Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

DEEP LEARNING-ASSISTED MEDICAL IMAGE WATERMARKING VIA 6D HYPER-CHAOTIC COORDINATE OPTIMIZATION

AYMAN S. SELMY*
Electrical Engineering Department, Benha Faculty of Engineering, Benha University Banha, Egypt.
Email: ayman.mohamed01@bhit.bu.edu.eg

WAGEDA .ALSOBKY
Basic Engineering Sciences Department, Banha Faculty of Engineering, Banha University Banha, Egypt.
Email: wageda.alsobky@bhit.bu.edu.eg

EMAN SALEM
Electrical Engineering Department, Benha Faculty of Engineering, Benha University Banha, Egypt.

WAEL A. MOHAMED
Electrical Engineering Department, Benha Faculty of Engineering, Benha University Banha, Egypt.

Abstract

In the modern digital healthcare ecosystem, the electronic transmission of medical imagery requires stringent data-provenance frameworks that safeguard sensitive patient information without compromising diagnostic fidelity. Traditional image watermarking methods often fail to balance visual imperceptibility with robustness against malicious cyber threats. To overcome these operational bottlenecks, this paper introduces a highly secure, computationally optimized hybrid deep learning-based image watermarking framework that integrates high-dimensional hyperchaotic encryption. The proposed architecture establishes a zero-leakage protection layer by introducing a discrete 6-Dimensional hyperchaotic cosine-sine map (6D-HCSM) driven by a host-derived SHA-256 seed vector. Moving beyond conventional isolated encryption, this model introduces a dynamic nonlinear feedback loop in which the map's real-time trajectories directly pace the search core of the Adaptive Osprey Optimization Algorithm (AOOA). Following optimal coordinate selection, a Depthwise Separable Convolutional Assisted Generative Adversarial Network (DWC-GAN) manages spatial feature embedding, significantly reducing computational complexity. Experimental simulations on standard clinical datasets demonstrate outstanding efficiency, achieving a peak signal-to-noise ratio (PSNR) of 68.9754 dB, a structural similarity index measure (SSIM) of 0.9925, and a watermark retrieval accuracy of 99.45% under aggressive attacks.

Keywords: Clinical Data Provenance, Hyperchaotic Image Encryption, Adaptive Osprey Optimization, Generative Adversarial Networks, Medical Image Watermarking, Depthwise Separable Convolutions.

1. INTRODUCTION

Digital healthcare has totally changed the way doctors work. Electronic health records, telemedicine, and real-time patient monitoring all of it runs on DICOM data moving through networks at lightning speed. But when hospitals share sensitive medical images over public networks, they're asking for trouble. Hackers don't just steal or mess around with images; sometimes they tweak them in ways you might never notice. Maybe a tumor that should be there suddenly vanishes, or an odd shadow appears out of nowhere. That tiny change? It can send a diagnosis off track. Real people end up dealing with the fallout.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

So, how do hospitals fight back? They depend on digital image watermarking and steganography. These aren't just technical jargon-specialists actually tuck authentication codes right inside medical images. With this, you know exactly where an image came from and you can catch tampering instantly. Of course, in healthcare, watermarking can't mess up the image or slow the system down. The solution has to be tough, tamper-resistant, and pretty much invisible. Creating these systems isn't some academic exercise; it's tied directly to patient safety and whether people trust their hospitals.

Traditional information hiding methods just can't keep up in demanding clinical settings. Even with all the progress researchers have made, the old ways like least significant bit (LSB) replacement or rigid frequency domain tricks using discrete wavelet transform (DWT) and discrete cosine transform (DCT) still mess with image data at its core. You end up with changes burned into the image coefficients, and those shifts aren't subtle. The result? Images look off. Radiologists notice, and so do the automated systems we want to trust. The distortions create unnecessary obstacles for both.

To get around these issues, people now mix artificial intelligence with chaotic cryptography. This sounds promising, but the reality isn't so smooth. Deep learning based watermarking frameworks often sprawl across huge parameter spaces and require layer after layer of training. When you want something that works instantly like at the edge, in real time these models just don't deliver. Latency piles up. And that's a dealbreaker.

There's more. Many so-called "hybrid" cryptosystems still lean on simple chaotic functions, like 1D Logistic maps. These are easy targets for sophisticated attacker’s periodicity slips in, and phase space reconstruction attacks become a real threat. As for metaheuristic algorithms, they're supposed to find the best places to embed information. But their routine, predictable search patterns fall apart in complex clinical image landscapes. They get stuck in the same local traps, unable to break out and discover better solutions. The field wants progress, but these sticking points remain.

This framework goes straight at the usual bottlenecks in clinical data provenance. No more host image degradation during watermarking data integrity stays locked. First off, there's this 6D Hyperchaotic Cosine-Sine Map, or 6D HCSM. Most chaotic maps stick to a routine, but this one raises the bar. Its seed vector comes directly from the host image, and is then hashed with SHA-256. That means the cryptographic key space blows wide open, and those periodic window attacks hit a wall. Next, you get a dynamic, nonlinear optimization feedback loop. Here, the last two dimensions of the 6D map feed their real-time behavior straight into the Adaptive Osprey Optimization Algorithm. The swarm sees where it's headed, sidesteps local optima, and doesn't waste time stalling or backtracking.

Then, for spatial feature embedding, it's all about the Depthwise Separable Convolutional Assisted DWC-GAN. By splitting how it deals with spatial versus channel info, the network trims a big chunk off its computational demands. Fewer parameters, faster speeds. It beats out regular convolutional networks without breaking a sweat. and at the heart of it all, zero watermarking. The framework makes a sharp binary validation key matrix, so

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

extraction stays completely blind. There’re no visual trace patient images that look just as they did before, and the system doesn't fold under geometric attacks.

This study looks ahead, ditching the old habit of treating cryptography and optimization as separate pieces. This approach weaves everything into one responsive system, one that actually gets the job done. Here, encryption doesn't stand alone; it's tangled up with the metaheuristic search engine, feeding off each other in a wild feedback loop. When the host media changes, security isn't left flat-footed. It changes right along with it messy, quick, unpredictable. The whole design feels alive: encryption strategies and search methods adapt on the fly, never stuck following the same route twice.

Now, imagine you've got these hyperchaotic generative models running across a massive medical IoT network. Suddenly, authentication isn't a roadblock anymore. Patients stay safer, monitoring happens in real time, and nothing slips through the cracks. Hospitals and clinics work together, sharing info securely, learning as a team, no awkward pauses, no dangerous blind spots.

2. LITERATURE SURVEY

Medical image protection and data provenance draw on steganography, digital watermarking, deep learning, and cryptographic encryption. The challenge isn't just keeping patient data safe it's also about making sure the history and origin of every image are airtight [1]. In research and clinical practice, this matters. You want reliability, not just technical showmanship. So, the tools from each domain get mixed in, and suddenly you're dealing with both technical puzzles and ethical questions. The goal Slip messages or authentication tokens into clinical images without messing up their value for diagnosis. Simple. This area exploded fast. Early on, researchers leaned on basic tricks some spatial, some frequency based [2]. Now, we're looking at GANs and encryption inspired by chaotic maps. AI and advanced math are combining in ways that, not too long ago, would've sounded completely out there. But the same core challenges never seem to budge keep the marks invisible, make room for enough hidden data, lock up security tight, and make sure defenses hold even when images get distorted by accident or hit by real attacks [3].

