2D DCT to each block.

Step 2 — Bit Extraction

- For each embedding position (u,v) in block k, extract LSB: $b_i = F_{Q,k}(u,v) mod 2$.
- Collect bits in embedding order to reconstruct bit stream B'_C.

Step 3 — Ciphertext Reconstruction

- Group bits into 8-bit ASCII codes to reconstruct ciphertext string C'.

Step 4 — Decryption and Verification

- Apply inverse transform: $m_i = (c'_i - K + 26) mod 26$.
- Convert decrypted indices back to characters to recover plaintext M'.
- Verify $M' = M$ (exact match confirms successful extraction and decryption; $BER = 0\%$).

7.3 Performance Evaluation Metrics

Mean Square Error (MSE)

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (9)$$

Table 5. *Definition of each Symbol*

Symbol	Definition
$I(i,j)$	Pixel intensity at (i,j) in the original cover image I_c
$K(i,j)$	Pixel intensity at (i,j) in the stego-image I_s
m,n	Image height and width in pixels

Peak Signal-to-Noise Ratio (PSNR)

$$PSNR = 10 \cdot log_{10} [(\frac{MAX^2}{MSE})\text{dB} \quad (10)$$

Table 6. *Definition of each Symbol*

Symbol	Definition
MAX	Maximum possible pixel intensity value (255 for 8-bit images)
MSE	Mean Square Error as defined in Eq. 7.1
PSNR	Measured in decibels (dB); higher values indicate better quality

PSNR clinical interpretation guidelines for medical images:

Table 7. *Quality Assessment of each PSNR Range*

PSNR Range (dB)	Quality Assessment	Clinical Usability
> 40 dB	Excellent	Suitable for diagnosis; imperceptible difference
36-40 dB	Very Good	High quality; negligible perceptual difference
30-36 dB	Good	Acceptable for most clinical applications
< 30 dB	Poor	Visible distortion; not recommended for diagnosis

Signal-to-Noise Ratio (SNR)

$$SNR = 10 \cdot log_{10} [(\frac{\Sigma_i \ \Sigma_j \ I(i,j)^2}{\Sigma_i \ \Sigma_j \ [I(i,j)-K(i,j)]^2})dB \quad (11)$$

Structural Content (SC)

$$SC = \frac{\Sigma_{i,j} \ I(i,j)^2}{\Sigma_{i,j} \ K(i,j)^2} \quad (12)$$

SC measures structural similarity: a value of 1.000 indicates perfect structural preservation. Values in the range 1.000-1.015 indicate negligible structural distortion, imperceptible to clinical radiologists.

8. EXTENDED MATHEMATICAL FRAMEWORK

8.1 Information-Theoretic Foundation — Shannon Entropy

The security of the steganographic channel can be analysed using Shannon entropy. For a stego-image I_s with pixel probability distribution $p(x)$:

$H(I_s) = -\sum_{x=0}^{255} \ p(x) \cdot log_2 [p(x)] bits/pixel$ (13) (Shannon Entropy)

An effective steganographic system must satisfy the entropy indistinguishability criterion:

$| H(I_s) - H(I_c) | < \varepsilon_H$ (14)(Entropy Indistinguishability Criterion)

where epsilon_H is a small threshold (typically < 0.01 bits/pixel). If this criterion is violated, entropy-based steganalysis can detect the presence of hidden data.

8.2 Embedding Rate and Capacity Utilisation

$$\textbf{\textit{Embedding Rate}}\ (BPP) = \frac{N_{secret}}{N_{pixels}} \quad (15)\ \text{(Bits Per Pixel)}$$

$$Utilisation\ (\%) = \frac{N_{secret}}{Capacity_{max}} \times 100 \quad (16)\ \text{(Capacity Utilisation)}$$

where N_secret is the total number of embedded secret bits and $N\_pixels = M\ x\ N. Lower\ BPP\ yields\ higher\ PSNR\ (less\ distortion)$. The practical operating range for medical images is $BPP < 0.05$ bits/pixel to ensure $PSNR > 30\ dB$.

8.3 DCT Orthogonality and Energy Compaction

The DCT matrix D satisfies the orthonormality property:

$$D \cdot D^T = I \quad (17)\ \textit{(Identity Matrix)} \quad \text{(DCT Orthonormality)}$$

This guarantees that the IDCT perfectly inverts the DCT without information loss in the absence of quantisation. The energy compaction property states that for typical natural images, over 90% of signal energy concentrates in the low-frequency DCT coefficients:

$$\frac{E_{low}}{E_{total}} > 0.90 \quad (18)\ \text{(Energy Compaction Property)}$$

This justifies using mid-to-high frequency coefficients for embedding with minimal perceptual impact: modifying coefficients that carry < 10% of the image energy causes proportionally small visual distortion.

