یک طرح حفاظت از امنیت محتوا در حوزه فشرده شده JPEG

چکیده

راحتی دسترسی و توزیع شبکه های عمومی, یک تهدید امنیتی محتوای قابل توجه را در هنگام ارسال، دریافت و استفاده از اطلاعات چند رسانه ای باز نموده است. در این مقاله، یک طرح حفاظت از امنیت محتوا که رمزگذاری و انگشت نگاری دیجیتال را ادغام می کند, برای فراهم آوردن حفاظت امنیتی جامع برای اطلاعات چند رسانه ای در زمان انتقال و استفاده از آن پیشنهاد شده است. در مقابل طرح های دیگر، این روش در حوزه JPEG فشرده بدون کدگذاری یا فشرده سازی پیاده سازی می شود، بنابراین، این طرح برای اطلاعات چند رسانه ای که به ندرت در یک فرم غیر فشرده در دسترس است, بسیار کارآمد و مناسب می باشد. علاوه بر این، یک روش رمزگذاری مدولار متغیر برای حل مسئله کدنویسی نامعتبر با طول متغیر (VLC) پیشنهاد می شود, در هنگامی که یک جریان فشرده از داده ها به طور مستقیم رمزگذاری می شود. نتایج تجربی, بهبود امنیت و بهره وری ارائه شده توسط طرح پیشنهادی را اثبات می نمایند. آزمایشات نیز مقاومت آثار انگشت در برابر غیرقابل مشاهده بودن و تبانی را نیز اثبات نموده اند.

کلید واژه ها: امنیت محتوا، حوزه فشرده شده، رمزگذاری، اثر انگشت، انطباق با فرمت، کد نویسی با طول متغیر، نگاشت فضایی، جریان داده های فشرده شده

1. مقدمه

با توسعه سریع فن آوری های اطلاعات و ارتباطات، توزیع اطلاعات چند رسانه ای از طریق اینترنت, به امری عادی تبدیل شده است. با این حال، این راحتی دسترسی و توزیع داده ها در هنگام ارسال و دریافت اطلاعات حساس و تصاویر موجب افزایش خطرات امنیتی می شود. استراق سمع، نسخه برداری غیر مجاز، و انتشار یک تهدید در حال رشد است که باید به طور موثر رسیدگی شود. در برخی موارد، بروز و نشت این اطلاعات باعث آسیب به حریم خصوصی شخصی و یا حتی امنیت ملی می شود. بنابراین، اقدامات امنیتی محتوای موثر باید برای تضمین ایمنی اطلاعات حساس و یا اختصاصی چند رسانه ای اتخاذ شوند.

دو الزام باید به منظور تضمین امنیت اطلاعات چند رسانه ای، محرمانه بودن و استفاده صحیح [1،2،26] برآورده شوند. رمزگذاری, یک روش معمول برای اطمینان از محرمانه بودن اطلاعات است، اما امنیت داده ها پس از رمزگشایی را نمی تواند تضمین نمود زیرا داده ها را می توان کپی نمود و به طور نادرست به کاربران قانونی توزیع کرد. انگشت نگاری, یک تکنولوژی در حال ظهور است که به طور غیرقابل مشاهده یک شماره شناسایی منحصر به فرد وابسته به کاربر را در محتوای رسانه تعبیه می کند. اگر کاربران توزیع داده را به طور نادرست انجام دهند، اثرات انگشت پنهان را می توان از رسانه های کپی شده استخراج نمود و برای ردیابی کاربران غیر مجاز مورد استفاده قرار داد. اما، هنگام انگشت نگاری داده های دیجیتال، مشکل حملات تبانی باید در نظر گرفته شوند [3]. تبانی کنندگان, نسخه های انگشت نگاری خود از داده ها را مقایسه می کنند, تفاوت ها را تغییر می کنند و یک نسخه جدید را برای جلوگیری از کشف تولید می کنند. با این حال، انگشت نگاری دیجیتال, یک شکل منفعل امنیتی است و تنها پس از دریافت محتوا و دردسترس قرار گرفتن برای کاربر [4] کار می کند. بنابراین، تنها ترکیبی از رمزنگاری و انگشت نگاری می تواند حفاظت از امنیت محتوای جامع را برای اطلاعات چند رسانه ای فراهم کند، زیرا هر دوی محرمانه بودن و آسیب پذیری استفاده صحیح مورد بررسی قرار می گیرند.

چند هدف میانی باید به منظور برآورده سازی الزامات امنیتی در حفاظت محتوای اطلاعات چند رسانه ای به دست آیند که عبارتند از:

1. امنیت رمزنگاری. متفاوت از رمزگذاری متن / دودویی، رمزگذاری چند رسانه ای نیاز به هر دو امنیت رمزنگاری و امنیت ادراکی دارد [5]. امنیت رمزنگاری به امنیت در برابر حملات رمزنگاری اشاره می کند و امنیت ادراکی به این معنی است که محتوای چند رسانه ای رمزگذاری شده برای درک انسان ناخوانا است.

2. انطباق فرمت. اطلاعات فرمت پس از رمزگذاری داده های چند رسانه ای مانند هدرهای فایل و اطلاعات هماهنگ سازی تولید می شوند. این اطلاعات توسط دیکدر برای بازیابی موفق داده ها و برای هماهنگ نگهداشتن ارتباطات چند رسانه ای استفاده خواهند شد [5]؛ بنابراین، اطلاعات فرمت نباید توسط رمزنگاری تحت تاثیر قرار گیرند. متن

رمزی در صورتی سازگار با فرمت در نظر گرفته می شود که جریان داده های رمزگذاری شده را بتوان توسط یک دیکدر استاندارد رمزگشایی نمود.

3. غیرقابل مشاهده بودن. اطلاعات اثر انگشت تعبیه شده باید نامرئی باشد و تاثیر ادراکی کمی بر کیفیت تصویر داشته باشد.

4. مقاومت بودن در برابر حملات تبانی. کد اثر انگشت جاسازی شده باید در برابر حملات تبانی مستحکم باشند.

5. کارایی. عملیات های رمزگذاری و انگشت نگاری باید بسیار کارآمد باشند چرا که اطلاعات چند رسانه ای بزرگ است و تعداد کاربران بسیار بزرگ است. به طور گسترده ای اعتقاد بر اینست که اطلاعات ویدیویی باید به طور کارآمد به دلیل نرخ داده ها و اندازه بزرگ آن توزیع شوند. با این حال، برخی از اطلاعات تصویر نیز گسترده است [15]. برای مثال، یک تصویر سنجش از راه دور ابر طیفی معمولی که یک منطقه کوچک از چند کیلومتر را پوشش می دهد حاوی میلیون ها پیکسل است و هر پیکسل توسط گروههای مختلف [27] ارائه می شود. بنابراین، حجم داده ها می تواند چند گیگابایت و یا حتی چند صد گیگابایت [28] باشد.

6. نسبت فشردگی. در تمام موارد، الگوریتم های رمزنگاری چند رسانه ای نباید نسبت تراکم را تغییر دهند یا باید حداقل تغییرات را در یک محدوده کوچک [5] حفظ نمایند.

7. پیاده سازی حوزه فشرده شده. از آنجا که اکثر سیگنال های چند رسانه ای در یک فرم فشرده در دسترس هستند، رمزگذاری و تعبیه اثرات انگشت به طور مستقیم در جریان بیت رسانه های فشرده شده بدون هیچ آزادسازی, کدنویسی متقابل یا حتی نسخه های جزئی چنین محاسباتی [6-8،15] مطلوب است.

