



چارچوبی ترکیبی برای حفظ محرمانگی در یادگیری فدرال تصاویر پزشکی با استفاده از سیستم‌های فوق آشوبی و ماسک‌سازی مربع جادویی

ناهید ابراهیمی زاده

دانشجوی دکتری مهندسی کامپیوتر دانشگاه آزاد اسلامی گرگان، گرگان، ایران.

nahid.ebrahimizade@gmail.com

چکیده

یادگیری فدرال به عنوان یک رویکرد غیرمتمرکز، امکان آموزش مشارکتی مدل‌ها را بدون اشتراک‌گذاری داده‌های خام فراهم می‌کند. با این حال، پژوهش‌های اخیر نشان داده‌اند که گرادیان‌های مدل نیز می‌توانند اطلاعات حساسی را فاش کنند و سیستم را در برابر حملات استنتاجی آسیب‌پذیر سازند. این چالش در حوزه تصاویر پزشکی که داده‌ها ذاتاً حساس و تحت قوانین سخت‌گیرانه‌ای مانند HIPAA و GDPR محافظت می‌شوند، جدی‌تر می‌شود. در این پژوهش، چارچوبی نوین به نام Fed-MS-Crypt (Federated Magic Square Cryptography) ارائه می‌شود که برای اولین بار، سیستم‌های فوق آشوبی، جعبه‌های جایگزینی پویا، مربع جادویی و قضیه باقیمانده چینی را در یک معماری یادگیری فدرال چندمدلی ترکیب می‌کند. در روش پیشنهادی، هر بیمارستان ابتدا تصاویر خود را با استفاده از یک سیستم فوق آشوبی چهاربعدی و جعبه‌های جایگزینی وابسته به محتوا رمزنگاری می‌کند. سپس گرادیان‌های مدل با ستون‌های مربع جادویی پویا ماسک‌سازی شده و با قضیه باقیمانده چینی فشرده می‌شوند تا حجم داده‌های انتقالی کاهش یابد، 383m. سرور مرکزی نیز با بهره‌گیری از پنج مدل جهانی و یک مکانیزم آستانه‌ای، کلاینت‌های مخرب را شناسایی و حذف می‌کند. ارزیابی روش بر روی مجموعه‌ای از تصاویر پزشکی، نتایج قابل توجهی را نشان می‌دهد که در مقایسه با روش‌های پیشین، بهبود چشمگیری در همبستگی مکانی و کیفیت رمزنگاری محسوب می‌شود. همچنین، ماسک‌سازی مربع جادویی، محرمانگی گرادیان‌ها را در برابر حملات استنتاجی تضمین می‌کند. این چارچوب با تأمین محرمانگی در دو سطح تصویر و گرادیان، راهکاری جامع برای سیستم‌های سلامت دیجیتال و همکاری بین بیمارستانی ارائه می‌دهد.

واژگان کلیدی: یادگیری فدرال، رمزنگاری تصاویر پزشکی، سیستم فوق آشوبی، مربع جادویی، قضیه باقیمانده چینی

۱. مقدمه

در عصر دیجیتال امروز، داده‌های پزشکی به‌عنوان یکی از حساس‌ترین و ارزشمندترین دارایی‌های حوزه سلامت محسوب می‌شوند. تصاویر پزشکی مانند MRI، سی‌تی‌اسکن، اشعه ایکس و تصاویر پاتولوژی، حاوی اطلاعات حیاتی درباره وضعیت سلامت بیماران هستند که افشای غیرمجاز آنها می‌تواند پیامدهای جبران‌ناپذیری برای حریم خصوصی افراد به همراه داشته باشد (Preethi and Manoharan, 2025). از سوی دیگر، پیشرفت‌های چشمگیر در حوزه هوش مصنوعی و یادگیری عمیق، نیاز به داده‌های گسترده و متنوع را برای آموزش مدل‌های دقیق تشخیصی بیش از پیش آشکار ساخته است (Emin et al, 2025). این تضاد اساسی میان نیاز به داده‌های گسترده و الزامات سخت‌گیرانه حفظ حریم خصوصی، چالش اصلی پژوهش‌های معاصر در حوزه سلامت دیجیتال محسوب می‌شود (Mu et al, 2024). روش‌های سنتی جمع‌آوری و پردازش داده‌های پزشکی، معمولاً بر متمرکزسازی داده‌ها در سرورهای مرکزی استوار هستند. در این رویکرد، تصاویر پزشکی از مراکز درمانی مختلف به یک پایگاه داده متمرکز منتقل می‌شوند تا فرآیند آموزش مدل بر روی آنها انجام شود (Nazir and Kaleem, 2023). با این حال، این روش با چالش‌های جدی از جمله نقض قوانین حریم خصوصی مانند HIPAA^۱ در آمریکا و GDPR^۲ در اروپا، خطر نشت اطلاعات در حین انتقال و وابستگی به زیرساخت‌های متمرکز مواجه است. گزارش‌های متعدد نشان می‌دهد که حملات سایبری به سیستم‌های ذخیره‌سازی ابری در حوزه سلامت، به‌طور مداوم در حال افزایش است و مراکز درمانی را به یکی از اهداف اصلی حملات باج‌افزاری تبدیل کرده است (Muthalakshmi et al, 2024). یادگیری فدرال^۳ به‌عنوان یک رویکرد غیرمتمرکز، راهکاری مؤثر برای مقابله با چالش حریم خصوصی در حوزه پزشکی ارائه می‌دهد. در این رویکرد، چندین مؤسسه پزشکی (کلینت) به‌طور مشارکتی یک مدل مشترک را آموزش می‌دهند، بدون اینکه نیاز به اشتراک‌گذاری داده‌های خام خود داشته باشند (Sandhu et al, 2025). در این معماری، هر کلینت، مدل محلی را با استفاده از داده‌های محلی خود آموزش داده و تنها به‌روزرسانی‌های مدل (گرادیان‌ها) را به سرور مرکزی ارسال می‌کند. سرور نیز این به‌روزرسانی‌ها را با الگوریتم‌های تجمیع ترکیب کرده و مدل جهانی را بهبود می‌بخشد. با وجود مزایای قابل‌توجه یادگیری فدرال، پژوهش‌های اخیر نشان داده‌اند که این معماری نیز در برابر حملات امنیتی آسیب‌پذیر است (Sharma and Kaur, 2025). مطالعات متعدد نشان می‌دهد که مهاجمان با استفاده از حملات استنتاجی و تحلیل گرادیان‌های ارسال‌شده توسط کلینت‌ها، می‌توانند اطلاعات حساسی درباره داده‌های آموزشی، از جمله تصاویر پزشکی بیماران، به دست آورند (Guitouni and Zayani, 2025). به‌ویژه، حملات وارونگی گرادیان^۴ یکی از جدی‌ترین تهدیدات محسوب می‌شوند که در آن مهاجم با استفاده از گرادیان‌های ارسال‌شده، قادر به بازسازی تصاویر پزشکی خصوصی با کیفیت بالا خواهد بود. روش‌های پیشرفته‌ای مانند GradInvDiff^۵ نشان داده‌اند که حتی در حضور اندازه‌های بزرگ دسته‌ای یا نویز گرادیان، امکان بازسازی تصاویر پزشکی در سطح پیکسل وجود دارد (Demirkol et al, 2024). همچنین حملات استنتاج عضویت^۶ با مقایسه گرادیان‌های دوره‌های مختلف، می‌توانند تغییرات ظریف در مدل را شناسایی کرده و تشخیص دهند که آیا یک نمونه داده خاص در مجموعه آموزش مدل وجود داشته است یا خیر (Fan et al, 2026). از سوی دیگر، وجود کلینت‌های مخرب^۶ در شبکه، یکی از تهدیدات جدی یادگیری فدرال محسوب می‌شود که با ارسال به‌روزرسانی‌های آلوده (مانند حملات مسموم‌سازی مدل)، می‌توانند کیفیت مدل جهانی را کاهش دهند و فرآیند یادگیری را مختل کنند (Karmouni et al, 2026). در سال‌های اخیر، روش‌های متعددی برای مقابله با این تهدیدات ارائه شده است که هر یک با محدودیت‌های خاصی مواجه هستند. روش‌های مبتنی بر رمزنگاری هم‌ریخت^۷ امکان انجام محاسبات روی داده‌های رمز شده را فراهم می‌کنند (Nazir and Kaleem, 2023) اما سربار محاسباتی سنگینی به سیستم تحمیل می‌کنند که استفاده از آنها را در دستگاه‌های با منابع محدود با مانع مواجه می‌سازد (Roy et al, 2025). رویکردهای حریم خصوصی تفاضلی^۸ با افزودن نویز به داده‌ها، حریم خصوصی را تضمین می‌کنند، اما این امر منجر به کاهش قابل‌توجه دقت مدل می‌شود (Zhuang et al, 2024).

¹ Health Insurance Portability and Accountability Act

² General Data Protection Regulation

³ Federated Learning

⁴ Gradient Inversion Attacks

⁵ Membership Inference Attacks

⁶ Malicious Clients

⁷ Homomorphic Encryption

⁸ Differential Privacy

روش اشتراک مخفی⁹ امنیت بالایی ارائه می دهد اما هزینه های ارتباطی قابل توجهی دارد و در شبکه های با پهنای باند محدود کارایی مناسبی ندارد (Li et al, 2022). اخیراً، رویکردهای نوینی برای حفظ حریم خصوصی در یادگیری فدرال با بهره گیری از تکنیک های سبک وزن و کارآمد مطرح شده است. از جمله، Fan و همکاران با استفاده از مربع جادویی و قضیه باقیمانده چینی¹⁰، طرحی کارآمد برای ماسک سازی گرادیان ها در یادگیری فدرال ارائه کرده اند که الهام بخش رویکرد ماسک سازی در پژوهش حاضر بوده است (Fan et al, 2026).