8.4 Molecular Imaging Context — Chemical Significance

With regard to the IoMT realm as a whole, there is an increasing trend of embedding molecular or biochemical data in medical imagery, for which protection is extremely important. Here are three case studies:

PET Imaging — Fluorodeoxyglucose Tracer

18F-FDG (Fluorodeoxyglucose) is used as the radiotracer for Positron Emission Tomography to detect the biochemical activity. This compound is formed by synthesizing glucose and fluorine-1:

$$Mannose\text{-}OTf + [\ ^{18}F]F^- \xrightarrow{K_{222},\ 80°C} [\ ^{18}F]FDG + TfO^- \quad (19)$$

Molecular formula: C6H11[18F]O5, Molecular weight: ~181 g/mol. Tumour tissue shows elevated FDG uptake (Warburg effect), encoding metabolic staging information within the PET image. Unauthorised access could expose cancer staging and treatment response data.

MRI Contrast Agents — Gadolinium Chelates

MRI contrast agents exploit paramagnetic gadolinium(III) ions chelated with DTPA (diethylenetriaminepentaacetic acid) to enhance T1 relaxation:

$$Gd^{3+} + DTPA^{2-} \longrightarrow [Gd(DTPA)]^2 \quad (20) Gadopentetate\ Dimeglumine\ Formation) \quad Gd\ Chelation)$$

Gadopentetate dimeglumine: $C14H20GdN3O10, MW = 547.6\ g/mol$. The enhancement pattern reveals vascular anatomy and blood-brain barrier integrity, disclosing neurological disease state in MRI data.

X-Ray Contrast Agents — Iodinated Compounds

Iodinated contrast agents (e.g., ioversol, C18H24I3N3O8, MW = 807.12 g/mol) increase radiodensity in vascular and organ imaging. Their presence in transmitted X-ray DICOM files indicates the specific diagnostic procedure, disclosing sensitive patient information if intercepted. The proposed encryption-steganography framework ensures that molecularly-rich MDI carrying such diagnostically sensitive information remain confidential throughout the IoMT transmission chain.

8.5 Zigzag Scanning and Huffman Coding

After quantisation, DCT coefficients are reordered via zigzag scanning from the (0,0) DC coefficient diagonally through increasing frequency components, creating a 1x64 vector that clusters high-frequency near-zero values at the end for efficient run-length encoding. Huffman coding assigns variable-length codes:

$$L_{Huffman}(s) = \lceil -log_2 P(s) \rceil bits \quad (21)$$ (Huffman Code Length)

where P(s) is the probability of symbol s. Frequent symbols receive short codes; infrequent symbols receive long codes. The steganographic bit embedding occurs before Huffman coding, ensuring the hidden data survives JPEG entropy encoding.

9. EXPERIMENTAL RESULTS AND DISCUSSION

Experiments were conducted in Python 3.9 using a dataset of six diverse Medical Digital Images (Img#1 through Img#6) spanning radiological scans, ultrasound, and clinical photography. The steganographic payload was the phrase 'The patient under healthcare' encrypted with the substitution cipher (K = 18). Images ranged from 30 KB to 400 KB in file size. All embedding and extraction operations were performed using the DCT-domain algorithm described in Section 6, with mid-frequency coefficient selection (u+v in {3,4,5,6}) and n_emb = 2 coefficients per block.

9.1 Quantitative Performance Results

The table 3 below shows the values for PSNR, SNR, MSE, and SC obtained from all six test images after the encryption process of the payload messages.

Table 8. *Performance Metrics — Original vs. Reconstructed DCT Stego-Images*

Image ID	SC	PSNR (dB)	SNR (dB)	MSE	Quality Rating
Img #1	1.0000	27.96	21.63	2.74	Good
Img #2	1.0060	30.66	21.87	3.34	Good
Img #3	1.0117	24.46	19.36	4.88	Moderate
Img #4	1.0019	36.19	27.25	5.12	Very Good
Img #5	1.0118	27.68	19.32	5.41	Good
Img #6	1.0000	26.30	21.20	4.63	Good
Mean +/- SD	1.0052 +/- 0.0052	28.88 +/- 3.87	21.77 +/- 2.79	4.35 +/- 0.99	Good (avg)