تحقیقات موجود در مورد حفاظت از امنیت محتوا برای اطلاعات چند رسانه ای را می توان به سه نوع طبقه بندی نمود، اما روش های مورد بحث دارای کاستی های قابل توجهی هستند. نوع اول [3،24] اثر انگشت هر کاربر را در متن تعبیه می کند و سپس آن را به صورت جداگانه در سمت فرستنده رمز گذاری می کند که منجر به بهره وری پایین و مقیاس پذیری ضعیف می شود. نوع دوم, رمز گذاری داده ها را در سمت فرستنده انجام می دهد و اثرات انگشت را در سمت گیرنده با سخت افزار ضد-رشوه [9] و یا گره های شبکه اعتماد [10،23] تعبیه می کند. این راه

حل ها می توانند موجب صرفه جویی زیادی در زمان محاسبه و استفاده از پهنای باند شوند، اما اثبات شده است که آنها در کاربرد, اغلب ناامن و غیر قابل انعطاف هستند. نوع دیگری از راه حل ها, رمزگشایی و انگشت نگاری را در سمت گیرنده ادغام می کنند. Anderson یک طرح Chameleon [11] را پیشنهاد داد که داده های صوتی متن غیر فشرده را در منبع رمز گذاری می کند. کاربران مختلف, همان متن رمزی را با کلید های کمی متفاوت رمزگشایی می کنند و بیت های کم ارزش کمی متفاوت (LSB) را از داده های صوتی متن به دست می آورند. هر چند، این طرح بسیار کارآمد است و اثر انگشت در LSB, در برابر عملیات های پردازش سیگنال رایج مستحکم نیست. به منظور قراردادن واترمارک های طیف گسترده, Adelsbach و همکاران, یک طرح Chameleon اصلاح شده را پیشنهاد نمودند [1]. اما، این رویکرد هنوز هم تنها سیگنال های باند غیر فشرده را در نظر می گیرد. Celik و همکاران نیز طرح Chameleon را با استفاده از عملیات های جبری در طول رمزگذاری / رمزگشایی بهبود دادند و سپس واترمارک های طیف گسترده [25] مستحکم را تعبیه نمودند. این طرح را می توان برا هدایت رمزگشایی پیوسته و نهان نگاری روی تصاویر کوانتیده برداری اصلاح نمود [26]. Kundur و همکاران یک طرح انگشت نگاری و رمزگشایی پیوسته (JFD) [4] را پیشنهاد دادند که اجزای ادراکی مرتبط را توسط تقلا در سمت فرستنده رمز گذاری می کند و گیرنده ها تا حدی محتوای رسانه ها را به منظور به دست آوردن نسخه های انگشت نگاری شده رمزگشایی می نمایند. این طرح بسیار کارآمد است، اما معایبی نیز دارد. محتوای رمزگذاری شده رسانه از ادراک, امن نیست و مقاومت بودن در برابر حملات تبانی را نمی توان تایید کرد. Lemma و همکاران یک طرح را بر اساس رمزنگاری افزودنی ارائه نمودند [12]؛ امنیت ادراکی آن بهتر از [4] است، اما در برابر حملات رمزنگاری امن نیست. علاوه بر این، مقاوم بودن آن در برابر حملات تبانی, تمرکز این پژوهش نیست. Lian و همکاران یک طرح بهبود یافته را در [13،14] پیشنهاد نمودند که در آن محتوای رسانه توسط مدولاسیون افزودنی رمزگذاری شده است. یک ویدئوی-رمزی توسط دمدولاسیون قابل کنترل توسط کدهای اثر انگشت رمزگشایی شد. اگر چه این روش ها می توانند بسیاری از الزامات مورد نیاز برای حفاظت از محتوای اطلاعات چند رسانه ای را برآورده نمایند، آنها در یک محیط " حوزه به شدت فشرده شده " پیاده سازی نمی شوند. بسیاری از این روش ها را می توان تا حدی از حالت

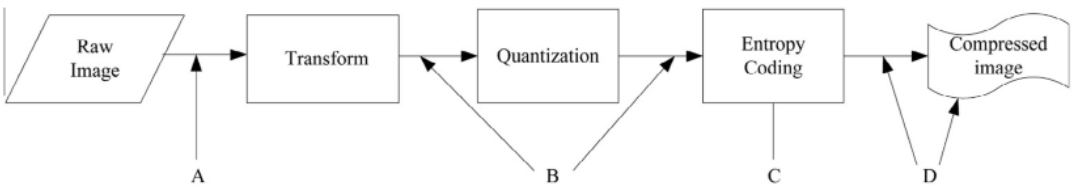
فشرده درآورد تا دسترسی به ضرایب تبدیل حاصل شود به طوری که آنها روش های حوزه به شدت فشرده [15] نیستند. تنها یک روش حوزه واقعی فشرده شده پیشنهاد شده است [16]؛ با این حال، این روش نیز دارای برخی از مشکلات است، زیرا امنیت رمزنگاری آن ثابت نشده است، متن رمزی آن را نمی توان با فرمت سازگار نگه داشت، و مقاوم بودن آن در برابر حملات تبانی آزمایش نشده است.

JPEG یک استاندارد فشرده سازی چند رسانه ای است که به طور گسترده ای استفاده می شود. یک طرح حفاظت از امنیت محتوای جدید برای حوزه فشرده شده JPEG در این مقاله پیشنهاد شده است. یک روش رمزگذاری متغیر-مدولار بر اساس نقشه برداری فضایی برای رمزگذاری یک جریان داده فشرده به طور مستقیم مورد استفاده قرار می گیرد، به طوری که یک متن رمزی سازگار با فرمت حاصل می شود. یک تصویر انگشت نگاری شده منحصر به فرد به طور طبیعی برای هر کاربر با رمزگشایی جریان داده های رمزگذاری شده با کلید های مختلف رمزگشایی تولید می شود. در مقابل طرح های دیگر، این طرح در حوزه JPEG فشرده بدون تراکدنویسی و رفع فشردگی پیاده سازی می شود؛ به همین دلیل بسیار کارآمد و مناسب برای اطلاعات چند رسانه ای است که به ندرت در یک فرم غیر فشرده در دسترس هستند. نتایج تجربی, مزایای امنیتی طرح پیشنهادی، غیرقابل مشاهده بودن تعبیه اثر انگشت، و مقاوم بودن آن در برابر حملات تبانی را نشان می دهند.

سازماندهی این مقاله به شرح زیر است: بخش 2, بحث در مورد تحقیقات مرتبط، و بخش 3, پیشنهاد طرح ماست. بخش 4 نتایج تجربی و یک تجزیه و تحلیل عملکرد و بخش 5, نتایج را ارائه می کند.

2. پیش زمینه

معماری کلی برای فشرده سازی JPEG در شکل 1 نشان داده شده است. یک تصویر اصلی در ابتدا تبدیل و کوانتیده می شود. علاوه ضرایب کوانتیزه حاصل برای تشکیل یک جریان فشرده آنتروپی کدگذاری می شوند. با توجه به این فرآیند، مکان های رمزگذاری بالقوه به شرح زیر فهرست می شوند: (A) یک رمزگذاری داده خام؛ (B) رمزگذاری ضریب تبدیل شده, قبل یا بعد از کوانتیزاسیون. (C) رمزگذاری توسط کدگذاری آنتروپی؛ و (D) رمزگذاری جریان داده های فشرده شده. این مکان های رمزگذاری در شکل 1 نشان داده شده است.