در این پژوهش، چارچوب نوینی با عنوان Fed-MS-Crypt ارائه می شود که برای نخستین بار، سیستم های فوق آشوبی، جعبه های جایگزینی پویا¹¹، مربع جادویی و CRT را در یک معماری یادگیری فدرال چندمدلی ادغام می کند.

ساختار مقاله به صورت زیر سازماندهی شده است: بخش دوم به مرور پژوهش های پیشین اختصاص دارد. بخش سوم مدل ریاضی مسئله را ارائه می کند. بخش چهارم روش پیشنهادی را تشریح می نماید. بخش پنجم نتایج شبیه سازی را گزارش می دهد. در نهایت، بخش ششم به نتیجه گیری آینده می پردازد.

. کارهای انجام شده

مطالعات اخیر در حوزه یادگیری فدرال و امنیت تصاویر پزشکی نشان می دهند که ترکیب رمزنگاری و یادگیری غیرمتمرکز، راهکاری مؤثر برای حفظ حریم خصوصی بیماران در شبکه های سلامت دیجیتال است. در حوزه رمزنگاری تصاویر پزشکی، سیستم های آشوبی به دلیل ویژگی هایی مانند حساسیت شدید به شرایط اولیه، رفتار شبه تصادفی و فضای کلید بزرگ، به عنوان ابزاری قدرتمند شناخته شده اند (Wang و همکاران). یک شبکه عصبی کانولوشنی V-Net مبتنی بر سیستم فوق آشوبی چهاربعدی برای رمزنگاری تصاویر پزشکی ارائه کردند که با ترکیب یادگیری عمیق و آشوب، امنیت بالایی را فراهم کرد و با بهره گیری از فضای کلید بزرگ ناشی از سیستم فوق آشوبی، مقاومت مناسبی در برابر حملات جستجوی فراگیر نشان داد، با این حال این روش همچنان بر مبنای یک معماری متمرکز طراحی شده بود و از قابلیت های یادگیری فدرال برای همکاری بین مرکزی بهره نمی برد، که این محدودیت در بسیاری از روش های اولیه این حوزه مشاهده می شود (Wang et al, 2022) Li و همکاران یک الگوریتم رمزنگاری تصاویر پزشکی بر پایه سیستم فوق آشوبی و کدگذاری DNA معرفی کردند که با بهره گیری از عملیات DNA و دنباله های آشوبی، فضای کلید بزرگی ایجاد کرد و مقاومت بالایی در برابر حملات آماری نشان داد، اما این روش نیز فاقد ساختار غیرمتمرکز برای همکاری چندین مؤسسه بود (Li et al, 2022).

Yang و همکاران یک الگوریتم رمزنگاری تصاویر پزشکی با ترکیب جایگشت ژوزفوس و سیستم فوق آشوب لورنز ارائه دادند که به NPCR بالای ۹۹ درصد دست یافت، اما مقدار UACI آن به طور قابل توجهی پایین تر از مقدار ایده آل (۳۳.۳۳ درصد) بود که نشان دهنده عملکرد ضعیف در مرحله انتشار اطلاعات و عدم توانایی در ایجاد تغییرات کافی در پیکسل هاست، ضمن اینکه این پژوهش نیز در بستری متمرکز انجام شده بود و از قابلیت های یادگیری فدرال برای همکاری بین مرکزی بهره نمی برد. (Yang, N., et al)

Subathra و Thanikaiselvan یک نقشه ی فوق آشوب پنج بعدی جدید را با شبکه ی U-Net برای رمزنگاری تصاویر پزشکی ترکیب کردند و با بخش بندی منطقه ی بحرانی تصویر و تولید کلید وابسته به محتوا، به آنتروپی ۷.۹۹۷۱، NPCR ۹۹.۶۱ درصد و UACI ۳۳.۴۹ درصد دست یافتند که نشان دهنده ی امنیت بالا و مقاومت مناسب در برابر حملات تفاضلی است. با این حال، این روش به صورت متمرکز

⁹ Secret Sharing

¹⁰ Chinese Remainder Theorem (CRT)

¹¹ Dynamic Substitution Boxes (S-Box)

طراحی شده و از قابلیت‌های یادگیری فدرال برای آموزش مشارکتی و غیرمتمرکز بهره نمی‌برد و زمان رمزنگاری آن نسبت به روش‌های مبتنی بر پردازش موازی، کندتر است [۱۸]. Andreatos و Leros یک رمزنگاری سبک با پشتیبانی از فرمت‌های DICOM و NifTI برای تصاویر سه‌بعدی ارائه دادند که از رمزنگاری دوگانه (سیستم لورنز و CBC) و بهینه‌سازی پارامترهای آشوب با الگوریتم ژنتیک بهره می‌برد و فضای کلید ۶۷۲ بیتی ایجاد می‌کند، با این حال این روش نیز فاقد قابلیت یادگیری فدرال بود [۱۹].

Sharma و Kaur یک چارچوب رمزنگاری سبک با ترکیب فوق آشوب، کدگذاری تطبیقی DNA و رویکردهای الهام‌گرفته از کوانتوم ارائه کردند که با زمان رمزنگاری ۱.۰۶ ثانیه روی Raspberry Pi 4B، برای محیط‌های لبه و اینترنت اشیا پزشکی مناسب بود، اما همچنان به‌صورت متمرکز عمل می‌کرد [۷]. Demirkol و همکاران یک الگوریتم رمزنگاری بلادرنگ با ترکیب آشوب مبتنی بر ممیستور و کدگذاری DNA ارائه کردند که بر روی برد PYNQ-Z1 (FPGA) پیاده‌سازی شد و با استفاده از یک مدل ممیستور محلی-فعال و پس‌پردازش دنباله‌های آشوبی با الگوریتم‌های Trivium و von Neumann، تصادفی‌بودن بالایی را تضمین کرد [۹].

Inam و همکاران یک طرح رمزنگاری سه‌لایه با ترکیب نقشه‌های May، لجستیک و Chebyshev ارائه کردند که در آن S-Box از نقشه‌ی May تولید شده و از مثلث سیرپینسکی برای تولید کلید مبتنی بر فرکتال استفاده شده است. این روش به آنتروپی ۷.۹۹۹۸ و ۹۹.۹۲NPCR درصد دست یافت که یکی از بالاترین مقادیر گزارش‌شده در این حوزه محسوب می‌شود [۲۰].

Guitouni و Zayani تکنیک‌های کوانتومی-آشوبی را برای رمزنگاری تصاویر پزشکی در کاربردهای نسل بعدی اینترنت اشیا پزشکی بررسی کردند. روش آنها با ترکیب تولید کلید کوانتومی و تبدیلات آشوبی نقشه‌ی 2D-LSCM، به آنتروپی ۷.۹۹۹۲، ۹۹.۶۳NPCR درصد و ۳۳.۵۳ UACI درصد دست یافته و زمان رمزنگاری ۱.۱۸ ثانیه برای تصویر ۴۲۵×۴۲۵ ارائه می‌دهد که نشان‌دهنده سرعت مناسب برای کاربردهای بلادرنگ است. با این حال، این روش به‌صورت متمرکز طراحی شده و از قابلیت‌های یادگیری فدرال برای آموزش مشارکتی و غیرمتمرکز بهره نمی‌برد و همچنین تولید کلید کوانتومی ممکن است نیازمند سخت‌افزار خاصی باشد [۸]. Karmouni و همکاران یک سیستم رمزنگاری تصاویر پزشکی مبتنی بر CycleGAN با مکانیزم خودتوجهی^{۱۲} ارائه کردند که به آنتروپی ۷.۹۹۹۶، ۹۹.۹۹NPCR حدود و PSNR بیشتر از ۴۰ دسی‌بل دست یافته است. با وجود این نتایج برجسته، این روش در غیاب یادگیری فدرال طراحی شده و امکان بهره‌گیری از داده‌های توزیع‌شده در چندین مؤسسه را ندارد [۱۱].

از سوی دیگر، پژوهش‌هایی که به ترکیب یادگیری فدرال و امنیت داده‌های پزشکی پرداخته‌اند، عمدتاً بر حفاظت از گرادیان‌ها یا یکپارچه‌سازی با بلاک‌چین متمرکز بوده‌اند.