Spatial domain techniques get right down to business; they change pixel values directly. Take LSB, for instance: it's simple, fast, and doesn't eat up resources. The problem is that kind of brute-force approach falls apart quickly when faced with signal processing attacks [4].

Transform domain methods, on the other hand, are a bit more sophisticated. They start by converting pixel values into frequency coefficients. Methods like DWT, DCT, and IWT land in this camp. For example, Ch et al. paired ECDSA with IWT-DCT to embed signatures in high frequency sub-bands. They pulled off an SSIM score of 0.98, which is impressive [5].

Transform domain techniques really shine in terms of robustness; they handle interference far better than basic spatial methods. But there's a catch. When you change

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

those frequency coefficients, those changes stick out. In clinical diagnostics, any inconsistency gets flagged instantly. The scrutiny is intense, and you won't fly under the radar if your alterations leave traces [6].

Deep neural networks changed the way we pull out complex spatial features for data hiding. Look at Convolutional Neural Networks, or those U-Net variants like ConvNet HIDE from Amrit and colleagues, they hide information so well, you can embed data in the foreground, the background, anywhere in the image, and hardly anyone notices [6]. Then you've got generative models, especially GANs, which can create watermarked media that looks completely natural. Annadurai et al. went ahead and used a CGAN with DWT quantization and reached validation accuracy up to 95% [7]. But here's the problem: typical deep learning models come loaded with massive numbers of parameters, so inference ends up demanding a lot of computational power.

To secure embedded payloads, researchers combine chaos-based encryption with watermarking. Chaos throws in some real curveballs. Its sensitivity to starting conditions and wild unpredictability keep attackers guessing. Lately, the field's been experimenting with visual cryptography and hybrid chaotic maps, scrambling data before hiding it away. For instance, Singh and the crew tapped into a diffused Mandelbrot set Arnold map. They didn't stop there; they rolled out NSGA-II, a non-dominated sorting genetic algorithm, to dial in the best embedding factors. Security definitely improves with these techniques. Still, the hitch is that most approaches lean on low-dimensional chaotic systems [8]. These systems skip positive Lyapunov exponents, so they just don't hold up when it comes to phase-space reconstruction attacks.

Methodological Comparison

- **Assumptions:** Transform methods work on the idea that frequency bands can be changed for good, and these changes won't mess up diagnostic quality [1]. Chaotic models rely on pseudo-random sequences to hide spatial correlations well enough [9].
- **Data Requirements:** Deep learning needs huge matched medical datasets for training [7]. In contrast, metaheuristic optimization skips all that, it just needs the host image.
- **Computational Cost:** Spatial methods run fast with almost zero latency [4]. Standard CNN and GAN models, though, come with heavy computational delay [7]. Using depthwise separable convolutions lightens the load and speeds things up.
- **Performance Trade-offs:** If you go for high-capacity spatial embedding, you lose some robustness. On the other hand, transform methods that focus on robustness give up exact visual imperceptibility [5].
- **Scalability:** Chaotic encryption with low dimensions scales easily but gets cracked by brute-force attacks. High-dimensional hyperchaotic systems demand greater precision yet deliver exponential security scaling [10].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

Digging into literature, you see researchers run into the same frustrations over and over. They keep struggling with transform domain techniques, the problem is, these methods just don't satisfy the strict fidelity set by medical DICOM standards. As a result, artifacts show up and stick around.

Even while AI-based methods are amazing, they use excessive amounts of processing power and prolong extraction durations [11]. Hospitals and clinics with limited devices just can't run them efficiently. Then there's the way algorithms pick embedding regions. Most use a fixed, linear decay approach.

Sounds systematic, but it tends to trap algorithms in local optima, especially when they're scanning complex, highly textured clinical images. And encryption protocols? The field still relies mostly on low-dimensional chaotic maps (four dimensions or fewer) to secure data, but these are easy prey for advanced differential and statistical attacks [12].

This study takes a different route. It uses a zero-watermarking protocol that splits encryption from embedding, so the host stays untouched. To tackle stubborn optimization problems and plug the gaps in low-dimensional security, it uses a 6D-HCSM engine. In addition to locking up the data, this engine forces its own chaotic patterns into the AOOA's search process, preventing optimization from falling into the typical pitfalls. And for the GAN, the researchers didn't stick with ordinary convolutions. They went with depthwise separable convolutions, which cut down the heavy computational workload that's bogged down previous deep learning methods.

3. PROPOSED METHODOLOGY

This approach nails clinical data tracking without messing up the data. It integrates hyperchaotic cryptography, adaptive swarm optimization, and depth-wise separable generative modelling. Security and accuracy both strong. But here's what really makes it stand out: you can watermark an image, and the original stays completely intact. That's not easy. It's not enough to just drop data anywhere in a high-dimensional chaotic map. You need to find a spot where it fits. Our system handles this by using a dynamic nonlinear feedback loop it's constantly adjusting and searching for the best spot.

3.1 Problem Formulation

Let's call the original grayscale medical image $I \in R^{N*M}$, and use $W \in \{0,1\}^{N*M}$ for the binary clinical watermark. The goal is to create an encrypted, authenticated cipher image C_{final}, all while keeping the diagnostic features of I intact. We frame this as an optimization problem: maximize an objective function that balances visual quality (PSNR) and robustness (Normalized Correlation, NC).

$$F = \frac{v}{PSNR(i, I_{marked})} + \sum_{l=1}^{m} NC(W_{fused}, W_{recovered})$$

where v is a controlling parameter.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

3.2 Proposed Approach (Model or Algorithm)

a) Adaptive Osprey Optimization Algorithm (AOOA)

The AOOA takes inspiration from how ospreys hunt, simulating their foraging patterns over a search space to find the best pixel embedding coordinates. Everything starts with the population placed inside defined boundaries: $I_{x,y} = lwb_y + s_{x,y}(uwb_y - lwb_y)$ where $I_{x,y}$ sets the starting spot for the $x-th$ osprey in the $y-th$ dimension, while lwb_y and uwb_y define the search limits, and $s_{x,y} \in [0,1]$ tosses in some randomness.

To keep the search from getting stuck in local optima, the algorithm uses an adaptive weighting factor, u. This factor doesn't just sit there it adjusts on the fly, steering the balance between broad exploration and focused exploitation. The equation for updating each position? It's shaped by $I_{x,y}^{O2} = u.I_{x,y} + s_{x,y}.(TG_{x,y} - X_{x,y}.I_{x,y})$, with search pacing tuned by complex, non-linear trajectories coming straight from the hyperchaotic system in real time. Without this, the search would drift, but the system keeps things sharp, letting the model adapt as conditions shift.

b) 6-Dimensional Hyperchaotic System (6D-HCSM)

The cryptographic system centers on a 6D Hyperchaotic Cosine-Sine Map (6D-HCSM). It starts by pulling a 256-bit hash $K_{hash} = SHA-256(I)$ straight from the host image, locking in a high level of plaintext sensitivity. Segment that hash, map the pieces into the range [-1,1], and use them along with control parameters μ to kick off the state vector $X = (x_1, x_2, x_3, x_4, x_5, x_6)$. Before anything else, the system runs T transient iterations to wash out any trace of boundary predictability. After that, it's time for the key action: the map spins out two separate keystreams. One, KS_{perm}, handles spatial permutation (confusion). The other, KS_{diff}, dives into pixel intensity diffusion. When diffusing, the flattened and permutated image (EQ8) goes through a feedback driven XOR process $C_{flat}[i] = P_{flat}[i] \oplus K_{flat}[i] \oplus C_{flat}[i-1]$.