تصویر خام تبدیل کوانتیزاسیون کدگذاری آنتروپی تصویر فشرده شده

شکل 1. موقعیت های پنهان سازی در فرایندهای کدگذاری فشرده سازی

در رمزنگاری داده های خام، داده های رسانه ها قبل از فشرده سازی رمزگذاری می شوند. از آنجا که عملیات رمزنگاری, روابط مجاور پیکسل های تصویر را تغییر می دهد، نسبت فشردگی را می توان تا حد زیادی کاهش داد و در نتیجه انطباق فرمت نمی تواند حفظ شود [17]. انواع رمزگذاری دوم و سوم, یک عملیات رمزگذاری را در طول فشرده سازی پیاده سازی می نمایند؛ این تکنیک ها وابسته به کدک هستند. از آنجا که روابط مجاورت ضرایب تبدیل توسط رمزگذاری تغییر می یابند، نسبت فشردگی نیز کاهش می یابد [18-19]. نوع چهارم, جریان داده های فشرده را به طور مستقیم با برخی از مزایای قابل توجه رمز گذاری می کند. این امنیت بهتر را فراهم می کند زیرا داده های فشرده تقریباً هیچ فزونی ندارند. نوع چهارم نیز کارآمدتر است چرا که طول متن کوتاه تر از هر نوع دیگر است. نسبت تراکم آن و انطباق با فرمت را می توان به راحتی حفظ نمود؛ و ادغام با سیستم های برنامه مختلف آسان تر است زیرا مستقل از کدک [20] است. این رویکرد, جهت جریان اصلی پژوهش در زمینه رمزگذاری رسانه های تصویری است.

انگشت نگاری دیجیتال نوع خاصی از نهان نگاری دیجیتال است و می توان آن را یا در یک حوزه مکانی و یا تبدیل تعبیه نمود. اطلاعات جاسازی در حوزه مکان دارای مشکل مقاوم بودن ناکافی در برابر عملیات های رایج مانند نویز مختصر و فشرده سازی است؛ بنابراین، تعبیه اثر انگشت ها در ضرایب انتخاب در حوزه تبدیل یک روش است که به طور گسترده ای استفاده می شود. با این حال، این عملیات به عنوان یک روش " حوزه به شدت فشرده شده " در نظر گرفته نمی شود و به بهره وری پایین منجر خواهد شد. از این رو, توسعه الگوریتم های نهان نگاری که به طور

کامل در حوزه فشرده شده هستند بسیار مطلوب است. تا به حال، چند روش برای تعبیه اطلاعات به طور مستقیم در جریان داده های فشرده شده [6-8،15] پیشنهاد شده است.

با توجه به این دلایل، می توان نتیجه گرفت که رمزگذاری و یا انگشت نگاری جریان داده های فشرده شده به طور مستقیم مناسب تر است چرا که بسیاری از سیگنال های چند رسانه ای شده در یک فرم فشرده منتقل و یا ذخیره می شوند. بهره وری بالا است, زیرا فشرده سازی زمان-محور یا فرآیندهای تراکدگذاری نیز اجتناب می شوند. با این حال، یک مسئله ناشی از عملیات روی یک جریان داده های فشرده به طور مستقیم, دشواری سازگار نگه داشتن آن با فرمت است. در استانداردهای فشرده سازی تصویر و ویدیویی، تبدیل و کوانتیزه کردن توسط یک فرآیند کد نویسی با طول متغیر (VLC) برای به دست آوردن یک نسبت فشرده سازی بالاتر دنبال می شوند. یک ویژگی مشخصه کلمه کد VLC اینست که طول آن متغیر است و فضای کلی کلمه کد اشغال نمی شود؛ به عبارت دیگر، مجموع یک کلمه کد VLCمعتبر n بیتی برابر با Vn نیست، و Vn, مجموع همه ترکیبات ممکن دوتایی n بیتی است. با گرفتن یک کلمه کد 3 بیتی برای مثال، 8 کلمه کد باینری مختلف در کل وجود دارد؛ با این حال، تنها 2 کلمه کد VLC معتبر هستند, به خصوص 100 و 101، که در منطقه خاکستری تیره در شکل 2 نشان داده شده است. عملیات رمزگذاری برای یک کلمه کد در واقع یک نگاشت از فضای متن p به فضای متن رمزی $c = E(p)$ است. به علت تصادفی بودن در عملیات رمزگذاری E()، یک کلمه کد متن معتبر به احتمال زیاد در یک موقعیت تصادفی در فضای متن رمزی نگاشته خواهد شد، که منطقه خاکستری تیره و خاکستری شفاف در شکل 2 نشان داده شده است. اگر یک کلمه کد متن معتبر به منطقه خاکستری شفاف نقشه برداری شود، آنگاه متن رمزی با نحو استاندارد فشرده سازی مطابقت نخواهد داشت و نمی تواند سازگار با فرمت نگه داشته شود.

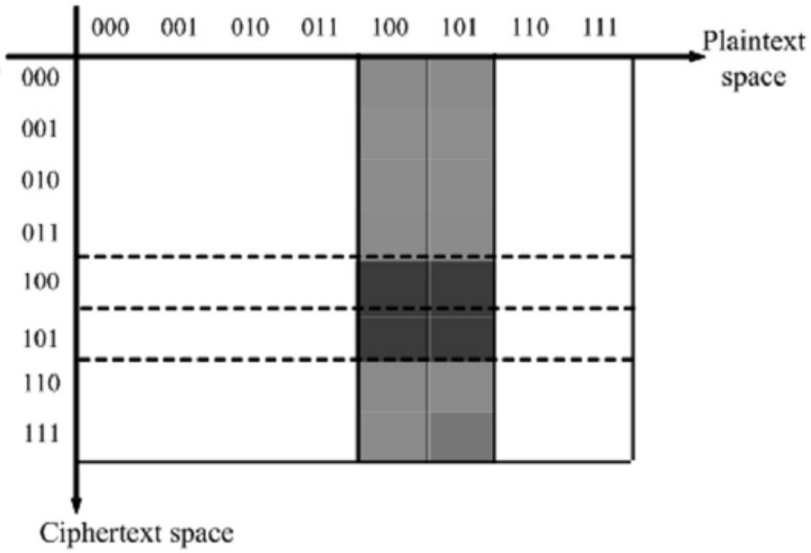
3. طرح پیشنهادی

این بخش, جزئیات روش حفاظت از امنیت محتوای پیشنهادی را بیان می کند که محدودیت های روش های موجود را حل. معماری عمومی طرح پیشنهادی در شکل 3 نشان داده شده است. در سمت چپ، تصویر X خام فشرده می شود و رمزنگاری مدولار متغیر در یک جریان داده فشرده در سمت فرستنده برای به دست آوردن یک فرمت متن