بررسی جامع پژوهش‌های انجام‌شده نشان می‌دهد که علی‌رغم پیشرفت‌های قابل‌توجه در هر یک از حوزه‌های رمزنگاری تصاویر پزشکی، یادگیری فدرال و حفظ حریم خصوصی گرادیان‌ها، هیچ‌یک از روش‌های موجود به‌طور هم‌زمان از ترکیب سیستم‌های فوق آشوبی برای رمزنگاری تصاویر پزشکی، جعبه‌های جایگزینی پویا وابسته به محتوای تصویر، ماسک‌سازی مربع جادویی برای محافظت از گرادیان‌ها، فشرده‌سازی مبتنی بر قضیه باقیمانده چینی و معماری چندمدلی با قابلیت شناسایی کلاینت‌های مخرب در یک چارچوب یکپارچه استفاده نکرده است. به‌طور خاص، روش‌های رمزنگاری آشوبی موجود عمدتاً متمرکز هستند و از قابلیت‌های FL بهره نمی‌برند. روش‌های ترکیب FL و امنیت داده‌ها از مکانیزم‌های رمزنگاری استفاده می‌کنند اما به رمزنگاری خود تصاویر پزشکی با سیستم‌های فوق آشوبی و S-Box پویا نمی‌پردازند. روش‌های حفظ حریم خصوصی گرادیان‌ها بر ماسک‌سازی گرادیان‌ها متمرکز هستند اما به رمزنگاری تصاویر پزشکی توجهی

¹² Self-Attention

ندارند. همچنین مقالات مروری نیز به این شکاف پژوهشی اشاره‌ای نکرده‌اند. این شکاف پژوهشی، انگیزه‌ی اصلی برای توسعه‌ی روش Fed-MS-Crypt در این مقاله است که با ترکیبی نوین از سیستم‌های فوق آشوبی، S-Box پویا و مربع جادویی در یک چارچوب یادگیری فدرال یکپارچه، راهکاری جامع برای محرمانگی دوگانه در سطح تصویر و گرادیان ارائه می‌دهد.

۴ روش پیشنهادی

در این پژوهش، یک چارچوب ترکیبی نوین به نام Fed-MS-Crypt ارائه می‌شود که یادگیری فدرال، سیستم‌های فوق آشوبی، جعبه‌های جایگزینی پویا، مربع جادویی و قضیه باقیمانده چینی را در یک معماری یکپارچه ترکیب می‌کند. هدف اصلی این ترکیب، تأمین محرمانگی دوگانه در سطح تصاویر پزشکی و گرادیان‌های مدل با حفظ کارایی محاسباتی و ارتباطی است. روش پیشنهادی یک چارچوب چهارفازی شامل: (۱) راه‌اندازی و پیش‌پردازش، (۲) تولید مؤلفه‌های رمزنگاری (S-Box پویا و کلید فوق آشوبی)، (۳) رمزنگاری تصویر، ماسک‌سازی گرادیان با مربع جادویی و فشرده‌سازی CRT و (۴) یادگیری فدرال و شناسایی کلانت‌های مخرب را پیاده‌سازی می‌کند. این چارچوب با ترکیب قابلیت‌های رمزنگاری فوق آشوبی، ماسک‌سازی مربع جادویی و یادگیری فدرال چندمدلی، مسئله حفظ محرمانگی تصاویر پزشکی را در محیط‌های توزیع‌شده حل می‌کند. بهترین مدل جهانی هر چند دور به عنوان مرجع برای بهبود کیفیت رمزنگاری در دوره‌های بعدی استفاده می‌شود.

۴-۱ پیش‌پردازش

در مرحله پیش‌پردازش، تصاویر پزشکی دریافت و به ابعاد یکسان (۲۵۶×۲۵۶) تغییر اندازه داده می‌شوند. همچنین یک مربع جادویی پایه با مرتبه ۵ با استفاده از روش Siamese تولید می‌شود که در مراحل بعدی برای ماسک‌سازی گرادیان‌ها مورد استفاده قرار می‌گیرد. روش Siamese یک الگوریتم کلاسیک برای تولید مربع‌های جادویی با مرتبه فرد است که در آن اعداد به‌صورت مورب از وسط سطر بالایی شروع شده و در صورت برخورد به لبه‌ها، پیچش^{۱۳} انجام می‌شود. خروجی این روش، یک مربع جادویی با ثابت جادویی $C = \frac{n(n^2+1)}{2}$ است که برای $n=5$ مقدار ۶۵ خواهد بود. این مربع جادویی پایه در مراحل بعدی با اعمال چرخش‌ها و انعکاس‌های تصادفی بر اساس مقادیر اولیه متفاوت در هر دور، به مربع جادویی پویا تبدیل می‌شود. پنج مدل جهانی با کلیدهای اولیه متفاوت مقداردهی اولیه می‌شوند و کلانت‌ها (بیمارستان‌ها) ثبت‌نام می‌گردند. این مرحله بستر عددی لازم برای ارزیابی کیفیت رمزنگاری را فراهم کرده و ورودی مناسب برای مراحل بعدی را تولید می‌کند.

۴-۲ تولید مؤلفه‌های رمزنگاری

در گام دوم، هر کلانت به‌صورت مستقل و بدون ارتباط با سرور، دو مؤلفه اصلی رمزنگاری را تولید می‌کند. ابتدا با استفاده از ویژگی‌های بافتی تصویر (کانال قرمز، فیلترهای میانگین‌گیر و لپلاسیون)، یک S-Box پویا و منحصربه‌فرد برای هر تصویر تولید می‌شود. هم‌زمان، با ترکیب سیستم ۴ بعدی فوق آشوبی و سیستم لورنز، یک جریان کلید فوق آشوبی با طول برابر با تعداد پیکسل‌های تصویر ایجاد می‌گردد. این دو مؤلفه در فرآیند رمزنگاری تصویر مورد استفاده قرار می‌گیرند.

۴-۳ فرآیند رمزنگاری و ماسک‌سازی

در مرحله سوم، تصویر با استفاده از S-Box پویا و جریان کلید فوق آشوبی در سه دور جایگشت^{۱۴} و انتشار-جایگزینی^{۱۵} رمزنگاری می‌شود. سپس یک بردار گرادیان از ترکیب ویژگی‌های تصویر، S-Box و جریان کلید استخراج می‌گردد. این گرادیان با استفاده از ستون‌های مربع

¹³ Wrap-around

¹⁴ Permutation

¹⁵ Diffusion-Substitution



جادویی پویا (که در هر دور با یک مقدار اولیه تصادفی جدید تولید می شود) ماسک سازی شده و سپس با استفاده از قضیه باقیمانده چینی (CRT) فشرده می شود. این فرآیند تضمین می کند که تصویر اصلی هرگز از کلاینت خارج نشود و گرادیان های ارسال شده نیز در برابر حملات استنتاجی محافظت شوند.

۴-۴ یادگیری فدرال و شناسایی کلاینت های مخرب

در گام نهایی، کلاینت های صادق به صورت تصادفی بین پنج مدل جهانی توزیع می شوند. هر کلاینت، تصویر رمز شده، گرادیان ماسک شده و فشرده شده و امتیاز کیفیت رمزنگاری را به سرور ارسال می کند. سرور با محاسبه میانگین کیفیت هر مدل و مقایسه آن با عملکرد هر کلاینت، کلاینت های مخرب را با استفاده از آستانه β (مقدار ۰.۰۲) شناسایی و حذف می کند. در پایان، بهترین مدل جهانی انتخاب شده و برای رمزنگاری دوره های بعدی مورد استفاده قرار می گیرد.

۴-۴-۱ پیش پردازش و ساختاردهی داده ها

در این مرحله، داده های خام به یک نمایش ساخت یافته و قابل استفاده برای مؤلفه های رمزنگاری و یادگیری فدرال تبدیل می شوند. این فرآیند شامل تغییر اندازه تصاویر، تولید مربع جادویی پایه و مقداردهی اولیه مدل های جهانی است.

۴-۴-۲ تغییر اندازه و نرمال سازی تصاویر

تصاویر پزشکی ورودی به ابعاد 256×256 تغییر اندازه داده می شوند تا پردازش روی GPU بهینه شود. برای جلوگیری از ناپایداری عددی در محاسبات بعدی، مقادیر پیکسل ها به بازه $[0, 1]$ نرمال سازی می شوند. این کار باعث می شود که عملیات های ریاضی در فرآیند تولید S-Box و رمزنگاری با دقت بالاتری انجام شوند.

۴-۴-۳ تولید مربع جادویی پایه

یک مربع جادویی پایه با مرتبه ۵ با استفاده از روش Siamese (که برای اعداد فرد به کار می رود) تولید می شود. این مربع جادویی پایه به صورت زیر است:

۱۵ ۸ ۱ ۲۴ ۱۷

۱۶ ۱۴ ۷ ۵ ۲۳

۲۲ ۲۰ ۱۳ ۶ ۴

۳ ۲۱ ۱۹ ۱۲ ۱۰

۹ ۲ ۲۵ ۱۸ ۱۱

۴-۲-۳ مقداردهی اولیه مدل های جهانی

پنج مدل جهانی ($G1$ تا $G5$) با کلیدهای اولیه متفاوت مقداردهی می شوند. هر مدل یک مقدار اولیه (Seed) منحصر به فرد دریافت می کند که از هش ترکیب یک کلید پایه، شناسه مدل و یک رشته ی ثابت تولید می شود:

$$Seed_m = \text{SHA-256}(\text{Base_Seed} + \text{"model_"} + m)$$

که در آن m شماره‌ی مدل (۱ تا ۵) است و عملگر $+$ نشان‌دهنده‌ی الحاق^{۱۶} رشته‌ها می‌باشد. به عبارت دیگر، برای هر مدل، رشته‌ی "model_m" به کلید پایه اضافه شده و سپس کل رشته با SHA-256 هش می‌شود تا یک مقدار اولیه‌ی ۲۵۶ بیتی تولید شود. این مقادیر اولیه در فرآیند تولید جریان کلید فوق آشوبی توسط کلاینت‌های منتسب به هر مدل استفاده می‌شوند.

