# توصیف کامل و جامع مقاله: چارچوب بازیابی امن تصاویر پزشکی SMedIR با индексینگ مبتنی بر ConvNeXt و رمزنگاری قابل جستجو در ابر

# SMedIR: secure medical image retrieval framework with ConvNeXt-based indexing and searchable encryption in the cloud

این مقاله با عنوان "SMedIR: secure medical image retrieval framework with ConvNeXt-based indexing and searchable encryption in the cloud" توسط نویسندگان Arun Amaithi Rajan، Vetriselvi V، Mayank Raikwar و Reshma Balaraman نوشته شده است. مقاله در سال ۲۰۲۴ در مجله Journal of Cloud Computing: Advances, Systems and Applications (جلد ۱۳، مقاله ۱۳۹) منتشر شده و دارای doi: https://doi.org/10.1186/s13677-024-00702-z است. این مقاله دسترسی باز (Open Access) دارد و تحت مجوز Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 منتشر شده است. مقاله بر روی امنیت و حریم خصوصی تصاویر پزشکی تمرکز دارد که به دلیل طبیعت حساس آن‌ها و عواقب احتمالی تغییرات غیرمجاز (مانند نقض داده‌ها و تشخیص‌های نادرست) حیاتی است. نویسندگان روشی برای بازیابی بدون از دست دادن تصاویر پزشکی رمزنگاری شده از ابرهای شخص ثالث پیشنهاد می‌کنند. رویکرد پیشنهادی از طرح رمزنگاری تصویر متقارن متمرکز بر یکپارچگی (با استفاده از نقشه‌های آشوب چندگانه و تکنیک‌های هش رمزنگاری) برای تضمین بازسازی تصویر بدون از دست دادن استفاده می‌کند. تصاویر پزشکی ابتدا توسط مالکان رمزنگاری شده و به هش‌کدهایی تبدیل می‌شوند که ویژگی‌های ضروری را با تکنیک هشینگ عمیق با شبکه ConvNeXt به عنوان backbone در حالت موازی encapsulation می‌کنند. برای تضمین حریم خصوصی индекс، این هش‌کدها به صورت قابل جستجو رمزنگاری می‌شوند. تصاویر رمزنگاری شده همراه با индекс امن به ذخیره‌سازی ابر آپلود می‌شوند. کاربران مجاز تصاویر پزشکی می‌توانند تصاویر مشابه برای اهداف تشخیصی درخواست کنند با ارسال تصویر پرس‌وجو، که از آن trapdoor جستجو تولید شده و به ابر ارسال می‌شود. فرآیند بازیابی شامل جستجوی امن تصاویر مشابه روی индексهای رمزنگاری شده، سپس رمزگشایی همراه با تأیید یکپارچگی تصاویر بازیابی‌شده است. روش پیشنهادی روی سه مجموعه داده پزشکی استاندارد آزمایش شده و بهبود ۵-۲۰٪ در دقت بازیابی نسبت به baselines استاندارد نشان می‌دهد. تحلیل امنیت رسمی و نتایج تجربی نشان می‌دهد که طرح پیشنهادی امنیت و دقت بازیابی بالاتری ارائه می‌دهد و راه‌حلی مؤثر برای ذخیره‌سازی رمزنگاری شده و بازیابی امن داده‌های تصاویر پزشکی است.

کلمات کلیدی: تصاویر پزشکی رمزنگاری شده، رمزنگاری تصویر متمرکز بر یکپارچگی، هشینگ عمیق، رمزنگاری قابل جستجو، جستجوی امن تصاویر مشابه.

چکیده (Abstract)