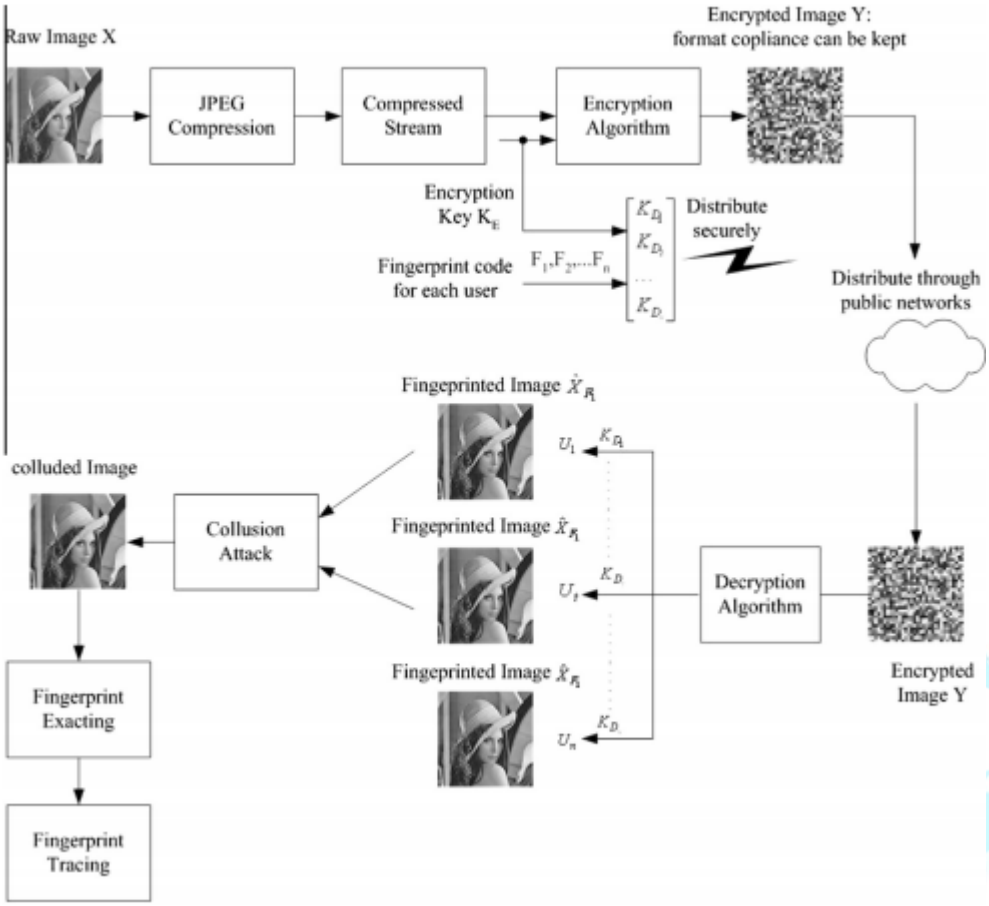
رمزی سازگار پیاده سازی می شود. در سمت راست پایین تر نمودار، کپی های انگشت نگاری شده توسط رمز گشایی متن رمزی با کلیدهای مختلف در کنار متقاضی تولید می شود. استخراج و تشخیص اثر انگشت در سمت چپ پایین تحلیل می شوند.

3.1. روش رمزگذاری مدولار متغیر بر اساس نقشه برداری فضایی

در فرایند کدگذاری JPEG، پس از کوانتیزاسیون، یک ضریب DC و 63 ضریب AC برای رمزگذاری آنتروپی آماده می شوند. برای ضریب DC، ضریب DC قبلاً کوانتیزه شده برای پیش بینی ضریب DC کوانتیزه شده کنونی استفاده می شود. اندازه تفاوت به عنوان یک کلمه کد VLC از بیت های CODELENGTH، پس از کد باینری بیت های SIZE برای دامنه کد گذاری می شود. برای ضرایب AC، یک مقدار ترکیبی برای توصیف طول اجرای ضرایب صفر (Run) و دامنه ضریب غیرصفر بعدی (Level) مورد استفاده قرار می گیرد؛ این Huffman کدگذاری شده به عنوان بیت های CODELENGTH VLC کلمه کد دنبال شده توسط کد باینری از بیت های SIZE برای دامنه است که دامنه ضریب را مشخص می کند. بنابراین، بدون در نظر گرفتن مقادیر برای ضرایب AC و DC، طول کلی جریان داده فشرده شده SIZE + TOTALLENGTH = CODELENGTH است.



شکل 2. نگاشت از فضای متن به فضای متن رمزی



شکل 3. معماری کلی طرح پیشنهادی

در ابتدا، جداول مختلف الفبایی ساخته می شوند: ما تمام کلمه کدهای VLC با طول یکسان را در یک جدول الفبایی قرار می دهیم و تعداد کلمه کدهای VLC را به صورت M ماژول آن تعریف می کنیم. جدول 1, شامل جداول القبایی متعدد می شود که برای ضرایب AC لومینانس مطابق با جدول K.5 در [21] ساخته می شوند؛ چون تنها یک کلمه کد VLC برای طول های کلی 3,4 و 5 وجود دارد, ما این سه کلمه کد را در یک جدول الفبایی قرار می دهیم.

فرض می کنیم که عنصر iام از جدول الفبایی متناظر با یک فضای مستقل V(i) است که از n نقطه تشکیل شده است, یعنی $V(i) = \{P(i+1)\cdots, P(i+n), \cdots\}$ برای جدول الفبایی دارای یک TOTALLENGTH, $n \in [1, 2^{SIZE}]$ ؛ در غیراینصورت $n \in [0, 2^{\text{MAXTOTAL- LENGTH} - \text{TOTALLENGTH} + \text{SIZE}}]$, که در آن

MAXTOTALLENGTH عنصر در جدول الفبایی است که دارای ماکزیمم TOTALLENGTH است. به طور مثال, برای جدول الفبایی V با همان TOTALLENGTH, اندازه عنصر 1ام 5 است, $n = 2^5 = 32$, $V(1) = \{1101000000, 1101000001, \cdots, 1101011111\}$ ؛ برای جدول الفبایی I با یک TOTAL LENGTH دیگر, MAX TOTAL LENGTH, 5 است و TOTAL LENGTH عنصر اول, 3 است, $n = 2^{5-3+1} = 8$، بنابراین, 8 نقطه در $V(1),\ V(1) = \{00000, 00001, \cdots,\ 00111\}$ گنجانده می شوند.

برای فضای V(i), با فرض اینکه کلمه کد اصلی, Xi است, کلمه کد متناظر با یک نقطه $P(i+r)$ در V(i) مطابق با قاعده نگاشت S() است, همانطور که در معادله (1) است:

$$P(i+r) = S(X_i) \qquad (1)$$

بنابراین, نقطه P(i+r) با یک عملیات اضافه نمودن ماژول توسط عدد صحیح تصادفی Ki رمزگذاری می شود؛

$$P(j+s) = E(P(i+r), K_i) = (P(i+r) + K_i)\, Mod\, M \qquad (2)$$

که در آن Ki یک عدد صحیح تصادفی است که به طور یکنواخت در بازه $[0, M-1]$. توزیع می شود. ماژول M از هر جدول الفبایی متفاوت است؛ بنابراین, روش پیشنهادی, روش رمزگذاری ماژولار متغیر است.

بعد از عملیات رمزگذاری, نقطه $P(i+r)$ در V(i) به نقطه تصادفی $P(j+s)$ در V(j) نگاشته می شود. $P(j+s)$ متناظر با متن رمزی Cj است که کلمه کد VLC معتبر jام در همان جدول الفبایی است:

$$C_j = S^{-1}(P(j+s)) \qquad (3)$$

فرآیند رمزگذاری در شکل 4 نشان داده شده است.