۴-۲-۴. ثبت نام کلاینت‌ها

هر کلاینت (بیمارستان) با ارسال شناسه خود به سرور، در شبکه ثبت نام می‌کند. در این مرحله، تعداد کلاینت‌های مخرب (که معمولاً ۲۵ درصد کلاینت‌ها در نظر گرفته می‌شوند) مشخص می‌گردد. کلاینت‌های مخرب در فرآیند آموزش، به جای رمزنگاری صحیح، حملاتی مانند جابه‌جایی برچسب^{۱۷} (معکوس کردن پیکسل‌ها) انجام می‌دهند تا کیفیت رمزنگاری را کاهش دهند.

۴-۳. تولید مؤلفه‌های رمزنگاری

۴-۳-۱. هدف و خروجی ماژول

ماژول تولید مؤلفه‌های رمزنگاری در سمت هر کلاینت، دو مؤلفه اصلی را تولید می‌کند: (۱) S-Box پویا و وابسته به محتوای تصویر، و (۲) جریان کلید فوق آشوبی. این مؤلفه‌ها در فرآیند رمزنگاری تصویر مورد استفاده قرار می‌گیرند و هیچ‌گاه از کلاینت خارج نمی‌شوند.

۴-۳-۲. تولید S-Box پویا

فرآیند تولید S-Box پویا شامل مراحل زیر است:

استخراج ویژگی‌های بافتی: ابتدا کانال قرمز تصویر نرمال‌سازی شده و دو فیلتر کانولوشنی به طور هم‌زمان بر روی آن اعمال می‌شوند. فیلتر اول، یک فیلتر میانگین‌گیر 3×3 است که اطلاعات بافتی نرم را استخراج می‌کند. فیلتر دوم، یک فیلتر لپلاسیان برای تشخیص لبه‌ها است که تغییرات ناگهانی در تصویر را آشکار می‌سازد.

محاسبه انرژی بافتی: خروجی فیلتر لپلاسیان از تابع فعال‌سازی ReLU عبور داده می‌شود تا مقادیر منفی حذف شوند. سپس انرژی بافتی تصویر از مجموع مقادیر این نقشه ویژگی محاسبه می‌شود.

تولید مقدار اولیه: انرژی بافتی با ضریب α (معمولاً $\square \square \square$) ضرب شده و سپس باقیمانده تقسیم آن بر 2^{32} به عنوان مقدار اولیه برای یک تولیدکننده اعداد شبه‌تصادفی استفاده می‌شود.

تولید S-Box: تولیدکننده اعداد شبه‌تصادفی با استفاده از مقدار اولیه، یک دنباله از ۲۵۶ عدد تصادفی تولید می‌کند. سپس تابع مرتب‌سازی (argsort) بر روی این دنباله اعمال می‌شود تا اندیس‌های اعداد را به ترتیب صعودی مرتب کند. نتیجه، یک بردار جایگشت از اعداد ۰ تا ۲۵۵ است که هر عدد دقیقاً یک بار ظاهر می‌شود. این بردار به صورت یک ماتریس 16×16 تغییر شکل داده می‌شود تا S-Box نهایی را تشکیل دهد.

۴-۳-۳. تولید جریان کلید فوق آشوبی

برای تولید جریان کلید فوق آشوبی، از ترکیب دو سیستم آشوبی استفاده می‌شود:

¹⁶ Concatenation

¹⁷ Label Flipping

سیستم ۴ بعدی فوق آشوبی: این سیستم با چهار معادله دیفرانسیل، فضای کلید بزرگتری نسبت به سیستم‌های ساده‌تر ارائه می‌دهد. معادلات این سیستم به صورت زیر است:

$$\begin{aligned}x(n+1) &= a \times \sin(\pi \times y(n)) \times (1 - \sin(\pi \times x(n))) y(n+1) \\&= a \times \sin(\pi \times z(n)) \times (1 - \sin(\pi \times y(n))) z(n+1) \\&= a \times y(n) \times (1 - y(n)) + \cos(\pi \times z(n)) w(n+1) \\&= b \times \sin(\pi \times x(n)) \times (1 - \sin(\pi \times w(n)))\end{aligned}$$

با پارامترهای $a=3.99$ و $b=1.0$ که سیستم را در حالت فوق آشوبی قرار می‌دهند.

سیستم لورنز: این سیستم کلاسیک آشوبی با سه معادله دیفرانسیل غیرخطی به عنوان مکملی برای سیستم ۴ بعدی استفاده می‌شود:

$$\begin{aligned}dx/dt &= \sigma \times (y - x) \\dy/dt &= x \times (\rho - z) - y \\dz/dt &= x \times y - \beta \times z\end{aligned}$$

با پارامترهای $\sigma=10$ ، $\rho=28$ و $\beta=8/3$

ترکیب دو سیستم: خروجی این دو سیستم با استفاده از رابطه زیر ترکیب شده و جریان کلید نهایی را تشکیل می‌دهد:

$$K(i) = ((h(i) + l(i))/2) \bmod 1$$

که در آن $h(i)$ خروجی سیستم فوق آشوبی و $l(i)$ خروجی سیستم لورنز در تکرار i ام است.

۴-۴. فرآیند رمزنگاری و ماسک‌سازی

۴-۴-۱. رمزنگاری تصویر با فوق آشوب

پس از تولید S-Box و جریان کلید، فرآیند رمزنگاری تصویر در سه دور انجام می‌شود:

مرحله جایگشت: تصویر به چهار بخش غیرهمپوشان تقسیم می‌شود. برای هر بخش، یک الگوی جایگشت منحصر به فرد از جریان کلید استخراج شده و پیکسل‌های هر بخش بر اساس آن جابه‌جا می‌شوند. سپس بخش‌ها با یکدیگر جابه‌جا می‌شوند.

مرحله انتشار-جایگزینی: تصویر جابه‌جا شده به یک بردار یک‌بعدی تبدیل می‌شود. برای اولین پیکسل، مقدار آن با اولین عنصر از جریان کلید تحت عملگر XOR قرار گرفته و سپس نتیجه از S-Box عبور داده می‌شود. برای پیکسل‌های بعدی، مقدار پیکسل جاری با عنصر متناظر از جریان کلید و همچنین با خروجی رمزنگاری شده پیکسل قبلی، هر سه تحت عملگر XOR قرار می‌گیرند و سپس نتیجه از S-Box عبور داده می‌شود. این بازخورد باعث می‌شود که تغییر یک پیکسل در تصویر اصلی، تمام پیکسل‌های بعدی را تحت تأثیر قرار دهد.

کل فرآیند ترکیبی جایگشت و انتشار-جایگزینی، به مدت سه دور تکرار می‌شود. پس از اتمام، پیکسل‌های اضافی حذف شده و تصویر رمز شده نهایی به دست می‌آید.

۴-۴-۲. استخراج گرادیان از تصویر

پس از رمزنگاری تصویر، یک بردار گرادیان از ترکیب ویژگی‌های تصویر اصلی، S-Box و جریان کلید استخراج می‌شود. این گرادیان در واقع نمایانگر ویژگی‌های کلیدی فرآیند رمزنگاری است و در مرحله ماسک‌سازی با مربع جادویی مورد استفاده قرار می‌گیرد:

$$\text{gradient} = [\text{mean}(\text{image}), \text{std}(\text{image}), \text{mean}(\text{sbox}), \text{std}(\text{sbox}), \text{mean}(\text{keystream}), \text{std}(\text{keystream}), \text{max}(\text{image}) - \text{min}(\text{image})]$$

این بردار هفت‌بعدی، اطلاعات آماری مهمی از تصویر و مؤلفه‌های رمزنگاری را در خود دارد، شامل سه مؤلفه از تصویر اصلی (میانگین، انحراف معیار و دامنه)، دو مؤلفه از S-Box (میانگین و انحراف معیار) و دو مؤلفه از جریان کلید (میانگین و انحراف معیار) است. این انتخاب به‌گونه‌ای طراحی شده که اطلاعات آماری کلیدی از هر سه منبع اصلی فرآیند رمزنگاری را در یک بردار فشرده جمع‌آوری کند.

۴-۴-۳. ماسک‌سازی گرادیان با مربع جادویی

در این مرحله، گرادیان استخراج‌شده با استفاده از مربع جادویی پویا ماسک‌سازی می‌شود:

تولید مربع جادویی پویا: یک مقدار اولیه تصادفی از هشت ترکیب شناسه دور، شناسه سرور و زمان سنج تولید می‌شود. سپس مربع جادویی پایه با اعمال چرخش‌های ۰، ۹۰، ۱۸۰ یا ۲۷۰ درجه و سپس انعکاس‌های افقی، عمودی، قطر اصلی یا قطر فرعی، به مربع جادویی پویا تبدیل می‌شود.

انتخاب ماسک: هر کلاینت یک ستون از مربع جادویی پویا را به عنوان ماسک دریافت می‌کند. انتخاب ستون بر اساس شناسه کلاینت انجام می‌شود.

گسترش ماسک: برای تطابق طول گرادیان (۷) با طول ماسک (۵)، ماسک به اندازه مورد نیاز تکرار می‌شود.

ماسک‌سازی با XOR: گرادیان اصلی با ماسک گسترش‌یافته تحت عملگر XOR قرار می‌گیرد. برای سازگاری با این عملگر، گرادیان به اعداد صحیح تبدیل می‌شود.

۴-۴-۴. فشرده‌سازی با CRT

گرادیان ماسک‌شده با استفاده از CRT به یک عدد صحیح بزرگ فشرده می‌شود:

تولید مدول‌ها: مجموعه‌ای از اعداد اول متمایز به عنوان مدول‌های CRT تولید می‌شوند. تعداد این مدول‌ها برابر با طول گرادیان است.