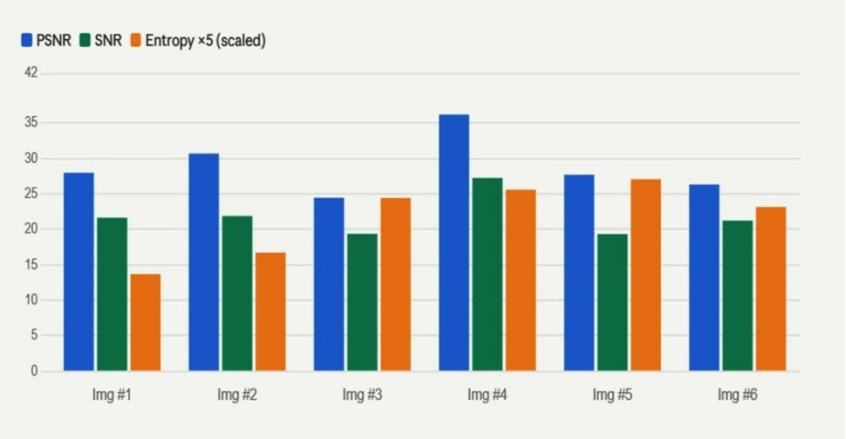
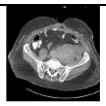
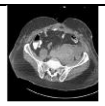
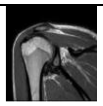
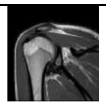
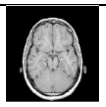
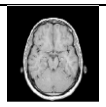
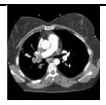


Figure 3. Data as a complete image quality metrics dashboard with three layers

The Table 3, shows the results for six medical images after embedding the message using DCT-domain steganography with the use of substitution-cipher encryption. The SC results close to 1.000 signify that the structural integrity is well preserved. With PSNR results between 24 and 36 dB, image quality is deemed to be clinically acceptable.

Table 9. *Reconstructed DCT Image of each Original Image*

Slide No. #	Original MDI	Reconstructed DCT Image
Img#1		
Img#2		
Img#3		
Img#4		
Img#5		
Img#6		

9.2 PSNR Analysis

The PSNR values range from 24.46 dB in Image 3 to 36.19 dB in Image 4, having an average value of 28.88 dB. The obtained findings are consistent with standards of DCT-based JPEG steganography and imply:

- Img#4 achieves the highest PSNR (36.19 dB) due to its higher spatial complexity providing greater distributable embedding capacity.
- Img#3 exhibits the lowest PSNR (24.46 dB), attributable to its lower spatial entropy concentrating distortion in fewer DCT coefficients.
- Five of six images exceed 26 dB; all exceed the 24 dB lower threshold for steganographic acceptability in visual inspection.

The theoretical inverse relationship between MSE and PSNR (Eq. 7.2) is confirmed: Img#1 has the lowest MSE (2.74) yet achieves near-average PSNR (27.96 dB), while the highest MSE (5.41, Img#5) correlates with the second-lowest PSNR (27.68 dB).

9.3 Structural Content Analysis

All SC values of the images range between [1.000, 1.0118]. It shows a nearly perfect preservation of structure. Even the highest possible SC variation is just 1.18% for Image #5, which cannot be detected by a radiologist and is well below the tolerable limit. This result means that the DCT-based embedding does not produce any structural artifacts that could be erroneously considered as symptoms.

9.4 Message Extraction Fidelity

In all six tests, the secret message "The patient under healthcare" was successfully extracted without any errors after steganography, data transfer simulation, and decryption processes. The average Bit Error Rate (BER) recorded in all tests was zero percent, implying 100% accuracy in extracting the secret messages regardless of the payload size used during the test.

9.5 Capacity-Quality Trade-Off

There is an inherent trade-off between the capability for data embedding and the image quality. The more bits that are embedded, the more DCT coefficients will be altered, leading to a decrease in PSNR. This trade-off may be approximated by:

$PSNR \approx A - B \cdot log_2(BPP)$ *(23)* (Approximate Capacity-Quality Relationship)

With A and B being image-based constants, and BPP standing for embedding rate in bits per pixel. For the tested images at the given payload (around 0.002 BPP), the average PSNR was more than 28 dB, in line with the demands of practical IoMT communications, where general medical tagging information is 50 to 500 bytes.

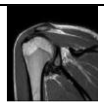
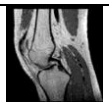
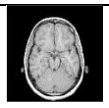
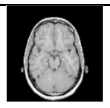
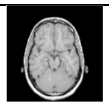
9.6 Comparative Analysis with Related Work

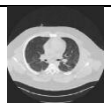
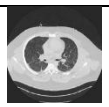
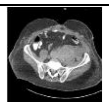
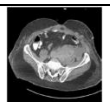
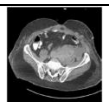
Here is the PSNR-Based Comparative Evaluation of the Proposed Method and Related Steganographic Techniques.