جدول 1جداول الفبایی برای کلمه کد VLC

Alphabetic table	Run/size	Code length	Code word	Total length	Module
I	0/1	2	00	3	3
	0/2	2	01	4	
	1/1	4	1100	5	
II	0/3	3	100	6	2
	2/1	5	11100	6	
III	1/2	5	11011	7	3
	3/1	6	111010	7	
	4/1	6	111011	7	
IV	0/4	4	1011	8	4
	5/1	7	1111010	8	
	6/1	7	1111011	8	
	7/1	8	11111010	9	
V	0/5	5	11010	10	6
	1/3	7	1111001	10	
	2/2	8	11111001	10	
	8/1	9	111111000	10	
	9/1	9	111111001	10	
	A/1	9	111111010	10	
...	.....	...	...		...

3.2 رمزگذاری و اثر انگشت نگاری پیوسته

کاربران, متن رمزی Ci را با کلید رمزگشایی K'_i, رمزگشایی می کنند که در آن $K'_i = K_i - W_i$, و در آن Wi, دنباله اثر انگشت است. K'i, به طور امن توسط فرستنده تولید و ارسال می شود.

بعد از دریافت متن رمزی Cj, کاربر, Cj را به یک نقطه منحصر به فرد P(J+S) در فضای V(j) مطابق با همان قواعد در سمت فرستنده که در معادله (4) نشان داده شده است, می نگارد:

$$P(j+s) = S(C_j) \tag{4}$$

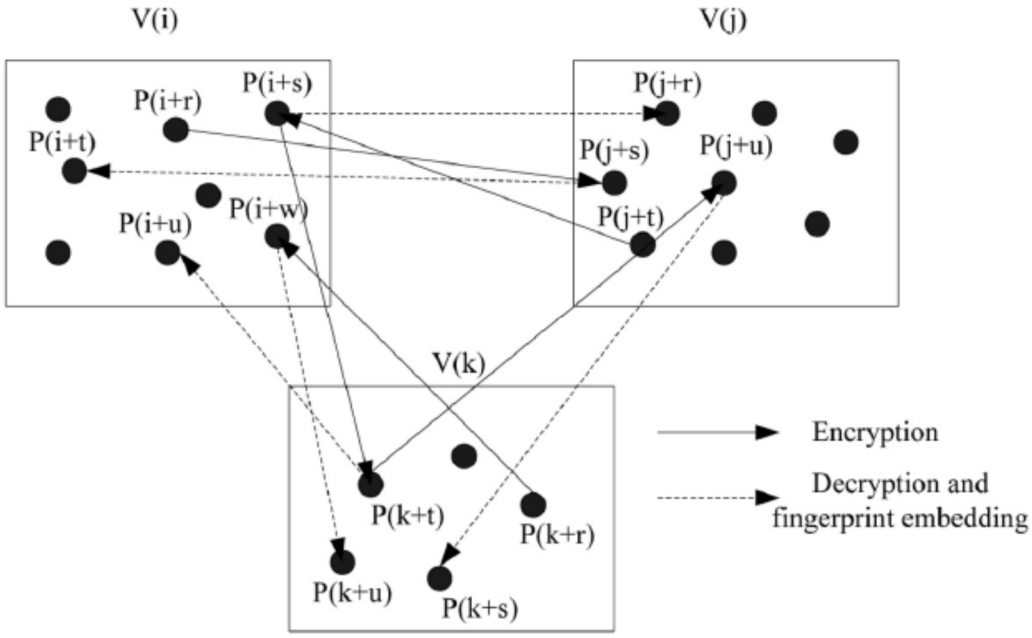
فرآیند تعبیه اثر انگشت و رمزگشایی به صورت زیر است:

$$D(P(j+s), K'_i) == (P(i+r) + K_i - K_i + W_i) \, Mod M = P(i+t) \tag{5}$$

$P(i+t)$, یک نقطه در V(i) است؛ بعد از نگاشت دوباره جریان فشرده شده با اثرانگشت تعبیه شده, X'i به صورت زیر تولید می شود:

$$X'_i = S^{-1}(P(i+t)) \tag{6}$$

X'i مشابه با Xi است و تنها به طور مختصر در مقدار دامنه خود, از Xi متفاوت است.



شکل4. رمزگذاری ماژولار متغیر بر اساس نگاشت فضایی

3.3 آشکارسازی اثر انگشت و ردیابی خائن

فرض کنید که یک جریان تبانی شده, z′ است. می توانیم z′ را با جریان اصلی x مقایسه نماییم, دنباله اثر انگشت را استخراج نماییم و یک کلمه کد اثر انگشت تبانی شده w′ را به دست آوریم. ما w′ را با هر دنباله اثر انگشت کاربر wi با استفاده از معادله (7) همبسته می نماییم:

$$T_N(\mathrm{i}) = \frac{w' w_i}{\sqrt{\|w_i\|^2}}, \quad i = 1,2,\ldots,N \tag{7}$$

کاربری که اثر انگشت آن دارای بالاترین مقدار همبستگی TN(i) است, به صورت یک تبانی کننده شناسایی می شود. با متوسط گیری تبانی, TN (i) از یک توزیع گوسی Nu-بعدی پیروی می کند:

$$\begin{aligned} T &= [T_N(1),\ldots,T_N(N_u)]^T \sim N\left([m_1,m_2]^T,\sigma_d^2\right) \\ m_1 &= \|s\|\left(\frac{1}{c}+\left(1-\frac{1}{c}\right)\rho\right), \quad m_2 = \|s\|\rho \end{aligned} \tag{8}$$

که در آن m1, بردار میانگین برای تبانی کنندگان, m2, بردار میانگین برای کاربران بی گناه است و ρ, همبستگی متوسط بین دو اثر انگشت مختلف است. مطابق با [22], برا یک کد L-tuple q-ary Reed-Solomon, با بعد t, $\rho = \frac{t-1}{L}$ است.

ما ماکزیمم آماره تشخیص را برای تبانی کنندگان و کاربران بی گناه به ترتیب به صورت T1 و T2 تعریف می نماییم:

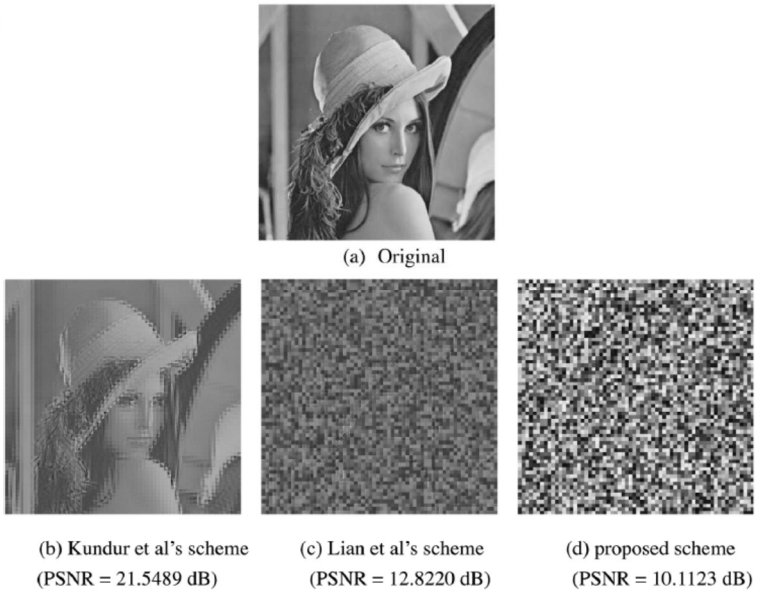
$$T_1 = \max_{j \in S_c} T_N(j), \quad T_2 = \max_{j \notin S_c} T_N(j) \tag{9}$$

که در آن Sc, مجموع تبانی کنندگان است. احتمال دستگیری یک تبانی کننده با استفاده از تشخیص دهنده ماکزیمم را می توان به صورت زیر بیان نمود:

$$P_d = P_r(T_1 > T_2) \approx \int_{-\infty}^{+\infty} P_r(T_1 > t) f_{T_2}(t) dt = \int_{-\infty}^{+\infty} \left(\int_x^{\infty} f_{T_1}(z) dz \right) f_{T_2}(t) dt$$

$$f_{T_i}(x) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(x-m_i)^2}{2\sigma_i^2}} \tag{10}$$

که در آن $P_r()$, تابع توزیع T1 و $f_{T_1}()$ و $f_{T_2}()$, به ترتیب تابع چگالی احتمال T1, T2 هستند.