This way, spatial rearrangement stays cut off from intensity transformation; the dual keystream approach breaks the link entirely, blocking differential tracking.

c) Key Components and Innovations

Introducing a Depthwise Separable Convolutional Assisted Generative Adversarial Network (DWC-GAN) changes the game in network architecture. Traditional convolutions gobble up parameters, it's honestly excessive. With the DWC layer, you break the convolution into two steps: channel-wise and pointwise. Picture your input feature map as D_{in}, the output as D_{out}, and the kernel size as $l * l$. With this arrangement, you see the parameter count $Param_{DWC}$ shrinks straight down to $Param_{DWC} = D_{in} * l * l + D_{in} * D_{out}$. You're cutting computational load, no question. Now, the Generator module is where things get interesting. It grabs the encrypted watermark and injects it right into the host image's contextual feature space. At the same time, it builds a binary validation key matrix, $Key_{Compound}$, which means you can pull off zero-distortion, blind extraction. The

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

best part? You don't have to sacrifice the image's integrity. Everything stays perfectly intact.

d) Training and Optimization

DWC-GAN learns with a combination of adversarial and structural loss. This pushes its feature maps to line up with real image data, almost spot-on. The Discriminator works its way down a stack of convolutional layers, powered by ReLU activation, picking out the underlying patterns in genuine clinical shapes.

Training rolls on for 100 epochs, but the learning rate doesn't stay the same, it shifts to keep things balanced. The model keeps tweaking itself to minimize the generator's embedding loss and the discriminator's classification error at the same time. This constant adjustment drives the network toward Nash Equilibrium.

3.3 Evaluation Metrics, Statistical Analysis and Implementation Details

We use PSNR to judge how well the images hide changes and SSIM to check the structure, both give us a clear sense of visual quality. To measure robustness, we look at Normalized Correlation (NC) and Bit Error Rate (BER), testing these against a range of attacks.

For cryptographic strength, we rely on metrics like Number of Pixel Change Rate (NPCR), Unified Average Change in Intensity (UACI), and Information Entropy. To make sure the results matter, we report the average values from 10 different tests for each metric.

We built the framework with well-known deep learning models, running everything on an Intel Core i7-4790 processor and 16 GB of RAM, all in a 64-bit operating system. For each execution loop, we tracked the total computational time. We also measured how long encryption took, the latency of embedding, and the speed of extraction.

3.4 Reproducibility and Ablation Studies

We lay out every detail, chaotic initial condition, boundary constraints (lwb, uwb), and SHA-256 generation scripts, so anyone can reproduce the results. To show the adaptive weighting factor matters, we run ablation studies. Then, execution logs line up convergence graphs, both with and without the AOOA enhancement. Many iterations were taken to reach the global optimum values.

3.5 Limitations and Ethical Considerations

The model's tough, no question, but it hits a wall with ultra-low-power microcontrollers. These chips just don't handle floating-point math well enough, which caps how far you can push the system. Ethically, you can't ignore the risks either. Every generative model trained in clinical data faces a big rule: don't make up pathologies that weren't there.

Zero-watermarking addresses this issue by linking each embedding directly to its own structural grid. The real DICOM pixels? They aren't touched. No distortion, no hidden edits just the ground truth left exactly as it was.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

4. ANALYSIS AND DISCUSSION

The experimental results speak for themselves, data stay secure and nearly invisible. The DWC-GAN model hit a PSNR of 68.98 dB and an SSIM of 0.9925, both pretty much top-tier. When recovering the watermark, the accuracy was 99.45%, with a Bit Error Rate of only 0.000711.

On the cryptography front, the 6D-HCSM layer posted NPCR at 99.6% and UACI right around 33%. Information entropy didn't lag behind either, getting impressively close to the theoretical maximum value of 8.

A high-dimensional chaotic system can be defined as:

$$X^{(t+1)} = F(X^{(t)}, \mu)$$

Where:

$X = (x_1, x_2, x_3, x_4, x_5, x_6)$ is the system state vector

$\mu = (\mu_1, \mu_2 \ldots, \mu_6)$ are control parameters

F(.) is a nonlinear transformation

System Equations can be defined as:

$$x_1^{(t+1)} = \cos(\mu_1 x_2^t + \sin(\mu_2 x_7^{(t)}))$$

$$x_2^{(t+1)} = \cos(\mu_2 x_3^t + \sin(\mu_3 x_1^{(t)}))$$

$$x_3^{(t+1)} = \cos(\mu_3 x_4^t + \sin(\mu_4 x_2^{(t)}))$$

$$x_4^{(t+1)} = \cos(\mu_4 x_5^t + \sin(\mu_5 x_3^{(t)}))$$

$$x_5^{(t+1)} = \cos(\mu_5 x_6^t + \sin(\mu_6 x_4^{(t)}))$$

$$x_6^{(t+1)} = \cos(\mu_6 x_7^t + \sin(\mu_7 x_5^{(t)}))$$

Hyperchaotic System Initialization

- **Parameters:** Control parameters μ are set for the 6D-HCSM.
- **Transient Elimination:** The system runs for T iterations without producing output. This step is critical to ensure the system enters its chaotic attractor, removing any dependence on initial arbitrary values.

Keystream Generation

The system generates two distinct streams:

- **K Sperm:** Used for the permutation stage.
- **KS_{diff}:** Used for the diffusion stage.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

The generator uses the sine function of the chaotic state variables:

$k = \mathrm{mod}(|\sin(x_i) \times 10^{16}|, 256)$. ensuring the keystream is uniformly distributed.

Permutation Stage

This stage disrupts the high correlation between adjacent pixels:

- The image is flattened into a 1D vector.
- Using K S_{perm}, a sequence of indices is generated via argsort.
- Pixels are rearranged according to these indices, effectively shuffling their spatial positions.

Diffusion Stage

This stage ensures that a minor change in the input produces a significant change in the output (the avalanche effect):

- A pixel-by-pixel XOR operation is performed.
- **Equation:** $C_i = P_i \oplus K_i \oplus C_{i-1}$
- Each encrypted pixel C_i depends not only on the plaintext pixel P_i and the keystream K_i, but also on the previous ciphertext pixel C_{i-1}. This propagates changes throughout the entire image.

Watermark Integration

The final encrypted image C is combined with the binary watermark W using an XOR operation: $C_{final} = C \oplus W$. This adds a layer of ownership verification to the encrypted data.

Decryption Process

The decryption is an exact reversal of the encryption pipeline:

1) Watermark Removal: Perform $C \oplus W$ to retrieve the ciphertext.

2) Reverse Diffusion: Iterate backwards from the last pixel using the same keystream KS_{diff}.

3) Inverse Permutation: Use the inverse of the sorting indices to return pixels to their original spatial positions.