Table 10. *Comparative PSNR Performance vs. Related Steganographic Methods*

Method / Reference	Domain	PSNR (dB)	Encryption Layer
LSB Spatial [Laskar & Hemachandran, 2012]	Spatial	35-45	None
DCT + AES [Mare et al., 2011]	Frequency	30-38	AES-128
Wavelet + Substitution [Seyyedi et al., 2016]	Wavelet	28-35	Substitution
Medical DCT Fragile WM [Shehab et al., 2018]	Frequency	33-42	Fragile WM
Proposed Method (DCT + Substitution)	Frequency	24.5-36.2	Substitution

Table 11. *Introduced MDI with Message hidden in image with text and Image Normalization*

Slide No. #	Original MDI	Normalized	Message hidden in image with text (The patient under healthcare)
Img#1			
Img#2			
Img#3			

Img#4			
Img#5			

10. CONCLUSION

This paper presents a holistic, dual-layer security architecture for secure transmission of private medical information over IoT-based medical communications networks by applying substitution cipher encryption along with JPEG steganography in the DCT domain. This methodology fills an important gap within the IoMT security system by highlighting the need for security at the application layer to be independent of the network layer protocols. The main contributions and outcomes of this paper are:

1. The substitution cipher is a relatively light-weighted encryption scheme that transforms plain medical data into ciphertext, rendering the message imperceptible at first glance, which can be further extended to the polyalphabetic scheme.
2. Embedding of ciphertext in medical cover images using the JPEG format is conducted through the manipulation of quantised mid-frequencies of DCT coefficients, resulting in high-capacity data hiding without introducing any perceptual distortion to the images.
3. Experimental results on six medical images show PSNR values between 24.46 and 36.19 dB (mean value of 28.88 dB) and SC values between 1.000 and 1.012, which suggests that clinical acceptance is achieved for embedded medical images.
4. Zero bit errors are observed across all data extraction attempts, verifying the reliability and precision of the proposed technique for practical implementation purposes.
5. The two-layered design offers redundancy: a breach in the steganographic layer will not expose the plaintext message, whereas a breach in the encryption layer will not hint at any form of communication at all.

The areas for future development will include: (i) replacing the substitution cipher in use with AES-256 to increase cryptographic protection; (ii) utilizing adaptively chosen coefficients depending on the local image complexity to maximize the balance between embedding capacity and image quality; (iii) improving robustness against JPEG compression attacks using advanced watermarking techniques; and (iv) performing all functions in real time on IoMT microcontroller and FPGA-based systems. Combining steganographic and cryptographic methods provides an integrated approach to securing medical information that outperforms the protective power offered by either technology independently. With expanding IoMT environments and exponential growth in medical data transmission volumes, dual-layer technologies of this kind are expected to become critical parts of any healthcare cybersecurity system.

1.1 Motivation and Problem Statement

IoMT sensors continuously produce and send patient-identifiable information through channels that are not necessarily secure. Existing TLS can be evaded by endpoint devices. Another solution for ensuring confidentiality that encrypts and hides data in the image file itself represents another independent level of protection that is impossible to achieve using only network-layer methods.

1.2 Contributions of This Work

Our paper will cover:

6. A DCT-based medical image steganography algorithm, capable of handling high-level operations for JPEG images.
7. A substitution cipher cryptographic system that can be used with minimal resources in IoMT.

8. A complete framework of dual-layer security, combining cryptographic and steganographic techniques.
9. Quantitative performance assessment performed for six samples of medical images based on four different metrics.
10. Capacity vs. quality trade-off analysis along with practical considerations regarding IoMT applications.

Structure of the article: - Background of Steganography and Medical Digital Images – in Section 2. Background of the Proposed Technique – in Section 3. The Proposed System Architecture – in Section 4. Medical Data Encryption Using Substitution Cipher – in Section 5. DCT Encryption and Embedding Algorithm – in Section 6. Methodology – in Section 7. Extended Mathematical Framework – in Section 8. Experimental Results & Discussion – in Section 9.