(a) Original

(b) Kundur et al's scheme (PSNR = 21.5489 dB)

(c) Lian et al's scheme (PSNR = 12.8220 dB)

(d) proposed scheme (PSNR = 10.1123 dB)

شکل 5. کیفیت تصویر رمزگذاری شده

4. نتایج تجربی و تجزیه و تحلیل

این آزمایش شامل سه بخش بود: یک تجزیه و تحلیل عملکرد رمزگذاری، غیرقابل مشاهده بودن اثر انگشت، و استحکام اثر انگشت.

4.1. تجزیه و تحلیل عملکرد رمزنگاری

عملکرد روش رمزگذاری پیشنهادی از نقطه نظر محرمانه بودن، بهره وری فشرده سازی، و انطباق فرمت مورد تحلیل قرار گرفت.

(1) امنیت ادراکی

طرح پیشنهادی، طرح Kundur و همکاران در [4] و طرح Lian و همکاران در [14] به ترتیب برای به رمز در آوردن تصویر Lena 512 * 512 استفاده می شوند. امنیت ادراکی توسط مقدار PSNR بررسی شد. به طور کلی، هرقدر مقدار PSNR پایین تر باشد، فهم اطلاعات رمزگذاری شده پایین تر و امنیت ادراکی بالاتر است. نتایج رمزگذاری در شکل 5 نشان داده شده است.

از این شکل، ما می توانیم ببینیم که طرح پیشنهادی دارای یک امنیت ادراکی بالاتر از دو طرح دیگر است. دلیلش این است که طرح Kundur و همکاران, تنها نشانه ای از ضرایب DCT را رمزگذاری می کند؛ بنابراین، امنیت ادراکی ضعیف است. طرح Lian و همکاران, ضرایب DC و نشانه ای از ضرایب AC را رمز گذاری می کند؛ بنابراین، امنیت ادراکی بالاتر را نسبت به طرح Kundur و همکاران به دست می آورد. طرح پیشنهادی ما, کلمه کدهای VLC را رمزگذاری می کند که با تمام ضرایب AC و DC مطابقت دارد و در نتیجه دارای بالاترین امنیت ادراکی از سه طرح است.

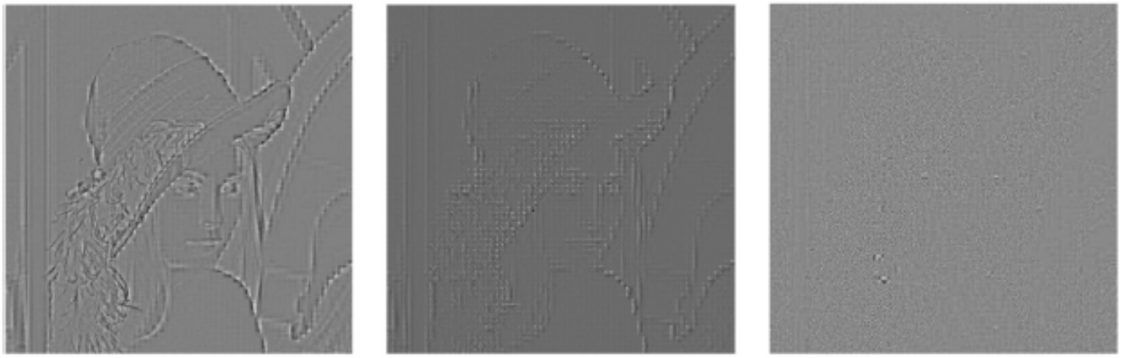
شکل. 6 کیفیت تصاویر بازیابی را از تصاویر رمزگذاری شده با یک حمله پنهان خطای معمولی ادراکی (ECA) [29] نشان می دهد. همانطور که نتایج نشان داده شده است، در مقایسه با طرح های دیگر، طرح پیشنهادی امن تر و در برابر حمله ادراکی مقاوم است.

جدول 2 نتایج مقایسه ای رمزگذاری را با تصاویر با اندازه های مختلف در پایگاه داده تصویر USC-Šípi نشان می دهد. نتایج نشان می دهد که طرح Lian و همکاران دارای امنیت بهتر از طرح Kundur و همکاران است، در حالی که طرح پیشنهادی ما امنیتی ادراکی بهتر از دو طرح دیگر را بدست می آورد.

(2) امنیت رمزنگاری

در روش رمزنگاری ارائه شده، هر کلمه کد VLC, توسط دیگر کلمه کد VLC معتبر با همان طول تحت کنترل توالی تصادفی Ki جایگزین می شود که اتفاقی بودن متن رمزی را تعیین می کند. اگر توالی های واقعاً تصادفی در Ki استفاده شوند، آنگاه رمزنگاری کلمه کد VLC برابر با رمز پد یک-باره است و در برابر حملات متن رمزی تنها، متن رمزی-مشخص و متن رمزی انتخاب شده مقاوم است.

کلمه کد VLC نه تنها به کلمه کد قبلی بلکه به کلمه کد بعدی مربوط می شود؛ بنابراین، فقط دانستن بخشهایی از اطلاعات می تواند برای دیدن غیر مجاز محتوای تصویر چندان مفید نباشد. بنابراین، مهاجمان باید تمام داده هایی را که بر کلمه کد قبلی و کلمه کد بعدی تاثیر می گذارند و یک حمله جامع را مشکل تر خواهد کرد, مورد تجزیه و تحلیل قرار دهند. با در نظر گرفتن تصویر Lena 512 * 512 به عنوان مثال، تعداد کلمه های کد VLC رمزگذاری شده 262144 است و طول کلی کلمه های کد VLC رمزگذاری شده 20581 بایت است؛ اگر مهاجم بخواهد رمز تصویر را به یک تصویر قابل فهم بازیابی نماید، مهاجم باید حداقل 50٪ از فضای کلیدی را تخلیه نماید؛ پس از آن، تعداد بیت هایی که باید تخلی شود, $20581 \times 8 \times 50\% = 82324$ ، تعداد محاسبات مورد نیاز $2^{82324} \approx 9.85*10^{24781}$ است، بنابراین هزینه صرف شده در تخلیه محاسبه, بسیار بزرگتر از مقدار خود تصویر خواهد بود. اگر مهاجم بخواهد بازیابی یک تصویر واضح تر و یا تصویر رمز شده در اندازه بزرگتر را صورت دهد، آنگاه زمان در تخلیه محاسبات به صورت تصاعدی رشد خواهد کرد.