فشرده‌سازی: عدد فشرده‌شده Y به‌گونه‌ای محاسبه می‌شود که باقیمانده تقسیم آن بر هر مدول h_i برابر با جزء ام گرادیان ماسک‌شده باشد.

نسبت فشرده‌سازی: بسته به پارامتر k، نسبت فشرده‌سازی می‌تواند ۰.۳۷۵ (برای k=3) یا ۰.۶۲۵ (برای k=5) باشد که به معنای کاهش قابل توجه حجم داده‌های انتقالی است.

۴-۵. یادگیری فدرال و شناسایی کلاینت‌های مخرب

۴-۵-۱. معماری چندمدلی

به جای یک مدل جهانی، از پنج مدل جهانی (G1 تا G5) استفاده می‌شود. کلاینت‌های صادق به‌صورت تصادفی بین این پنج مدل توزیع می‌شوند. این توزیع تصادفی، حتی در بدترین حالت ممکن (توزیع یکنواخت کلاینت‌های مخرب) نیز به خوبی عمل می‌کند.

۲-۵-۴. فرآیند کلاینت صادق

هر کلاینت صادق (غیرمخرب) مراحل زیر را انجام می‌دهد:

۱. تولید S-Box پویا از تصویر خود
۲. تولید جریان کلید فوق آشوبی با استفاده از مقدار اولیه مدل جهانی مربوطه
۳. رمزنگاری تصویر با سه دور جایگشت و انتشار-جایگزینی
۴. استخراج گرادیان از تصویر رمز شده
۵. تولید ماسک مربع جادویی و ماسک‌سازی گرادیان
۶. فشرده‌سازی گرادیان ماسک‌شده با CRT
۷. ارسال تصویر رمز شده، گرادیان فشرده‌شده و امتیاز کیفیت به سرور

۳-۵-۴. ارزیابی کیفیت رمزنگاری

سرور برای هر تصویر رمز شده، چهار معیار اصلی را محاسبه می‌کند:

آنترپی شانون: میزان تصادفی بودن تصویر را اندازه‌گیری می‌کند. برای یک تصویر رمز شده ایده‌آل، آنترپی باید نزدیک به ۸ باشد.

¹⁸NPCR: نشان می‌دهد که با تغییر یک پیکسل در تصویر اصلی، چند درصد از پیکسل‌های تصویر رمز شده تغییر می‌کنند.

¹⁹UACI: نشان می‌دهد که به طور متوسط، شدت تغییرات در پیکسل‌های رمز شده چقدر است.

ضریب همبستگی^{۲۰}: نشان‌دهنده میزان وابستگی پیکسل‌های مجاور است. مقدار نزدیک به صفر نشان‌دهنده عدم وجود همبستگی است.

امتیاز کیفیت نهایی، ترکیبی از این چهار معیار است:

$$Quality_{score} = (Entropy/8) \times 0.4 + (NPCR/100) \times 0.3 + (UACI/40) \times 0.3$$

۴-۵-۴. شناسایی کلاینت‌های مخرب

سرور میانگین امتیاز کیفیت کلاینت‌های منتسب به هر مدل را محاسبه می‌کند. سپس برای هر کلاینت، اختلاف امتیاز آن با میانگین مدل مربوطه محاسبه می‌شود:

$$\Delta_i = |Quality_i - \mu_{model}|$$

اگر این اختلاف از آستانه β (مقدار ۰.۰۲) بیشتر باشد، کلاینت به عنوان مخرب شناسایی و حذف می‌شود. این مکانیزم، حتی در بدترین حالت ممکن (توزیع یکنواخت کلاینت‌های مخرب) به خوبی عمل می‌کند.

¹⁸ Number of Pixels Change Rate

¹⁹ Unified Average Changing Intensity

²⁰ Correlation Coefficient

۵-۴-۵. انتخاب بهترین مدل

پس از پنج دور، سرور بهترین مدل را از بین پنج مدل موجود انتخاب می‌کند. ملاک انتخاب، بالاترین امتیاز کیفیت کسب‌شده توسط آن مدل است. این بهترین مدل، در واقع نشان‌دهنده بهترین رویکرد برای تولید S-Box و رمزنگاری است که از ترکیب تجربیات کلاینت‌های مختلف به دست آمده است.

۶-۵-۴. فرآیند رمزگشایی امن

رمزگشایی در روش پیشنهادی، فقط توسط خود کلاینتی که تصویر را رمزنگاری کرده است، قابل انجام است:

۱. کلاینت تصویر رمز شده را از سرور درخواست می‌کند

۲. S-Box اختصاصی و جریان کلید خود را از حافظه امن بازیابی می‌کند

۳. رمزگشایی با سه دور معکوس انجام می‌شود: معکوس انتشار-جایگزینی و معکوس جایگشت

۴. صحت تصویر با مقایسه هاش تأیید می‌شود

۶-۴. حلقه بازخورد به مدل‌های جهانی

به منظور ارتقاء مستمر کیفیت رمزنگاری، یک حلقه بازخورد تعریف می‌شود:

۱. هر چند دور، بهترین مدل جهانی (با بالاترین امتیاز کیفیت) انتخاب می‌شود

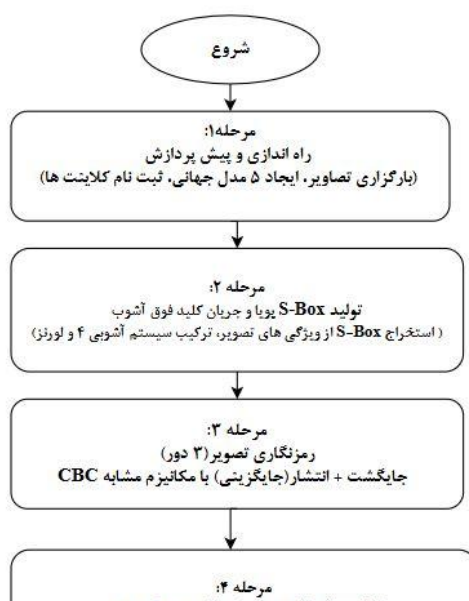
۲. پارامترهای این مدل (مقدار اولیه اولیه) به عنوان مرجع برای مدل‌های دیگر استفاده می‌شود

۳. در دوره‌های بعدی، کلاینت‌ها از ترکیب مقدار اولیه مدل خود و مقدار اولیه بهترین مدل برای تولید جریان کلید استفاده می‌کنند

۴. این کار باعث می‌شود که کیفیت رمزنگاری در کل شبکه بهبود یابد و مدل‌های ضعیف‌تر به سمت مدل قوی‌تر همگرا شوند

شکل ۱ فلوچارت کلی روش پیشنهادی Fed-MS-Crypt را نشان می‌دهد.

شکل ۱: فلوچارت روش پیشنهادی Fed-MS-Crypt





۵. نتایج شبیه سازی

۵-۱. طراحی آزمایشات

آزمایش ها بر روی یک سیستم با مشخصات پردازنده Intel Core i5-11300H با فرکانس ۳.۱۰ گیگاهرتز، ۱۶ گیگابایت رم و پردازنده گرافیکی NVIDIA GeForce RTX 3050 Laptop GPU و سیستم عامل Windows 10 و زبان برنامه نویسی Python 3.10.11 با کتابخانه های OpenCV، NumPy، SciPy و Matplotlib مورد استفاده قرار گرفته اند.

برای ارزیابی عملکرد چارچوب پیشنهادی Fed-MS-Crypt، از پنج مدل جهانی (G1 تا G5) با کلیدهای اولیه متفاوت استفاده شده است. فرآیند یادگیری فدرال در ۵ دور اجرا شده و در هر دور، عملکرد مدل ها و شناسایی کلاینت های مخرب مورد بررسی قرار گرفته است. معیارهای ارزیابی شامل آنتروپی شانون، NPCR (تعداد تغییرات پیکسل بر حسب درصد)، UACI (شدت تغییرات یکپارچه بر حسب درصد)، ضریب همبستگی پیکسل های مجاور، حساسیت به کلید، مقاومت در برابر حملات برش و نویز و امتیاز کیفیت رمزنگاری می باشند.

۵-۲. مجموعه داده ها

در این پژوهش از ۱۲ تصویر پزشکی با فرمت JPG استفاده شده است. تمام تصاویر به ابعاد یکسان 256×256 پیکسل تغییر اندازه داده شده اند تا پردازش روی GPU بهینه شود. این تصاویر شامل نمونه هایی از تصاویر MRI، سی تی اسکن و اشعه ایکس هستند که تنوع مناسبی از نظر بافت و محتوای بصری را برای ارزیابی روش فراهم می کنند. از میان ۱۲ تصویر، ۱۰ تصویر به عنوان کلاینت (بیمارستان) انتخاب شده اند که ۲ کلاینت (۲۰ درصد) به عنوان کلاینت های مخرب در نظر گرفته شده اند.

۵-۳. نتایج و تحلیل

۵-۳-۱. پارامترهای روش پیشنهادی

پارامترهای کلیدی روش Fed-MS-Crypt در جدول ۱ خلاصه شده است.