امنیت و حریم خصوصی تصاویر پزشکی به دلیل طبیعت حساس آن‌ها و عواقب احتمالی تغییرات غیرمجاز، از جمله نقض داده‌ها و تشخیص‌های نادرست، حیاتی است. این مقاله روشی برای بازیابی بدون از دست دادن تصاویر پزشکی رمزنگاری شده ذخیره‌شده در ابرهای شخص ثالث معرفی می‌کند. رویکرد پیشنهادی از طرح رمزنگاری تصویر متقارن متمرکز بر یکپارچگی، با استفاده از نقشه‌های آشوب چندگانه و تکنیک‌های هش رمزنگاری، برای تضمین بازسازی تصویر بدون از دست دادن استفاده می‌کند. تصاویر پزشکی ابتدا رمزنگاری شده و به هش‌کدهایی تبدیل می‌شوند که ویژگی‌های ضروری را با تکنیک هشینگ عمیق با شبکه ConvNeXt به عنوان backbone در حالت موازی encapsulation می‌کنند. برای تضمین حریم خصوصی индекс، این هش‌کدها به صورت قابل جستجو رمزنگاری می‌شوند. تصاویر رمزنگاری شده همراه با индекс امن به ذخیره‌سازی ابر آپلود می‌شوند. کاربران مجاز می‌توانند تصاویر مشابه برای اهداف تشخیصی درخواست کنند با ارسال تصویر پرس‌وجو، که trapdoor جستجو تولید شده و به ابر ارسال می‌شود. فرآیند بازیابی شامل جستجوی امن تصاویر مشابه روی индексهای رمزنگاری شده، سپس رمزگشایی همراه با تأیید یکپارچگی است. روش پیشنهادی روی سه مجموعه داده پزشکی استاندارد آزمایش شده و بهبود ۵-۲۰٪ در دقت بازیابی نسبت به baselines استاندارد نشان می‌دهد. تحلیل امنیت رسمی و نتایج تجربی نشان می‌دهد که طرح پیشنهادی امنیت و دقت بازیابی بالاتری ارائه می‌دهد و راه‌حلی مؤثر برای ذخیره‌سازی رمزنگاری شده و بازیابی امن داده‌های تصاویر پزشکی است.

مقدمه (Introduction)

در دهه‌های اخیر، پیشرفت‌های تصویربرداری پزشکی خدمات مراقبت‌های بهداشتی را به طور قابل توجهی بهبود بخشیده و پزشکان را قادر ساخته تا تصمیم‌گیری‌های آگاهانه‌تری در مورد تشخیص و درمان از طریق visualizations دقیق بگیرند. رشد نمایی حجم و پردازش داده‌های تصویربرداری پزشکی، همراه با نیاز به راه‌حل‌های ذخیره‌سازی مقیاس‌پذیر، منجر به ادغام فناوری ابر شده است. با وجود مزایا، ذخیره‌سازی تصاویر پزشکی مبتنی بر ابر ذاتاً قابل اعتماد نیست و ریسک‌های قابل توجهی مانند نقض داده‌ها، دسترسی غیرمجاز و دستکاری احتمالی ایجاد می‌کند که امنیت اطلاعات حساس بیمار، از جمله محرمانگی، یکپارچگی و دسترسی را به خطر می‌اندازد. برای کاهش این تهدیدها و حفظ اعتماد و یکپارچگی در ذخیره‌سازی تصاویر پزشکی مبتنی بر ابر، اقدامات امنیتی قوی و چارچوب‌های رعایت ضروری هستند.

رمزنگاری تصاویر پزشکی قبل از ذخیره در ابر برخی جنبه‌های ذخیره‌سازی امن را پوشش می‌دهد. با این حال، حتی تغییرات جزئی توسط افراد غیرمجاز در تصاویر رمزنگاری شده می‌تواند منجر به تشخیص‌های نادرست و درمان‌ها شود. روش‌های بازیابی سنتی برای بازیابی مبتنی بر محتوا امن (CBIR) تصاویر رمزنگاری شده ناکافی هستند، زیرا نمی‌توانند

تقاضاها برای بازیابی سریع و دقیق volumes بزرگ داده‌های تصاویر پزشکی رمزنگاری شده بدون نشت حریم خصوصی را برآورده کنند. بنابراین، نیاز به راه‌حل‌هایی وجود دارد که بازیابی کارآمد تصاویر پزشکی رمزنگاری شده را در حالی که حریم خصوصی را حفظ می‌کنند، امکان‌پذیر سازد. این نیاز به توسعه روش‌هایی دارد که تضمین کند تصاویر پزشکی به طور امن ذخیره و بازیابی شوند بدون هیچ از دست دادن اطلاعاتی وقتی در ابر شخص ثالث ذخیره می‌شوند.