(a) Kundur et al's scheme (PSNR = 23.8807dB) (b) Lian et al's scheme (PSNR = 18.1297dB) (c) Proposed scheme (PSNR = 14.2903dB)

شکل 6. کیفیت تصویر بازیابی از تصویر رمزگذاری شده با ECA

جدول 2مقایسه کیفیت تصویر رمزگذاری شده

File description	Size	Encrypted Image Quality (PSNR)			Recovered Image Quality (PSNR)		
		Lian's	Kundur	proposed	Lian's	Kundur	proposed
Airplane	256 × 256	8.2947	10.0474	8.0232	12.2143	15.6766	9.3566
Aerial	256 × 256	10.9257	12.2578	10.1060	15.8671	17.3904	13.9134
Clock	256 × 256	8.1208	12.8811	7.6901	10.9337	17.3904	9.7407
Chemical plant	256 × 256	12.6905	16.2263	9.9436	15.7578	19.3218	13.3204
Couple	512 × 512	14.8102	16.2980	11.5198	15.0135	17.1532	14.6816
Aerial	512 × 512	9.9296	15.5154	9.3301	12.3162	17.2841	10.7584
Tank	512 × 512	13.2237	15.9683	12.7572	17.0231	19.9842	14.8188
Man	1024 × 1024	12.0986	14.1028	8.9977	15.9341	18.4382	12.1644
Airport	1024 × 1024	14.2722	17.2226	9.6540	16.4676	21.5606	13.4611

جدول 3 نسبت فشردگی تصویر رمزگذاری شده

Method	Kundur's	Lian's	Proposed
Changed compression ratio	Unchanged	33%	Unchanged

(3) انطباق فرمت در متن رمزی

برای رسیدن به انطباق فرمت، کلمه کد اصلی VLC توسط یک کلمه کد VLC معتبر دیگر با همان طول با توجه به جدول حروف الفبای ساخته شده جایگزین می شود. حتی اگر دیکدر, کلید رمزگشایی را نداند، باز هم می تواند پایان دادن کلمه کد را بیابد و هماهنگی را حفظ کند و بنابراین، انطباق فرمت متن-رمز حفظ می شود. برای چند کلمه

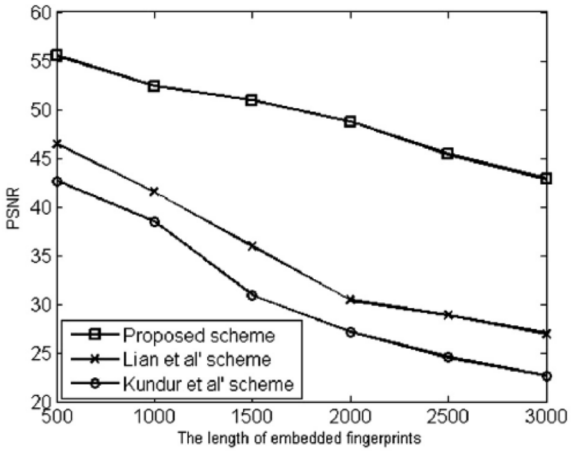
کد معدود که دارای یک TOTALLENGTH مختلف در همان جدول حروف الفبا هستند، برای مثال، کلمه کد ها در جدول الفبایی، بیت های اضافی را می توانددر پایان کلمه کد های کوتاه پر کرد و TOTALLENGTH از جدول را می توان ثابت نگه داشت.

(4) بهره وری فشرده سازی

ما استفاده نسبت تراکم تغییر (CCR) [5] برای ارزیابی کارایی فشرده سازی. جدول 3 نتایج مقایسه ای روش های مختلف نشان می دهد. روش Kundur نتوانست نسبت تراکم را تغییر دهید زیرا این راه تنها نشانه ای از ضرایب AC بدبختانه. در روش پیشنهادی، کلمه کد اصلی توسط جایگزینی کلمه کد معتبر دیگر با همان طول رمزگذاری شده. بنابراین، نسبت تراکم تغییر نخواهند کرد. با این حال، در روش Lian، روابط مجاورت ضرایب تبدیل با رمزگذاری را تغییر داد و نسبت تراکم تا حد زیادی تغییر کرده است.

4.2. غیرقابل مشاهده بودن تعبیه اثر انگشت

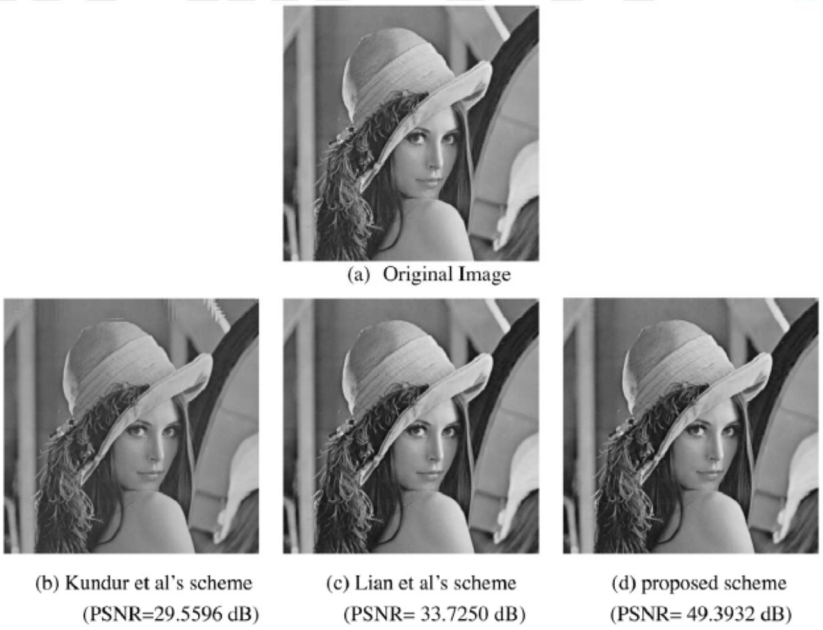
شکل. 7, مقایسه یک تصویر انگشت نگاری شده تولید شده را توسط روش های مختلف در زمانی نشان می دهد که طول دنباله اثر انگشت 1778 است. همانطور که در شکل دیده می شود، طرح ما کیفیت تصویر بهتر از تعبیه اثر انگشت را حاصل می کند.