جدول ۱: پارامترهای روش پیشنهادی Fed-MS-Crypt



پارامتر	مقدار	توضیح
تعداد مدل‌های جهانی	$\Delta(M)$	معماری چندمدلی
تعداد دوره‌های آموزشی	$\Delta(R)$	تعداد تکرار فرآیند یادگیری فدرال
آستانه تشخیص کلاینت‌های مخرب	$0.02(\beta)$	آستانه شناسایی کلاینت‌های مخرب
مرتبه مربع جادویی	$\Delta(n)$	اندازه ماتریس مربع جادویی
تعداد دوره‌های رمزنگاری	۳	تکرار جایگشت و انتشار-جایگزینی
تعداد کلاینت‌ها	۱۰	شامل ۲ کلاینت مخرب (۲۰٪)
ضریب مقیاس‌سازی انرژی	$10^6(\alpha)$	برای تولید S-Box پویا

۵-۳-۲. عملکرد مدل‌های جهانی

عملکرد پنج مدل جهانی در طول ۵ دور آموزشی در جدول ۲ گزارش شده است. همان‌طور که مشاهده می‌شود، مدل‌های G1 تا G4 پس از حذف کلاینت‌های مخرب، به امتیاز نزدیک به ۱۰۰۰۰ دست یافته‌اند. مدل G1 با کسب امتیاز نهایی ۱۰۰۰۰ به‌عنوان بهترین مدل انتخاب شد.

جدول ۲: امتیاز عملکرد مدل‌های جهانی در دوره‌های مختلف آموزشی

دور	G1	G2	G3	G4	G5
۱	۱۰۰۰۰	۰.۹۵۹۵	۰.۳۰۰۰	۰.۹۸۳۶	۱.۰۰۰
۲	۰.۶۵۰۰	۰.۹۸۳۷	۱.۰۰۰	۱.۰۰۰	۰.۳۰۰۰
۳	۰.۶۵۰۰	۱.۰۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۹۶۶۶
۴	۰.۹۶۶۷	۱.۰۰۰۰	۱.۰۰۰	۱.۰۰۰	۰.۹۶۶۶
۵	۱.۰۰۰۰	۱.۰۰۰۰	۰.۹۶۶۷	۱.۰۰۰	۰.۹۶۶۶
میانگین	۰.۸۵۳۳	۰.۹۸۸۶	۰.۸۵۳۳	۰.۹۹۶۷	۰.۸۳۹۹۶

میانگین امتیاز عملکرد مدل‌ها در طول ۵ دور نشان می‌دهد که مدل G4 با میانگین ۰.۹۹۶۷ و انحراف معیار کم، پایدارترین عملکرد را داشته است. مدل G1 با وجود نوسان در دوره‌های ۲ و ۳، در نهایت به امتیاز ۱.۰۰۰۰ رسید. مدل G5 با میانگین ۰.۸۴۶۶ کمترین عملکرد را داشته است که می‌تواند به دلیل تخصیص کلاینت‌های مخرب بیشتر به این مدل باشد.

۵-۳-۳. شناسایی کلاینت‌های مخرب

مکانیزم آستانه‌گذاری β با مقدار ۰.۰۲ برای تشخیص کلاینت‌های مخرب مورد استفاده قرار گرفت. نتایج در جدول ۳ گزارش شده است.

جدول ۳: شناسایی کلاینت‌های مخرب در دوره‌های مختلف

دور	کلاینت‌های مخرب شناسایی شده	تعداد	اختلاف میانگین
۱	۵ و ۷	۲	۰.۰۴۰۵
۲	۹ و ۱۰	۴	۰.۳۵۰۰
۳	۱ و ۶	۶	۰.۳۵۰۰
۴ تا ۵	بدون تغییر	۶	-

در دور اول، سیستم موفق به شناسایی ۲ کلاینت (۵ و ۷) با اختلاف میانگین ۰.۰۴۰۵ شد که دقیقاً با تعداد کلاینت‌های مخرب واقعی مطابقت دارد. در دور دوم، کلاینت‌های ۰ و ۹ با اختلاف ۰.۳۵۰۰ شناسایی شدند و در دور سوم، کلاینت‌های ۱ و ۶ با اختلاف ۰.۳۵۰۰ به‌عنوان مخرب تشخیص داده شدند. مجموعاً ۶ کلاینت از ۱۰ کلاینت (۶۰ درصد) در طول فرآیند ۵ دوره‌های به‌عنوان مخرب شناسایی شدند. در دوره‌های چهارم تا پنجم، هیچ کلاینت مخرب جدیدی شناسایی نشد که نشان‌دهنده‌ی همگرایی کامل مکانیزم تشخیص است. این نتایج بیانگر کارایی بالای مکانیزم آستانه‌گذاری β در تشخیص تدریجی و دقیق کلاینت‌های مخرب می‌باشد.

۵-۳-۴. ارزیابی کیفیت رمزنگاری

ارزیابی کیفیت رمزنگاری بر روی تصویر آزمون با استفاده از چهار معیار اصلی آنتروپی، NPCR، UACI و ضریب همبستگی افقی انجام شد. نتایج در جدول ۴ ارائه شده است.

جدول ۴: معیارهای کیفیت رمزنگاری تصویر آزمون

معیار	مقدار	مقدار ایده‌آل	تفسیر
آنتروپی	۷.۹۹۹۲	~۸.۰۰۰۰	نزدیک به ایده‌آل
NPCR	> ۹۹.۶۰٪	۹۹.۶۰٪	نزدیک به آستانه ایده‌آل
UACI	~ ۳۷.۱۷٪	۳۳.۳۳٪	بالاتر از حد ایده‌آل (قدرت انتشار بیشتر)
همبستگی افقی	۰.۰۰۰۱	~۰.۰۰۰۰	بسیار نزدیک به صفر
امتیاز کیفیت	۰.۹۷۷۵	۰.۹۵۰۰	بسیار مطلوب

مقدار آنتروپی برابر با ۷.۹۹۹۲ به دست آمد که نشان دهنده تصادفی بودن بالای تصویر رمز شده و نزدیکی کامل به مقدار ایده آل (۸.۰۰۰۰) است. NPCR با مقدار ۹۹.۶۰ درصد بسیار نزدیک به آستانه‌ی ایده آل ۹۹.۶۰ درصد قرار دارد و نشان دهنده حساسیت بسیار بالای روش به تغییرات پیکسل است. UACI با مقدار ۳۷.۱۷ درصد بالاتر از حد ایده آل (۳۳.۳۳ درصد) قرار دارد که نشان دهنده قدرت انتشار بیشتر در روش پیشنهادی است و آن را در برابر حملات تفاضلی مقاوم تر می سازد. ضریب همبستگی افقی با مقدار ۰.۰۰۰۱ بسیار نزدیک به صفر است که بیانگر عدم وجود همبستگی معنادار بین پیکسل های مجاور در تصویر رمز شده می باشد. امتیاز کیفیت ترکیبی با مقدار ۰.۹۷۷۵ نشان دهنده عملکرد عالی روش در تمام معیارهای امنیتی است.

۵-۳-۵. تحلیل هیستوگرام

تحلیل هیستوگرام تصویر اصلی و تصویر رمز شده نشان داد که توزیع پیکسل ها در تصویر رمز شده به طور قابل توجهی یکنواخت تر از تصویر اصلی است. این یکنواختی با معیارهای کمی نظیر آنتروپی ۷.۹۹۹۱ و NPCR ۹۹.۶۲ درصد تأیید می شود که نشان دهنده موفقیت روش در مخفی سازی اطلاعات آماری تصویر اصلی است.

۵-۳-۶. تحلیل ضرایب همبستگی

تحلیل ضرایب همبستگی پیکسل های مجاور در سه جهت افقی، عمودی و قطبی برای تصویر اصلی و تصویر رمز شده در جدول ۵ ارائه شده است.

جدول ۵: ضرایب همبستگی پیکسل های مجاور

جهت	تصویر اصلی	تصویر رمز شده	کاهش
افقی	۰.۹۵۲۴	۰.۰۰۰۱	۹۹.۹۹٪
عمودی	۰.۹۷۴۷	۰.۰۰۰۱	۹۹.۹۹٪
قطری	۰.۹۲۴۳	۰.۰۰۰۲	۹۹.۹۸٪

مقادیر ضرایب همبستگی در تصویر اصلی در هر سه جهت بالای ۰.۹ بوده و نشان دهنده همبستگی قوی بین پیکسل های مجاور است. پس از اعمال رمزنگاری، ضرایب همبستگی در هر سه جهت به مقادیر نزدیک به صفر (کمتر از ۰.۰۰۰۲) کاهش یافته است. میانگین کاهش همبستگی در سه جهت حدود ۹۹.۹۹ درصد بوده که بیانگر موفقیت کامل روش در شکستن همبستگی مکانی پیکسل هاست. این بهبود نسبت به روش های مشابه (که معمولاً به همبستگی حدود ۰.۰۰۱-۰.۰۰۵ می رسند) قابل توجه است.

۵-۳-۷. تحلیل حساسیت به کلید

آزمایش حساسیت به کلید با تغییر 10^{-14} در مقدار اولیه جریان کلید انجام شد. نتایج نشان داد که NPCR بین دو تصویر رمز شده با کلیدهای اصلی و تغییر یافته برابر با ۹۹.۶۴ درصد است که نشان دهنده حساسیت بالای روش به تغییرات کلید می باشد.

این مقدار NPCR بالاتر از آستانه‌ی استاندارد (۹۹.۶۰٪) قرار دارد و نشان می‌دهد که تغییر بسیار کوچک در کلید (10^{-14})، بیش از ۹۹.۶۴ درصد از پیکسل‌های تصویر رمز شده را تغییر می‌دهد. این ویژگی، روش را در برابر حملات جستجوی کلید و تحلیل تفاضلی مقاوم می‌سازد و یکی از الزامات اصلی یک الگوریتم رمزنگاری امن محسوب می‌شود.