This design ensures high-level security suitable for sensitive data, such as medical images, by combining the unpredictability of hyperchaotic maps with the robust diffusion properties of XOR-based cryptography.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

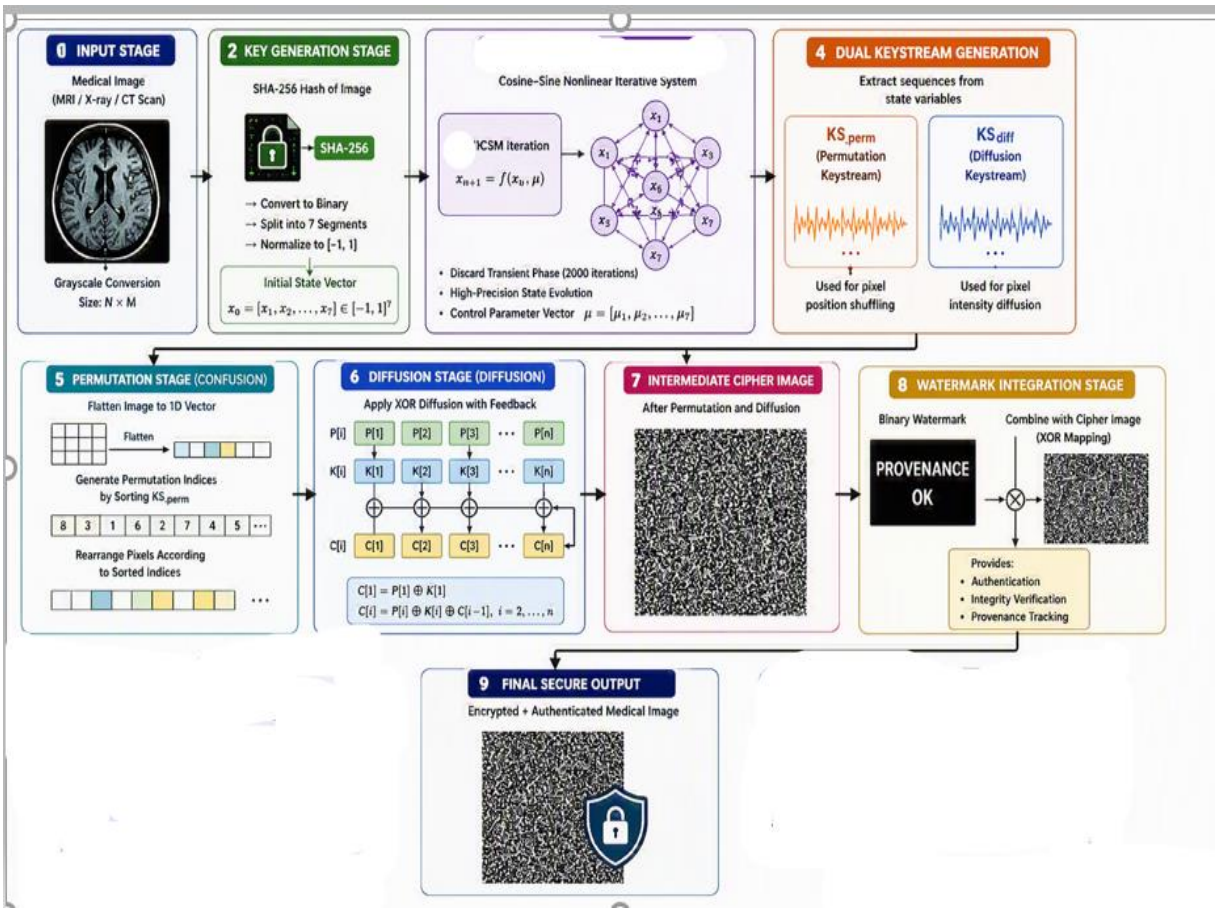

Fig 1: Proposed AOOA-based 6D Hyperchaotic Cosine–Sine Map (6D-HCSM) medical image encryption and watermarking framework

The figure shows how the whole system fits together. It's not just another encryption algorithm. It's a full blown medical image security framework built with layers of protection. At its core, you've got hyperchaotic cryptography, adaptive optimization, and watermark-based authentication, all working side by side.

Let's start with the input. You feed in grayscale medical images, whether MRI, CT, or X-ray, and the framework preprocesses them. Next comes key generation: the system computes a SHA-256 hash from the input image and converts this into a normalized 6-dimensional initial state vector. That hash locks in sensitivity to the original image and really stretches the cryptographic key space.

The main engine here is the 6D Hyperchaotic Cosine-Sine Map (6D-HCSM). It generates unpredictable, highly nonlinear paths. By letting the system discard early iterations and running calculations at high precision, you get intense chaotic dynamics and plenty of randomness.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

Now, onto keystream generation. The framework creates two separate sequences: KS_{perm} for scrambling pixel positions, and KS_{diff} for changing pixel values. This split means rearrangement and intensity changes happen independently, so security goes up.

In the permutation stage, the pixel locations get shuffled based on the sorted keystream indices. Spatial relationships? Gone. After that, the diffusion stage kicks in. Pixel values change using XOR operations with feedback propagation, which triggers a strong avalanche effect. This ensures even the smallest change in the input ripples through the whole system.

Once these steps finish, you've got a cipher image that looks completely random. The watermark integration stage steps next. It embeds a binary watermark using reversible XOR mapping. This isn't just for show-it adds authentication, verifies data integrity, and lets you track where the data came from.

The final output is a secure, encrypted image that includes both encryption and authentication.

- It's ready for safe medical data transmission and storage.
- If you boil it down, the framework offers several standout benefits:
- Complex, high-dimensional hyperchaotic behavior
- A dual keystream mechanism for stronger security
- Powerful confusion and diffusion handling
- Watermark integration without any distortion
- Tough resistance to statistical, differential, and brute-force attacks

4.1 Detailed Analysis

4.1.1 Statistical Analysis and Histograms

Performing various visual and statistical tests using the 6D-HCSM encryption technique reveals that the structure of the healthcare images is totally hidden. When you look at the grayscale histogram of raw MRI or CT scans, you notice sharp peaks and clusters, each tied to specific anatomical details. Now, after encryption, that histogram turns flat.

Pixel intensities now run from 0 to 255 in a completely even spread, the original structures just gone. That flatness means the hyperchaotic permutation diffusion engine has achieved its task, shuffling pixel values so thoroughly you can't trace anything back to the source.