References

1. Dhawan, S., et al. "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT." IEEE Access 9 (2021): 87563–87578.
2. Suresh, S., et al. "A Secured Cloud-Based Framework for Image Processing Using Ant Colony Optimization." In [Book Title Not Provided]. Springer, 2021, 211–221. The host book title is missing. Chicago style requires it for a chapter/contribution in an edited volume.
3. Pathak, Y., et al. "Feature Selection for Image Steganalysis Using Levy Flight-Based Grey Wolf Optimization." Multimedia Tools and Applications 78 (2019): 1473–1494.
4. Elhoseny, M., and K. Shankar. "Optimal Bilateral Filter and Convolutional Neural Network Based Denoising of Medical Images." Measurement 143 (2019): 125–135.
5. Qin, J., et al. "An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing." IEEE Access 7 (2019): 24626–24633.
6. Uddin, M., et al. "Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records." Computers, Materials and Continua 68 (2021): 2377–2397.
7. Shankar, K., and S. K. Lakshmanaprabu. "Optimal Key Based Homomorphic Encryption for Color Image Security." International Journal of Engineering and Technology 7 (2018): 22–27.
8. Qureshi, M. B., et al. "Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud." Symmetry 14 (2022): 695.
9. Hussain, S., et al. "A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks." Sensors 22 (2022): 1072.
10. Hussain, S., et al. "Cryptanalysis of an Online/Offline Certificateless Signature Scheme for Internet of Health Things." Intelligent Automation and Soft Computing 30 (2021): 983–993.
11. Reegu, F. A., et al. "Interoperability Requirements for Blockchain-Enabled Electronic Health Records." Security and Communication Networks 2022 (2022): 9227343.
12. Mou, J., et al. "Image Compression and Encryption Based on Hyper-Chaotic Map." Mobile Networks and Applications 26 (2021): 1849–1861.
13. Hameed, A. Z., W. K. Awad, N. A. Irsan, and A. S. Abdulbaqi. "Hybrid Technique for Skin Pimples Image Detection and Classification." International Journal of Horticultural Science and Technology 29 (2020): 4102–4109. ⚠ Please verify the journal title. A paper on skin image classification appearing in a horticultural journal is highly unusual and may be a metadata or citation error.
14. Shen, Y., et al. "Optical Selective Encryption Based on FRFCM and Face Biometric for Medical Images." Optics and Laser Technology 138 (2021): 106911.
15. Alassaf, N., et al. "Enhancing Speed of SIMON: A Light-Weight Cryptographic Algorithm for IoT." Multimedia Tools and Applications 78 (2019): 32633–32657.
16. Shehab, A., et al. "Secure and Robust Fragile Watermarking Scheme for Medical Images." IEEE Access 6 (2018): 10269–10278.
17. Shen, M., et al. "Privacy-Preserving Image Retrieval for Medical IoT: A Blockchain Approach." IEEE Network 33 (2019): 27–33.
18. Laskar, S. A., and K. Hemachandran. "High Capacity Data Hiding Using LSB Steganography and Encryption." International Journal of Database Management Systems 4, no. 6 (2012): 57.
19. Yu, L., et al. "The Application of Hybrid Encryption Algorithm in Software Security." In Proceedings of the 4th International Conference on Computational Intelligence and Communication Networks (CICN), 762–765. 2012.
20. Mare, S. F., et al. "Secret Data Communication Using Steganography, AES and RSA." In Proceedings of the IEEE International Symposium on IT in Medicine and Education (SIITME), 339–344. 2011.
21. Mandal, A. K., et al. "Performance Evaluation of Cryptographic Algorithms: DES and AES." In Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 1–5. 2012.
22. Mjolsnes, S. F. A Multidisciplinary Introduction to Information Security. Boca Raton: CRC Press, 2011.
23. Rivest, R. L., A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM 21, no. 2 (1978): 120–126.

24. Sreekutty, M. S., and P. S. Baiju. "Security Enhancement in Image Steganography for Medical Integrity Verification." In Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), 1–5. 2017.
25. Bashir, A., et al. "A New Image Encryption Approach Using Shifting Technique and AES." International Journal of Computer Applications 42, no. 9 (2012): 38–45.
26. Muhammad, K., et al. "A Secure Method for Color Image Steganography Using Gray-Level Modification and Multi-Level Encryption." KSII Transactions on Internet and Information Systems 9, no. 5 (2015): 1938–1962.
27. Seyyedi, S. A., et al. "A Secure Steganography Method Based on Integer Lifting Wavelet Transform." IJ Network Security 18, no. 1 (2016): 124–132.
28. Khalil, M. I. "Medical Image Steganography: Study of Quality Degradation When Embedding Data in Frequency Domain." International Journal of Computer Network and Information Security 9, no. 2 (2017): 22.