طرح‌های رمزنگاری تصاویر پزشکی عمدتاً بر محرمانگی محتوا تأکید دارند. روش‌های موجود مقاومت در برابر حملات خاص مانند حملات آماری و دیفرانسیل را هنگام توسعه مدل‌های رمزنگاری جدید پوشش می‌دهند. با این حال، اگر کاربر مخرب هوشمند یا ابر سعی کند تصاویر رمزنگاری شده را در ذخیره‌سازی تغییر دهد، می‌تواند منجر به رمزگشایی نادرست و تشخیص شود. برخی طرح‌ها authentications مبتنی بر watermarking معرفی کرده‌اند، اما این رویکردها overhead محاسباتی اضافه می‌کنند. چالش باقی‌مانده در انجام این وظایف به طور کارآمد است. این می‌تواند با ادغام رمزنگاری تصویر متمرکز بر یکپارچگی حل شود، جایی که الگوریتم رمزنگاری ذاتاً تأیید یکپارچگی را تضمین می‌کند و نیاز به فرآیندهای خارجی را حذف می‌کند. این رویکرد باید در مناطق امن با استفاده از پایگاه‌های داده قابل اعتماد اجرا شود. با اجرای این طرح، رمزگشایی تصویر بدون از دست دادن با تمایز ciphertext امکان‌پذیر است، که از adversaries احتمالی جلوگیری می‌کند از یادگیری یا تغییر هر اطلاعاتی در مورد تصاویر پزشکی.

بازیابی امن تصاویر پزشکی از پایگاه‌های داده تصاویر رمزنگاری شده وظیفه حیاتی دیگری است که محرمانگی و جستجوپذیری را در ابر تضمین می‌کند. با این حال، اکثر روش‌های بازیابی ranked top-k موجود از کارایی محدود رنج می‌برند و ممکن است به طور ناخواسته مقادیر و توالی امتیازهای شباهت را به سرور ابر آشکار کنند. این آشکارسازی ریسک ایجاد می‌کند، زیرا سرور ابر مخرب می‌تواند ترجیحات کاربر را استنتاج کند و محتوای تصویر مشابه‌ترین را بر اساس این امتیازهای شباهت پیش‌بینی کند اگر به اطلاعات پس‌زمینه کاربر از طریق روش‌های غیرقانونی دسترسی پیدا کند. بنابراین، هم کارایی و هم امنیت индекс نیاز به بهبود در زمینه بازیابی امن مبتنی بر محتوای تصاویر پزشکی (CBMIR) دارد. در حالی که برخی روش‌ها برای تولید هش‌کد کارآمد وجود دارد، اغلب در دقت وقتی برای индекسینگ امن رمزنگاری می‌شوند، کوتاهی می‌کنند. اخیراً، ConvNeXt عملکرد برتر در استخراج ویژگی نسبت به دیگر مدل‌های یادگیری عمیق نشان داده و آن را مناسب برای تولید هش‌کد کارآمد می‌کند. برای بهبود حریم خصوصی индекс و جستجو، این هش‌کدها قابل جستجو و رمزنگاری شده‌اند.

همانطور که بحث شد، سیستم‌های CBMIR امن موجود دقت بازیابی پایین، ریسک بالای آشکارسازی индекс به کاربران یا ابرهای مخرب، و مدل‌های رمزنگاری تصویر کمتر محافظ نشان می‌دهند. برای حل این مسائل در ذخیره‌سازی

و بازیابی تصاویر پزشکی از دیدگاه‌های امنیت و عملکرد، یک سیستم بازیابی امن تصاویر پزشکی نوین (SMedIR) در ابر پیشنهاد شده که شامل طرح‌های رمزنگاری تصویر متمرکز بر یکپارچگی و индекс‌ینگ امن است. شکل ۱ overview سطح بالا از SMedIR پیشنهادی در ابر را ارائه می‌دهد. کمک‌های اصلی این مقاله عبارتند از:

۱. چارچوب بازیابی امن و کارآمد تصاویر پزشکی نوین (SMedIR) پیشنهاد شده.
۲. طرح رمزنگاری تصویر متمرکز بر یکپارچگی برای ذخیره امن تصاویر پزشکی معرفی شده که رمزگشایی بدون از دست دادن را تضمین می‌کند.
۳. روش هشینگ عمیق مبتنی بر ConvNeXt برای استخراج هش‌کدهای حفظ‌کننده شباهت معنادار برای индекс‌ینگ استفاده شده که با طرح رمزنگاری قابل جستجو پیشنهادی رمزنگاری می‌شوند.
۴. تحلیل امنیت رسمی چارچوب SMedIR در TERMS حریم خصوصی индекс، حریم خصوصی پرس‌وجو، حریم خصوصی جستجو، و امنیت تصویر ارائه شده.
۵. یافته‌های تجربی نشان می‌دهد که تکنیک پیشنهادی امنیت بالاتر و کارایی بازیابی بهتر نسبت به مدل‌های baseline موجود دارد.