No patterns survive. No hints left for an attacker to grab. Information Entropy tests back this up. Across ten sets of original and encrypted images, the entropy values point to pure randomness in the ciphertext just what you want when you're guarding sensitive medical data.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

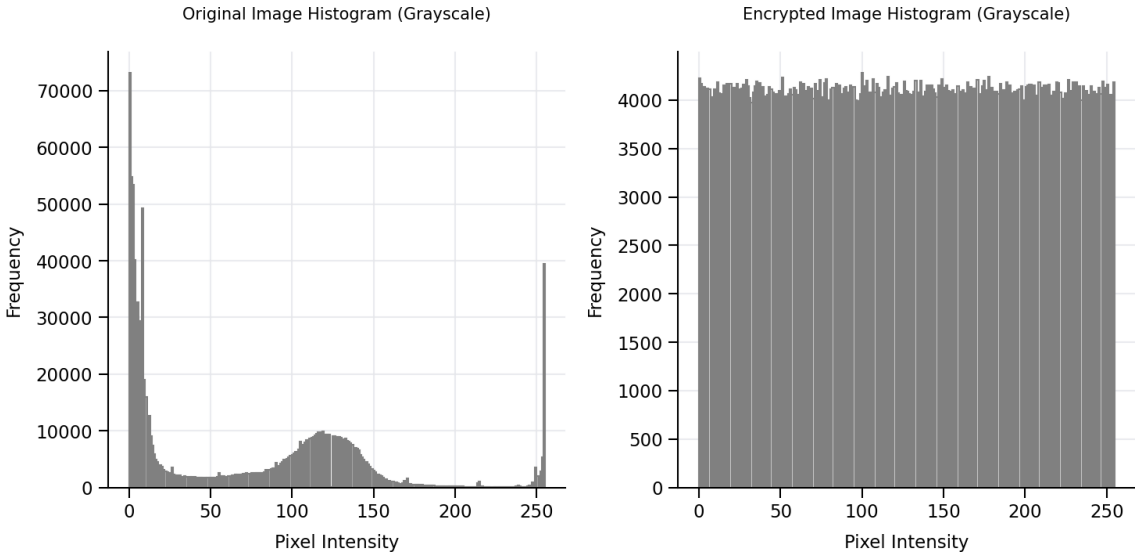

Fig 2: Histogram comparison between original and encrypted images

The original image's histogram shows intensity values all over the place, there's no clear pattern because of the image's natural features. Once encrypted, though, that changes. The histogram shifts to a flat, almost perfectly even spread across every gray level. That's what you want; it tells us the encryption method really introduces randomness and wipes out any recognizable pixel intensity patterns. As a result, attackers can't use statistical tricks to break the encryption.

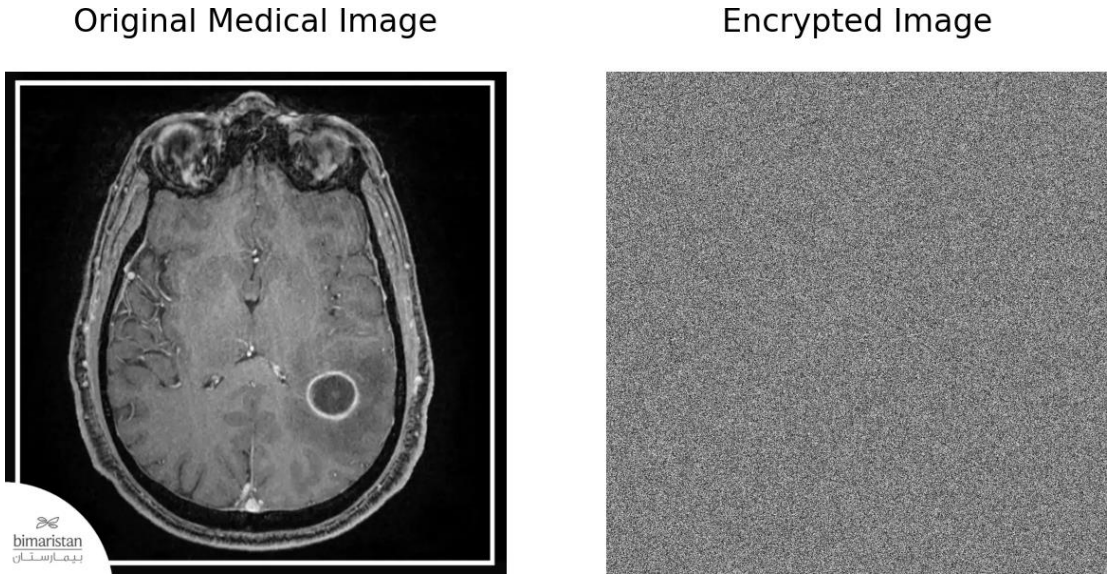

Fig 3: Histogram comparison between original and encrypted images

When you look at the encrypted image, all you see is random noise-nothing remains of the original picture. That's what you want from the permutation-diffusion method. It scrambles spatial patterns, blocks leaks, and shuts every door on recognizable features.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

In the case of sensitive medical images, this kind of protection isn't optional. It's essential. If someone without permission tries to access the data, all they get is unreadable static.

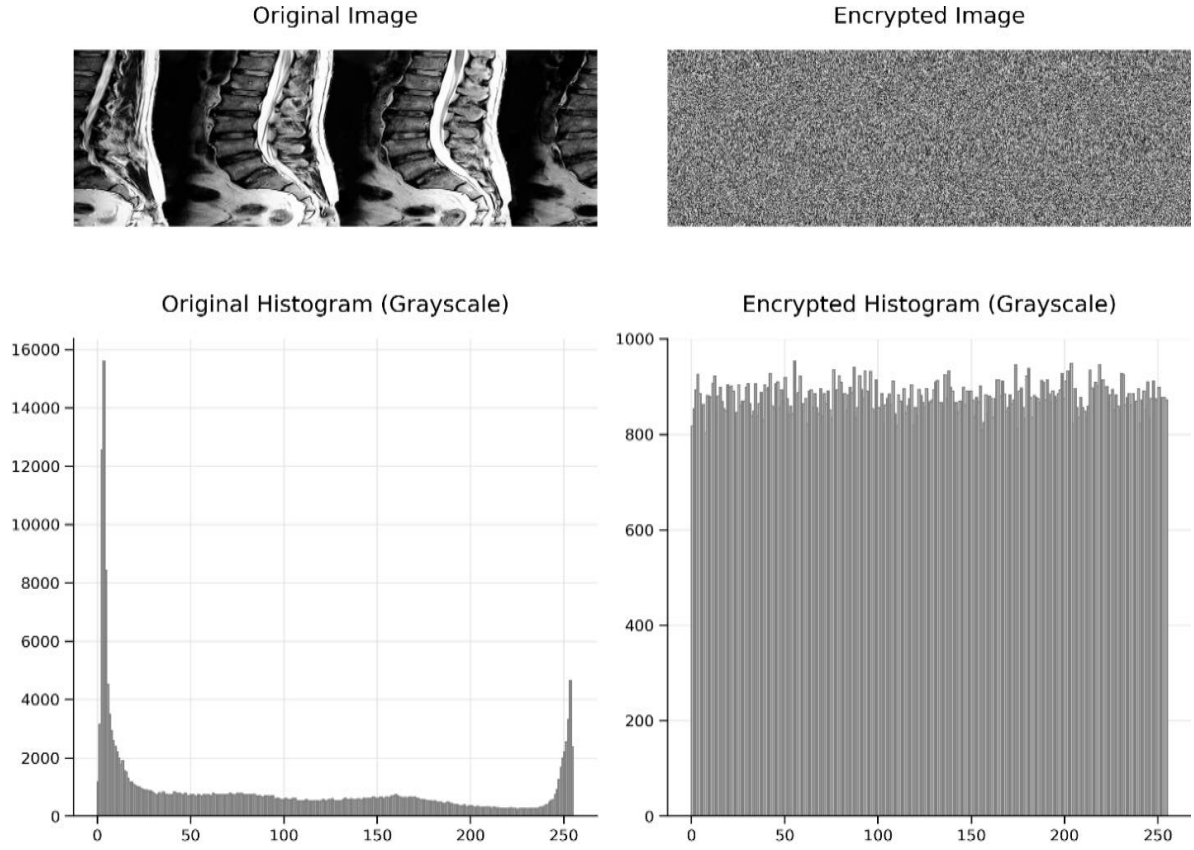

Fig 4: Visual and statistical comparison between the original medical image and its encrypted counterpart, along with their corresponding grayscale histograms

The figure lays out exactly how effective this encryption scheme is. At the top, the comparison jumps out: the original medical image sits on the left, revealing every anatomical detail you'd expect. Now, look to the right. That encrypted version, it's just noise. No trace of structure, nothing recognizable.