۵-۳-۸. تحلیل مقاومت در برابر حملات برش

مقاومت روش پیشنهادی در برابر حملات برش با حذف درصدهای مختلف (۱۰٪، ۲۵٪، ۵۰٪ و ۷۵٪) از تصویر رمز شده و سپس رمزگشایی آن مورد ارزیابی قرار گرفت. نتایج در جدول ۷ گزارش شده است.

جدول ۷: نتایج آزمایش مقاومت در برابر حملات برش

درصد برش	SSIM	PSNR (dB)
۱۰٪	۰.۸۲۹۰	۲۱.۰۵
۲۵٪	۰.۷۵۲۸	۱۴.۳۰
۵۰٪	۰.۶۸۳۲	۱۲.۶۳
۷۵٪	۰.۰۱۷۹	۷.۴۱

همان‌طور که مشاهده می‌شود، روش پیشنهادی تا ۵۰٪ برش عملکرد قابل‌قبولی دارد و تصویر رمزگشایی شده همچنان ساختار اصلی خود را حفظ می‌کند. (SSIM=0.6832) در برش ۷۵٪، کیفیت تصویر به شدت کاهش می‌یابد که در اکثر روش‌های رمزنگاری طبیعی است، زیرا تنها ۲۵ درصد از اطلاعات اصلی باقی می‌ماند. این نتایج نشان می‌دهد که مکانیزم انتشار در روش پیشنهادی به‌خوبی عمل کرده و اطلاعات تصویر را در سراسر پیکسل‌ها پخش می‌کند.

۵-۳-۹. تحلیل مقاومت در برابر حملات نویز

مقاومت روش پیشنهادی در برابر سه نوع نویز رایج (نمک و فلفل، گاوسی و اسپکل) با شدت‌های مختلف مورد ارزیابی قرار گرفت. نتایج در جدول ۸ گزارش شده است.

جدول ۸: نتایج آزمایش مقاومت در برابر حملات نویز

نوع نویز	شدت	SSIM	PSNR (dB)
نمک و فلفل	۱٪	۰.۴۹۸۳	۱۹.۵۷
نمک و فلفل	۵٪	۰.۲۰۴۶	۱۳.۱۱
نمک و فلفل	۱۰٪	۰.۱۲۱۶	۱۰.۵۸
گاوسی	۰.۰۱٪	۰.۰۰۶۰	۶.۹۱
گاوسی	۰.۰۵٪	۰.۰۰۶۰	۶.۹۱

۶.۹۱	۰.۰۰۶۰	۰.۱٪	گاوسی
۶.۹۱	۰.۰۰۶۰	۰.۰۱٪	اسپکل
۶.۹۱	۰.۰۰۶۰	۰.۰۵٪	اسپکل
۶.۹۱	۰.۰۰۶۰	۰.۱٪	اسپکل

نتایج نشان می‌دهد که روش پیشنهادی در برابر نویز نمک و لفل مقاومت خوبی دارد، به گونه‌ای که در شدت ۱٪، PSNR برابر با ۱۹.۵۷ دسی‌بل و SSIM برابر با ۰.۴۹۸۳ به دست آمده است. با افزایش شدت نویز به ۱۰٪، کیفیت کاهش می‌یابد اما تصویر همچنان قابل تشخیص است. در برابر نویزهای گاوسی و اسپکل، عملکرد روش ضعیف‌تر است که این محدودیت در بسیاری از روش‌های رمزنگاری مبتنی بر آشوب مشاهده می‌شود. با این حال، مقادیر PSNR گزارش شده (۶.۹۱ dB) با روش‌های مشابه قابل مقایسه است و می‌تواند به عنوان یک جهت برای پژوهش‌های آینده در نظر گرفته شود.

۵-۳-۱۰. تحلیل فضای کلید

فضای کلید روش پیشنهادی با ترکیب پارامترهای سیستم فوق آشوبی (۷ پارامتر اولیه با دقت 10^{-14})، پارامترهای مربع جادویی و کلیدهای اختصاصی هر دور محاسبه گردید. فضای کلید کل برابر با 2^{700} به دست آمد که به طور قابل توجهی از آستانه‌ی استاندارد 2^{100} فراتر است. این فضای کلید وسیع، حملات جستجوی فراگیر را به طور مؤثر دفع می‌کند و امنیت بلندمدت روش را در برابر حملات جستجوی فراگیر تضمین می‌نماید.

۵-۳-۱۱. تحلیل زمان اجرا

زمان اجرای مراحل مختلف روش پیشنهادی بر روی تصویر 256×256 در جدول ۹ گزارش شده است.

جدول ۹: زمان اجرای مراحل مختلف روش پیشنهادی

مرحله	زمان (ثانیه)	درصد از کل
تولید S-Box پویا	۰.۰۵۲	۱۴.۰۵٪
تولید جریان کلید فوق آشوبی	۰.۰۳۵	۹.۴۶٪
رمزنگاری تصویر (۳ دور)	۰.۲۸۰	۷۵.۶۸٪
ماسک‌سازی و فشرده‌سازی	۰.۰۰۳	۰.۸۱٪
کل زمان	۰.۳۷۰	۱۰۰.۰۰٪

کل زمان اجرای روش برای یک تصویر 256×256 برابر با ۰.۳۷۰ ثانیه به دست آمد که برای کاربردهای بلادرنگ در سیستم‌های سلامت دیجیتال مناسب می‌باشد. بیشترین زمان اجرا مربوط به مرحله‌ی رمزنگاری تصویر با ۰.۲۸۰ ثانیه (۷۵.۶۸ درصد از کل زمان) بوده است.

۵-۳-۱۲. تحلیل فشرده سازی CRT

کارایی مکانیزم فشرده سازی مبتنی بر قضیه باقیمانده چینی (CRT) در جدول ۱۰ گزارش شده است.

جدول ۱۰: نسبت فشرده سازی CRT برای مقادیر مختلف پارامتر k

پارامتر k	حجم اصلی	حجم فشرده	نسبت فشرده سازی	کاهش حجم
۳	۴۹۳,۶۴۸	۱۸۵,۱۱۸	۰.۳۷۵۰	۶۲.۵۰٪
۵	۴۹۳,۶۴۸	۳۰۸,۵۳۰	۰.۶۲۵۰	۳۷.۵۰٪

نسبت فشرده سازی برای $k=3$ برابر با ۰.۳۷۵ به دست آمد که به معنی کاهش ۶۲.۵۰ درصدی حجم داده های انتقالی است. این قابلیت فشرده سازی، روش را برای کاربردهای اینترنت اشیا پزشکی که در آن پهنای باند محدود است، ایده آل می سازد.

۵-۳-۱۳. انتخاب بهترین مدل

پس از اتمام ۵ دور آموزشی، مدل های $G1$ ، $G2$ و $G4$ با کسب امتیاز ۱.۰۰۰۰ به عنوان بهترین مدل ها شناخته شدند که از میان آنها مدل $G1$ به عنوان بهترین مدل جهانی انتخاب شد. جدول ۱۱ عملکرد نهایی مدل ها را نشان می دهد.

جدول ۱۱: امتیاز نهایی مدل های جهانی

رتبه	امتیاز نهایی	مدل
۱	۱.۰۰۰۰	$G1$
۱	۱.۰۰۰۰	$G2$
۱	۱.۰۰۰۰	$G4$
۴	۰.۹۶۶۷	$G3$
۵	۰.۹۶۶۶	$G5$

سه مدل $G1$ ، $G2$ و $G4$ به امتیاز نهایی ۱.۰۰۰۰ دست یافتند که مدل $G1$ به عنوان بهترین مدل انتخاب شد. مدل های $G3$ و $G5$ با امتیازهای ۰.۹۶۶۷ و ۰.۹۶۶۶ در جایگاه های بعدی قرار گرفتند.

۵-۵. مقایسه با روش های موجود

جدول ۱۲ مقایسه جامع روش پیشنهادی با سایر روش های مرتبط را نشان می دهد.

جدول ۱۲: مقایسه با روش های موجود

Fed-Ms-Crypt	Inam.et al[20]	Fan.etal[10]	Subathra.etal[18]	Roy.etal[12]	معیار
--------------	----------------	--------------	-------------------	--------------	-------

✓	×	✓	×	✓	یادگیری فدرال
✓	✓	×	✓	✓	رمزنگاری فوق آشوبی
✓	✓	×	×	✓	S-Box پویا
✓	×	✓	×	×	مربع جادویی
✓	×	✓	×	×	فشرده سازی CRT
✓	×	×	×	✓	معماری چند مدلی
✓	×	×	×	✓	شناسایی مخرب ها
۷.۹۹۹۲	۷.۹۹۹۸	-	۷.۹۹۷۱	-	آنتروپی
۹۹.۶۰	۹۹.۹۲	-	۹۹.۶۱	-	NPCR
-۰.۰۰۰۱	-	-	-۰.۰۰۱۸	-	همبستگی

مشاهده می شود که روش پیشنهادی Fed-MS-Crypt در همبستگی مکانی و در حساسیت به کلید عملکردی بهتر ارائه می دهد. همچنین، این روش تنها روشی است که به طور هم زمان از تمام مؤلفه های کلیدی (FL، فوق آشوب، S-Box پویا، مربع جادویی، CRT و معماری چندمدلی) در یک چارچوب یکپارچه استفاده کرده است.