بقیه مقاله به این صورت ساختاربندی شده: کارهای مرتبط در بخش کارهای مرتبط گردآوری شده. چارچوب پیشنهادی و مقدماتی آن در بخش معماری سیستم ارائه شده. علاوه بر این، بخش تحلیل امنیت و حریم خصوصی تحلیل نظری دقیق امنیت و حریم خصوصی چارچوب پیشنهادی را ارائه می‌دهد. نتایج تجربی و تحلیل عملکرد بازیابی به طور گسترده در بخش نتایج تجربی و تحلیل عملکرد بحث شده. در نهایت، کار پیشنهادی در بخش نتیجه‌گیری نتیجه‌گیری شده.

کارهای مرتبط (Related Works)

در این بخش، نویسندگان overview از تکنیک‌های رمزنگاری تصویر امن موجود و سیستم‌های بازیابی تصویر امن ارائه می‌دهند.

**تکنیک‌های رمزنگاری تصویر امن (Secure Image Encryption Techniques):** رمزنگاری تصویر تکنیکی است که تصویر محرمانه را با استفاده از روش رمزنگاری کدگذاری می‌کند تا فقط افراد مجاز بتوانند به آن دسترسی پیدا کنند. این تکنیک برای بازیابی امن تصویر حیاتی است، زیرا تصاویر به صورت رمزنگاری شده با индекс امن در ابر ذخیره می‌شوند. طرح‌های رمزنگاری تصاویر پزشکی عمدتاً بر محرمانگی محتوا تأکید دارند. روش‌های موجود مقاومت در برابر حملات خاص مانند حملات آماری و دیفرانسیل را پوشش می‌دهند. برخی authentications

مبتنی بر watermarking معرفی کرده‌اند، اما overhead اضافه می‌کنند. نویسندگان تکنیک‌های مختلف مانند استفاده از نقشه‌های آشوب، هش رمزنگاری، و طرح‌های متقارن را بررسی می‌کنند.

**سیستم‌های بازیابی تصویر امن (Secure Image Retrieval Systems):** سیستم‌های CBIR و CBMIR امن برای بازیابی تصاویر مشابه از پایگاه‌های داده رمزنگاری شده بررسی شده. چالش‌ها شامل دقت پایین، نشت حریم خصوصی، و کارایی محدود است. روش‌های هشینگ عمیق، رمزنگاری قابل جستجو، و مدل‌های یادگیری عمیق مانند ConvNeXt بحث شده. نویسندگان به کمبودها مانند عدم تمرکز بر یکپارچگی و امنیت индекс اشاره می‌کنند.

معماری سیستم (System Architecture)

چارچوب SMedIR شامل اجزای اصلی مانند مالک تصویر، کاربر مجاز، و سرور ابر است. مقدماتی شامل نقشه‌های آشوب برای رمزنگاری، ConvNeXt برای هشینگ، و رمزنگاری قابل جستجو برای индексینگ. فرآیند شامل رمزنگاری تصویر، تولید هش‌کد، رمزنگاری индекс، آپلود به ابر، تولید trapdoor جستجو، جستجوی امن، رمزگشایی و تأیید یکپارچگی است. شکل ۱ سیستم را نشان می‌دهد.

تحلیل امنیت و حریم خصوصی (Security and Privacy Analysis)

تحلیل رسمی نشان می‌دهد که SMedIR حریم خصوصی индекс، پرس‌وجو، جستجو و امنیت تصویر را تضمین می‌کند. از مدل‌های تهدید مانند ابر honest-but-curious استفاده شده. اثبات‌ها بر اساس سختی مشکلات محاسباتی مانند DDH ارائه شده.

نتایج تجربی و تحلیل عملکرد (Experimental Results and Performance Analysis)

آزمایش‌ها روی سه مجموعه داده پزشکی استاندارد (مانند ChestX-ray، CT Emphysema، و Diabetic Retinopathy) انجام شده. معیارها شامل mAP، دقت، recall، و زمان محاسباتی. SMedIR بهبود ۵-۲۰٪ در دقت نسبت به baselines مانند DSH، HashNet، و CSQ نشان می‌دهد. تحلیل overhead محاسباتی و امنیت تجربی نیز ارائه شده.

نتیجه‌گیری (Conclusion)

SMedIR راه‌حلی نوین برای ذخیره‌سازی و بازیابی امن تصاویر پزشکی در ابر ارائه می‌دهد. کارهای آینده شامل گسترش به ویدیوهای پزشکی و ادغام با بلاکچین است.

این توصیف جامع بر اساس محتوای کامل مقاله است و تمام بخش‌ها را پوشش می‌دهد. اگر جزئیات خاصی نیاز دارید، مشخص کنید.