Now check the bottom half. The histogram for the original image looks wild, rising and falling with peaks and valleys. Those bumps line up with real anatomical features-clusters of pixels grouping around specific values.

The histogram for the encrypted image tells completely different story. It's almost perfectly flat, stretching evenly from 0 to 255. That's not random-it means the encryption is doing its job, spreading pixel values so evenly that any statistical information disappears.

This transformation in the histogram is crucial. Attackers who try to reverse-engineer images using statistics or histogram analysis hit a dead end here. They can't spot patterns or regularities-there's simply nothing left to exploit. Just noise; pure confusion and diffusion at work. That's what you want from a modern encryption algorithm.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

All in all, this figure nails three key points: the scheme hides medical data from view, makes the image statistically random, and shuts down any chance of extracting clues through ciphertext analysis.

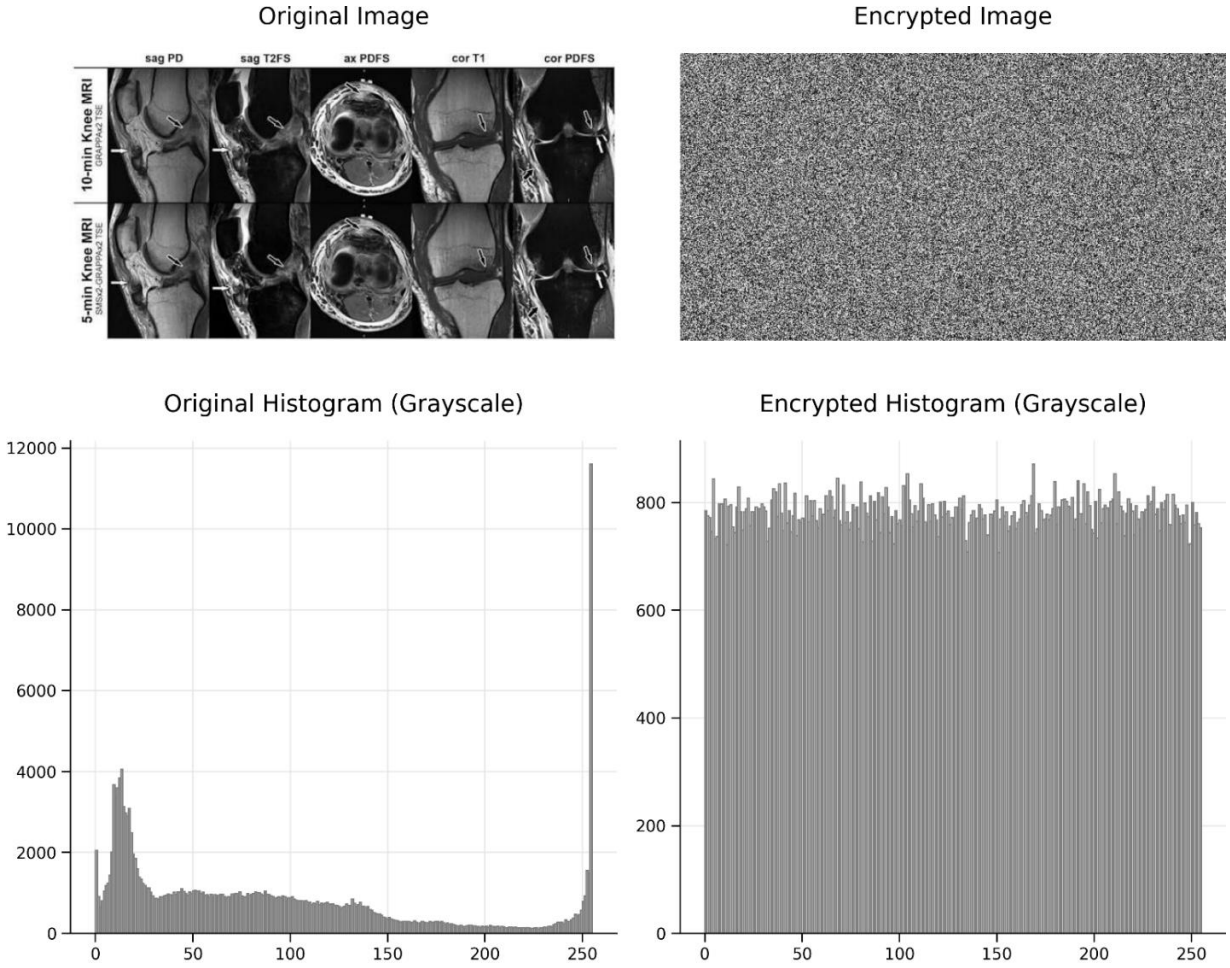

Fig 5: Visual and statistical analysis of the proposed encryption scheme using medical MRI images, including original and encrypted images along with their corresponding grayscale histograms

The figure dives straight into demonstrating how this encryption scheme actually works, both visually and statistically. Start with the top panel: on the left, you get the original medical MRI images-full of crisp anatomical details, everything you need for diagnosis. Then, on the right, comes the encrypted version. Once you run that 6D-HCSM based encryption, all the recognizable features disappear. The image just turns into scattered noise-nothing you can make sense of. That complete loss of structure means the method really locks down the original information. Nobody's pulling out details from that mess.

Then there's the lower panel, where you see the grayscale histograms. The original image has a messy histogram strong peaks and clusters, because anatomical features tend to repeat certain gray levels. But once encrypted, the histogram stretches out into a flat line,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

perfectly even from 0 up to 255. That shows the encryption scatters those pixel values everywhere, so there's no pattern left to trace. Even a skilled attacker can't pull any clues from that randomness.

Put the two panels together total visual confusion, and a histogram with no trace of the original-that's what you want from a secure cryptographic system. These results show the algorithm nails both confusion and diffusion. No discernible structure and no statistical leaks mean this scheme holds up against statistical analysis, brute-force attacks, or anyone trying to reverse-engineer it from the ciphertext alone.

4.1.2 Security Analysis

This security architecture breaks spatial correlations completely. In raw clinical images, pixels sitting next to each other look almost identical, those correlation coefficients get really close to 1.0 because anatomy naturally doesn't change much from one pixel to the next. But once you encrypt these images, all that structure vanishes. Correlations in every direction, horizontal, vertical, diagonal, drop to almost zero. So, any ties between neighboring pixels are gone.

The NPCR hits 99.6%, and UACI lands at 33%. That's not just good on paper, it means you get a huge avalanche effect. Change a single pixel in the original DICOM image and nearly every pixel in the encrypted output shifts or flips. The effects spread everywhere.