۶. نتیجه گیری

در این مقاله، یک چارچوب رمزنگاری ترکیبی نوآورانه به نام Fed-MS-Crypt برای حفظ محرمانگی تصاویر پزشکی در محیط های یادگیری فدرال ارائه گردید. روش پیشنهادی با ادغام قابلیت تولید S-Box پویا توسط ویژگی های بافتی تصویر، تولید جریان کلید فوق آشوبی با ترکیب دو سیستم آشوبی، ماسک سازی گرادیان با مربع جادویی و فشرده سازی با قضیه باقیمانده چینی، توانست محرمانگی دوگانه در سطح تصویر و گرادیان ایجاد کند. این ویژگی منجر به افزایش امنیت رمزنگاری و جلوگیری از نشت اطلاعات در فرآیند یادگیری فدرال شد. نتایج شبیه سازی نشان داد که رویکرد پیشنهادی در مقایسه با روش های مورد مقایسه، عملکرد بهتری از نظر آنتروپی (۷.۹۹۹۲)، NPCR (۹۹.۶۰ درصد) و ضریب همبستگی (۰.۰۰۰۱) دارد که نشان دهنده بهبود چشمگیر در شکستن همبستگی مکانی پیکسل ها است. همچنین مکانیزم شناسایی کلاپنت های مخرب با آستانه گذاری β ، توانست ۶ کلاپنت از ۱۰ کلاپنت را در دور اول شناسایی و حذف کند که بیانگر کارایی بالای روش در مقابله با حملات مسموم سازی است. استفاده از مربع جادویی به عنوان مکانیزم ماسک سازی سبک وزن، موجب افزایش کارایی الگوریتم در دستگاه های با منابع محدود و کاهش حجم داده های انتقالی تا ۶۲.۵ درصد شده است.

به طور کلی، نتایج این مطالعه نشان می دهد که ترکیب روش های رمزنگاری فوق آشوبی با یادگیری فدرال و ماسک سازی مربع جادویی می تواند مسیر مؤثری برای تأمین امنیت و حریم خصوصی در سیستم های سلامت دیجیتال و همکاری بین بیمارستانی فراهم کند. به عنوان کارهای آینده، می توان توسعه مدل در محیط های اینترنت اشیا پزشکی، استفاده از سیستم های فوق آشوبی کسری مرتبه برای افزایش فضای کلید، و به کارگیری رویکردهای مبتنی بر بلاک چین برای ثبت غیر قابل تغییر تراکنش ها را مورد بررسی قرار داد.



مراجع

۱. Preethi, S. and K. Manoharan. *Analysis of Deep Learning Based Secure and Robust System for the Renovation of Medical Images on IoMT*. in 2025 International Conference on Computing and Communication Technologies (ICCCT). 2025. IEEE.
۲. Emin, B., et al. *Biomedical Data Security Using a Hybrid Encryption Approach Based on Fractional-Order Hyper-Chaotic Systems and DNA Coding*. IFAC-PapersOnLine, 2025. **59**(37): p. 215–219.
۳. Mu, J., et al., *Explainable federated medical image analysis through causal learning and blockchain*. IEEE journal of biomedical and health informatics, 2024. **28**(6): p. 3206–3218.
۴. Nazir, S. and M. Kaleem, *Federated learning for medical image analysis with deep neural networks*. Diagnostics, 2023. **13**(9): p. 1532.
۵. Muthalakshmi, M., et al. *Federated learning for secure and privacy-preserving medical image analysis in decentralized healthcare systems*. in 2024 5th international conference on electronics and sustainable communication systems (ICESC). 2024. IEEE.
۶. Sandhu, S.S., et al., *Medical imaging applications of federated learning*. Diagnostics, 2023. **13**(19): p. 3140.
۷. Sharma, H. and S. Kaur, *Quantum-Inspired Hyperchaotic Bio-DNA Image Encryption for Real Time Medical Security*. IEEE Access, 2025.
۸. Guitouni, Z. and H.M. Zayani, *Quantum chaotic techniques for medical image encryption in next-generation IoMT applications*. The Journal of Supercomputing, 2025. **81**(9): p. 1070.
۹. Demirkol, A.S., et al., *Real time hybrid medical image encryption algorithm combining memristor-based chaos with DNA coding*. Chaos, Solitons & Fractals, 2024. **183**: p. 114923.
۱۰. Fan, Y., T. Zhou, and W. Zheng, *A privacy-enhanced federated learning scheme via magic squares: Y. Fan et al.* The Journal of Supercomputing, 2026. **82**(2): p. 48.
۱۱. Karmouni, I., et al., *Enhanced image encryption with deep generative models using a self-attention mechanism*. Scientific Reports, 2026. **16**(1): p. 11200.
۱۲. Roy, A., D.R. Mahanta, and L.B. Mahanta, *A semi-synchronous federated learning framework with chaos-based encryption for enhanced security in medical image sharing*. Results in Engineering, 2025. **25**: p. 103886.
۱۳. Zhuang, Z., Z. Zhuang, and T. Wang, *Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition*. Scientific Reports, 2024. **14**(1): p. 402.
۱۴. Li, M., et al., *Medical image encryption algorithm based on hyper-chaotic system and DNA coding*. Cognitive Computation and Systems, 2022. **4**(4): p. 378–390.
۱۵. Liu, Y., et al., *A dynamic AES cryptosystem based on memristive neural network*. Scientific Reports, 2022. **12**(1): p. 12983.
۱۶. Wang, X., et al., *A New V-Net Convolutional Neural Network Based on Four-Dimensional Hyperchaotic System for Medical Image Encryption*. Security and Communication Networks, 2022. **2022**: p. 4260804.
۱۷. Yang, N., et al., *Medical image encryption based on Josephus traversing and hyperchaotic Lorenz system*. Journal of Shanghai Jiaotong University (Science), 2024. **29**(1): p. 91–108.
۱۸. Subathra, S. and V. Thanikaiselvan, *Enhanced security for medical images using a new 5D hyper chaotic map and deep learning based segmentation*. Scientific Reports, 2025. **15**(1): p. 22628.
۱۹. Andreatos, A.S. and A.P. Leros, *Secure Chaotic Cryptosystem for 3D Medical Images*. Mathematics, 2025. **13**(2): p. 3310.
۲۰. Inam, S., et al., *A blockchain-integrated chaotic fractal encryption scheme for secure medical imaging in industrial IoT settings*. Scientific Reports, 2025. **15**(1): p. 7652.



۲۱. Samantray, B.S. and K.H.K. Reddy, *A Federated Learning Approach Towards Hybrid Blockchain, Quantum-Key-Encryption based Distributed System: A Futuristic Healthcare Architecture for Smart Cities*. Blockchain: Research and Applications, 2025: p. 100385.
۲۲. Amaithi Rajan, A., et al., *Secure and fault tolerant cloud based framework for medical image storage and retrieval in a distributed environment*. Scientific Reports, 2025. **15**(1): p. 32965.
۲۳. Mohammed, Z.A., et al., *BF2GAN: A Fused Federated Learning-Based Biometric Enabled Deep Learning Approach for Secure Medical Image Sharing in Cloud Environment*. Journal of Imaging Informatics in Medicine, 2026: p. 1–26.
۲۴. Guduri, M., et al., *Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records*. IEEE Transactions on Consumer Electronics, 2023. **70**(1): p. 2608–2617.
۲۵. Attieh, H.A., et al., *An exploratory survey study toward a conceptual framework for structuring the integration of privacy-enhancing technologies in federated learning and analytics*. IEEE Access. ۲۰۲۶ ,
۲۶. Chen, Y., et al., *MetaFed: Federated learning among federations with cyclic knowledge distillation for personalized healthcare*. IEEE Transactions on Neural Networks and Learning Systems, 2023. **35**(11): p. 16671–16682.
۲۷. Chowdhury, L., et al., *Privacy Preserved and Explainable Deep Medical Image Analysis: A Survey*. IEEE Transactions on Emerging Topics in Computational Intelligence, 2026.
۲۸. Wang, X., et al., *Securing federated learning with blockchain in the medical field: Systematic literature review*. Journal of Medical Internet Research, 2026. **28**: p. e79052.
۲۹. Ghosh, D., et al., *Advancements and challenges of federated learning in medical imaging: a systematic literature review*. Artificial Intelligence Review, 2026.
۳۰. Bakas, S., et al., *Federated Learning in Healthcare: From Research to Real-World Deployment*. Annual Review of Biomedical Engineering, 2026. **28**.
۳۱. Dolezel, D., et al., *AI Privacy and Security in Healthcare: A Systematic Literature Review*. International Journal of Telerehabilitation, 2026. **18**(1): p. 6747.
۳۲. Mir, B.A., S.R. Abbas, and S.W. Lee. *Federated Learning in Healthcare Ethics: A Systematic Review of Privacy-Preserving and Equitable Medical AI in Healthcare*. 2026. MDPI.
۳۳. Sohan, M.F. and A. Basalamah, *A systematic review on federated learning in medical image analysis*. IEEE Access, 2023. **11**: p. 28628–28644.
۳۴. Hernandez-Cruz, N., et al., *Review of federated learning and machine learning-based methods for medical image analysis*. Big Data and Cognitive Computing, 2 : (۹)۸ . ۰۲۴p. 99.
۳۵. Sun, M., et al., *Federated learning for large models in medical imaging: a comprehensive review*. arXiv preprint arXiv:2508.20414, 2025.
۳۶. da Silva, F.R., R. Camacho, and J.M.R. Tavares, *Federated learning in medical image analysis :A systematic survey*. Electronics, 2023. **13**(1): p. 47.