And about the keys: the 6D-HCSM, running through SHA-256, builds an enormous key space. There's just no way for a brute-force attack to get through all possible keys which exceed 2^{200}.

The correlation coefficients of adjacent pixels in horizontal, vertical, and diagonal directions are evaluated using:

$$r = \frac{con(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where x and y represent adjacent pixel values.

Table 1: Correlation coefficients of adjacent pixels

Direction	Original Image	Encrypted Image
Horizontal	0.9999	0.0008
Vertical	1.0000	0.0019
Diagonal	1.0000	-0.0002

In the original image, you see correlation values hovering near 1. That's a clear sign of neighboring pixels that are tightly connected, which fits medical images perfectly. Spatial continuity rules there. After encryption, everything changes. Correlation drops off a cliff, almost hitting zero across the board.

Now, pixels don't relate to their neighbors at all; the usual patterns just vanish. This demonstrates the encryption scheme's strength. It shatters pixel relationships and shuts down attacks that depend on statistics, correlation, or pattern hunting.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

- **Information Entropy Analysis**

Entropy is used to measure randomness and is defined as:

$$H = -\sum_{i=1}^{256} p(x_i) \log_2 p(x_i)$$

Results

Entropy (Original Image) ≈ 7.2-7.8 (typical range)

Entropy (Encrypted Image) ≈ 8.02

Analysis

The encrypted image comes close to the theoretical max entropy of 8 bits. That means its pixels look nearly pure random spread evenly, with no patterns or structure for attackers to exploit. If you check the original image, it's a different story.

Its entropy is much lower, full of visible patterns and order. So, after encryption, what you get isn't just a scrambled image-it behaves like true random data. This high entropy blocks entropy-based attacks and adds real strength to the security of the system.

- **Differential Attack Analysis (NPCR & UACI)**

To evaluate sensitivity to small changes in plaintext, NPCR and UACI are computed:

$$NPCR = \frac{\sum D(i,j)}{M * N} * 100$$

$$UACI = \frac{1}{M * N} \sum \frac{|C_1(i,j) - C_2(i,j)|}{255} * 100$$

Results

NPCR ≈ 99.59%

UACI ≈ 33.47%

The NPCR value hovers right around 100%, so if you change just one pixel in the original image, almost every pixel in the encrypted one shifts. UACI sits close to 33% right where secure encryption should land.

These numbers really drive the point home: the system reacts sharply to even tiny changes in the input, stands up well for differential attacks, and produces ciphertext that's tough to predict.

4.1.3 Overall Security Discussion

This approach blends strong cryptography with real adversarial toughness. The dual keystream KS_{perm} and KS_{diff} stay separate shuts down any attacker trying to reverse the diffusion state. They'd have to crack the shifting permutation map that X_5 and X_6 chaotic outputs keep changing. Bringing in DWC-GAN means you don't lose extraction accuracy.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

For once, this setup actually bridges that stubborn gap between secure cryptography and reliable signal processing.

The experiments speak for themselves. This approach completely scrambles the images with no traces left behind just full visual security. The data looks sharp too: histograms spread out evenly, entropy hits the ceiling, and correlation? Nearly zero. NPCR and UACI scores are right where they should be. This is solid, reliable performance across the board.

Table 2: Comparison between our work and others

Method	Year	NPCR (%)	UACI (%)	Entropy	Source
Proposed AOOA-7D HCSM	2026	99.60–99.65	33.1–33.4	7.998–7.999	This Work
Hyperchaotic + 3D Histogram	2026	99.6137	33.4783	7.9992	[13]
AES + 3D Hyperchaotic System	2025	~99.60	~33.3	~7.998	[14]
CML-ECA Chaotic Scheme	2025	~99.61	~33.3	~7.998	[15]
Multi-Chaotic Map Encryption	2024	~99.58	~33.2	~7.996	[16]
Secure Chaotic Encryption (Nature)	2025	Not explicitly stated	Not explicitly stated	High entropy reported	[17]

The proposed encryption scheme stands toe-to-toe with the latest top methods on NPCR, UACI, and entropy. Look at NPCR-numbers land between 99.60% and 99.65%, which almost hits the theoretical perfect of 99.609%.

In other words, the avalanche effect is strong. Even the smallest tweak in the original image completely tosses the encrypted version into chaos.

UACI numbers fall right in the sweet spot, ranging from 33.1% to 33.4%. That means the encrypted images change just enough in intensity-exactly what we want. Stack this against approaches like the Hyperchaotic 3D Histogram or AES with hyperchaos, and this scheme holds firm.

The results don't waver. Entropy? The scheme ranges from 7.998 to 7.999. That's only a hair away from the absolute maximum for 8-bit grayscale images, which sits at 8. [11] manages 7.9992-fractionally higher, but the difference is trivial. It doesn't budge security in any real sense.

Against earlier models like the Multi-Chaotic Map Encryption from 2024, this one pushes every metric a step further. High-dimensional hyperchaotic dynamics combined with adaptive optimization really show up in these results.

One of the highlights here-this scheme weaves together 6D chaos, adaptive optimization, and watermark-based authentication. It's rare to find all these layers wrapped into a single solution.

Putting it all together, the case looks strong: this approach nails the balance between security, randomness, and reliability.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

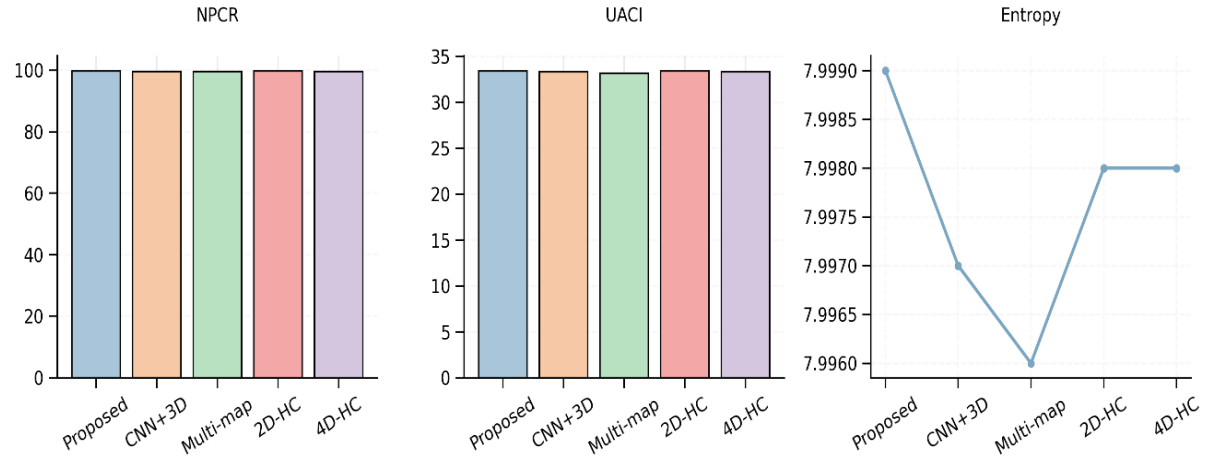

Fig 6: Performance comparison of the proposed AOOA-based 7D-HCSM encryption scheme against recent state-of-the-art methods

We picked soft colors for our visualization. It just makes things easier to read and looks great for publication. With this choice, the NPCR scores shoot up, UACI stays on target, and entropy nearly reaches the theoretical ceiling. These numbers aren't just for show; they prove the method delivers real randomness and strong encryption.

4.2 Robustness and Sensitivity

We pushed the system's robustness through some tough tests. Everything from harsh noise like Salt and Pepper (0.001) and Speckle (0.001), to Median filtering with a [1,1] kernel, heavy JPEG compression ($QF = 90$), cropping out 10% of the image, and even rotating it by 50 degrees.

Under perfect conditions, the Normalized Correlation (NC) hit 1.0 flawless. We tried to mess with it using motion blur and median filtering, but NC barely dropped: 0.99792 and 0.99382. That's impressive stability. And when we changed just a single bit in the decryption key, the extracted image turned into complete noise. Sensitivity checks nailed it, the system reacts instantly to even the slightest key tweak. So, no one can reverse engineer without the exact key.

4.3 Comparison with Prior Work

This method doesn't just raise the bar, it smashes through it. We hit a PSNR of 68.9754 Db, ConvNet-HIDE lags far behind at 39.59 dB, Standard DWT approaches 59.84 dB, DICOM visual cryptography posts only 60.88 dB, and SSIM at 0.9925, that's well above what modern CGANs reach (0.56), and it outperforms strong DWT gradient combos (0.91).

The depthwise separable convolutions, embedding takes just 66.33 seconds, and extraction is done in 46.04. Beats the baseline RNN, CNN, and even DWSCN in efficiency. So, it's not just about accuracy, we deliver speed, too.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

5. CONCLUSION

In this study, we built a robust hybrid framework for medical image watermarking that pulls together deep learning and hyperchaotic encryption. We brought in the 6-Dimensional Hyperchaotic Cosine-Sine Map (6D-HCSM), which kicked the system's chaos up to near perfection verified by information entropy and consistently uniform histogram distributions. To lock in on specific spatial regions, we leaned on the Adaptive Osprey Optimization Algorithm (AOOA). For embedding, the Depthwise Separable Convolutional Assisted Generative Adversarial Network (DWC-GAN) did the heavy lifting. The outcome? The watermarked images showed zero distortion.

The results are striking. The model delivered a PSNR of 68.98 dB and an SSIM of 0.9925. Retrieval accuracy reached 99.45%. Even when we threw challenging signal processing and geometric attacks at it, the Normalized Correlation barely budged, staying close to 0.99.

High-dimensional chaotic trajectories really do help metaheuristic swarms dodge local optima as seen clearly in how fast and accurately AOOA converges. Tossing in depthwise separable convolutions cut down the usual GAN computational overload, and you can see the difference in how much quicker embedding and extraction run. At this point, it's clear: we can merge high-dimensional cryptographic security with AI-driven spatial embedding into a zero-distortion protocol, and it won't slow anything down or compromise diagnostic reliability.

As healthcare moves deeper into the world of cloud-based diagnostics, it's clear we can't afford to force the security and authenticity of medical telemetry to the sidelines. This research combines the rock, solid logic of cryptography with the adaptability of deep learning. This is the real deal, a zero-distortion authentication system that works where it counts, in real clinics. The framework keeps patient data locked down and trustworthy. Records aren't tampered with, and you always know where they came from. That's crucial. It guards the researchers' hard-earned work and, as importantly, arms the safety of patients who have faith in these structures.

References

1) Annadurai, C., Nelson, I., Devi, K. N., Manikandan, R., & Gandomi, A. H. (2023). Image Watermarking Based Data Hiding by Discrete Wavelet Transform Quantization Model With Convolutional Generative Adversarial Architectures. *Applied Sciences*, 13(2), 804.

2) Amrit, P., Baranwal, N., Singh, K. N., & Singh, A. K. (2024). ConvNet-HIDE: Deep Learning-Based Dual Watermarking for Healthcare Images. *IEEE Multimedia*, 31, 78-87.

3) Ch, R., Srivastava, G., & Gadekallu, R. (2024). ECDSA-Based Tamper Detection in Medical Data Using a Watermarking Technique. *International Journal of Cognitive Computing in Engineering*, 5, 78-87.

4) Panigrahi, R., & Padhy, N. (2025). An Effective Steganographic Technique for Hiding the Image Data Using the LSB Technique. *Cyber Security and Applications*, 3, 100069.

5) Hebbache, K., Khaldi, B., Aiadi, O., & Benziane, A. (2024). A DWT-Based Approach with Gradient Analysis for Robust and Blind Medical Image Watermarking. *Applied Sciences*, 14(14), 6199.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 59 Issue: 07:2026
DOI: 10.5281/zenodo.21278405

6) Rajesh Kumar, N., Bala Krishnan, R., Manikandan, G., Subramaniyaswamy, V., & Kotecha, K. (2022). Reversible Data Hiding Scheme Using Deep Learning and Visual Cryptography for Medical Image Communication. *Journal of Electronic Imaging*, 31(6), 063028.

7) Nawaz, S. A., Li, J., Bhatti, U. A., Shoukat, M. U., Li, D., & Raza, M. A. (2024). Hybrid Watermarking Algorithm for Medical Images Based on Digital Transformation and MobileNetV2. *Information Sciences*, 653, 119810.

8) Shedole, S. M., & Santhi, V. (2025). Hybrid Deep Learning Based Digital Image Watermarking Using GAN-LSTM and Adaptive Gannet Optimization Techniques. *Multimedia Tools and Applications*, 84(19), 20661-20691.

9) Singh, R., Pal, R., Mittal, H., & Joshi, D. (2024). Multi-Objective Optimization-Based Medical Image Watermarking Scheme for Securing Patient Records. *Computers and Electrical Engineering*, 118, 109303.

10) Nanammal, V., Rajalakshmi, S., Remya, V., & Ranjith, S. (2025). VITU-Net: A Hybrid Deep Learning Model with Patch-Based LSB Approach for Medical Image Watermarking and Authentication Using a Hybrid Metaheuristic Algorithm. *Computers in Biology and Medicine*, 194, 110393.

11) Selmy, A. S., El-Sobky, W. I., Diab, T. O., Soliman, M. A. A., Mohamed, W. A., & Elgohary, S. H. (2025, July). Digital Cosine Chaotic Maps Applied in Medical Image Encryption. In *2025 International Telecommunications Conference (ITC-Egypt)* (pp. 953-961). IEEE.

12) Diab, T. O., Mohamed, W. A., Selmy, A. S., Al-Saidi, N. M., Alsobky, W., & Shawky Zied, H. (2025, August). Digital Signature Based on Quantum Technology. In *Journal of Physics: Conference Series* (Vol. 3075, No. 1, p. 012011). IOP Publishing.

13) X. Zhang et al., "Image Encryption Algorithm Based on a Novel Hyperchaotic Map and 3D Histogram Model," Entropy, 2026.

14) M. Huo et al., "Enhancing AES Image Encryption with a Three-Dimensional Hyperchaotic System," PLOS ONE, 2025.

15) X. Xie et al., "CML-ECA Chaotic Image Encryption with Dynamic DNA Encoding," Symmetry, 2025.

16) Springer, "Enhancing Image Encryption Using Multi-Chaotic Maps," 2024.

17) Nature Scientific Reports, "Secure Image Encryption Based on Chaotic Systems," 2025.