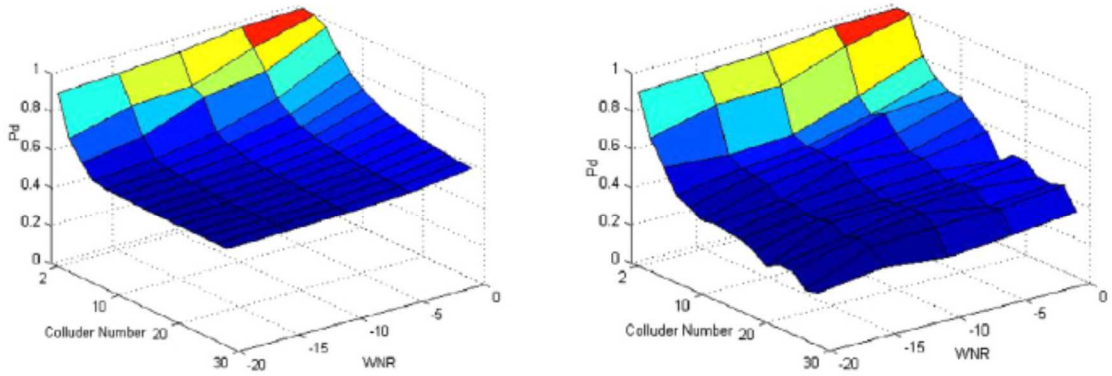
شکل 8. رابطه بین غیرقابل مشاهده بودن و طول دنباله های اثر انگشت تعبیه شده

در طرح ما، اثر انگشت در مقدار AC تعبیه می شود، که دارای اثر کوچکتری بر کیفیت تصویر در مقایسه با دو طرح دیگر است؛ بنابراین، اثر انگشت به طور نامحسوس تعبیه می شود. این یافته به این علت رخ می دهد که در طرح Kundur، اثر انگشت توسط رمز گشایی جزئی بیت نشانه ضرایب AC تولید می شود که به شیوه ای آشکار کیفیت تصویر را تحت تاثیر قرار می دهد؛ در طرح Lian و همکاران، اثر انگشت در ضریب DC توسط رمز گشایی تحت کنترل کلید و اثر انگشت تعبیه می شود و تغییر در ضریب DC نیز موجب تنزل کیفیت تصویر به گونه ای آشکار می شود؛ و تنزل طرح Kundur قوی تر از طرح Lian و همکاران است.

شکل. 8, مقدار PSNR تصویر انگشت نگاری شده را مقایسه می کند, زمانی که طول دنباله های اثر انگشت به طور مداوم افزایش می یابد. همانطور که شکل نشان می دهد، تصویر انگشت نگاری تولید شده توسط روش ما دارای کیفیت تصویر بهتر از دو روش دیگر است. بنابراین استفاده از روش ما می تواند به دستیابی به فضای تعبیه بزرگتر و رسیدن به مقاومت بهتر در برابر حملات تبانی منجر شود.



شکل 7. غیرقابل مشاهده بودن تصویر اثرانگشت



شکل 9. (a) تخمین تحلیلی اثر انگشت تحت یک حمله متوسط (b) نتایج شبیه سازی اثر انگشت تحت یک حمله متوسط

4.3. مقاومت در برابر تبانی اثرات انگشت

برای آزمایش مقاومت در برابر تبانی اثرات انگشت، ما کد Reed-Solomon (14,2) را به عنوان کد مقاومت در برابر تبانی انتخاب نمودیم که در آن $L = 14$، $T = 2$، $q = 16$، و تعداد کاربران $Nu = 256$. است دنباله طلایی به طول $l = 127$ برای انجام یک عملیات طیف گسترده مورد استفاده قرار گرفت. طول کد اثر انگشت ساخته شده برابر با 1778 بود، و تعداد کلی کاربران 256 بود. با فرض اینکه نسبت واترمارک-به-نویز (WNR) در گستره 0 تا 20 دسی بل بود، گنجاندن حالات مختلف از اعوجاج شدید تا اعوجاج خفیف صورت گرفت؛ بنابراین، با توجه به معادله (9)، نتایج نظری عملکرد شناسایی تبانی کننده تحت شرایط حمله معمولی در شکل. 9 (a) نشان داده شده است. همانطور که در این شکل نشان داده شده است، اثر انگشت می تواند حداقل در برابر یک دوجین ار تبانی کنندگان تحت WNR بالا و یک دوجین تبانی کنندگان نیمه تحت WNR پایین مقاومت نماید. ما احتمال دستگیری یک تبانی کننده (Pd) را برای شماره های مختلف تبانی کننده c برآورد نمودیم. نتایج حاصل از 100 تکرار در شکل 9 (b) نشان داده. شده. دیده می شود که نتایج شبیه سازی, تقریب تحلیلی را تایید می نمایند.

5. نتیجه گیری ها

یک طرح حفاظت از امنیت محتوا که رمزگذاری و اثرات انگشت دیجیتالی را برای حوزه های فشرده JPEG ادغام می کند, در این مقاله ارائه شده است. در سمت فرستنده، کلمه کد های VLC در حوزه فشرده به طور مستقیم رمزگذاری می شوند و محرمانه بودن داده ها را می توان تضمین نمود؛ در سمت گیرنده، کدهای اثر انگشت مقاوم در برابر تبانی در تصویر به طور طبیعی پس از رمزگشایی توسط کاربر تعبیه می شوند که می توانند برای ردیابی تبانی کنندگانی مورد استفاده قرار گیرند که به طور غیرقانونی نسخه هایی از رسانه ها را توزیع می کنند و در نتیجه از استفاده صحیح از رسانه ها اطمینان حاصل خواهد شد. طرح پیشنهادی در دو جنبه بسیار کارآمد است: اولاً، تنها فقط یک کپی رمزگذاری شده از محتوای رسانه توزیع می شود، کاربرانی که داده ها را با کلید های مختلف رمزگشایی, رمزگشایی می کنند, نسخه های مختلف انگشت نگاری را کسب می کنند: دوم، عملیات رمزگذاری و انگشت نگاری در یک حوزه فشرده شده پیاده سازی می شود که از رفع فشار زمانبر، رمزگذاری، و یا تعبیه اثر انگشت و فرآیندهای فشرده سازی دوباره اجتناب می کند. روش رمزگذاری مدولار متغیر پیشنهاد مشکل داشتن کلمه کد VLC نامعتبر ناشی از فشرده رمزگذاری جریان داده ها را حل میکند، در حالی که فرمت انطباق متن رمزی می توان نگهداری می شود. نتایج و تحلیل های تجربی, اثربخشی و مقاومت طرح پیشنهادی ما را نشان می دهند. طرح پیشنهادی ما برای حفاظت از امنیت محتوا در اطلاعات چند رسانه ای مناسب است.

References

[1] A. Adelsbach, U. Huber, A. Sadeghi, Fingercasting-joint fingerprinting and decryption of broadcast messages, in: ACISP, LNCS, 4058, Springer-Verlag, Berlin Heidelberg, 2006, pp. 136–147.
[2] A. Sadeghi, The marriage of cryptography and watermarking-beneficial and challenging for secure watermarking and detection, LNCS, 5041, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 2–18.
[3] D. Boneh, J. Shaw, Collusion-secure fingerprinting for digital data, IEEE Trans. Info. Theory 44 (5) (1998) 1897–1905, http://dx.doi.org/10.1109/18.705568.
[4] D. Kundur, K. Karthik, Video fingerprinting and encryption principles for digital rights management, Proc. IEEE 92 (6) (2004) 918–932.
[5] S. Lian, Multimedia Content Encryption: Techniques and Applications, Auerbach Publications, New York, 2009.
[6] B. Mobasseri, R. Berger. Watermarking in the JPEG bitstream, Proc. SPIE 5681, Security, Steganography, and Watermarking of Multimedia Contents VII.
[7] F. Hartung, B. Girod, Digital watermarking of MPEG-2 coded video in the bitstream domain, in: ICASSP, Proc. IEEE, 4, IEEE Computer Society, Washington, DC, USA, 1997, pp. 2621–2624.
[8] A.V. Subramanyam, Sabu Emmanuel, Mohan S. Kankanhalli, Robust watermarking of compressed and encrypted JPEG2000 images, IEEE Trans. Multimedia 14 (3) (2012) 703–716.
[9] J. Bloom, "Security and rights management in digital cinema", Proc. ICME 2003 1, 621–624, IEEE, Piscataway, NJ (2003).

[10] J. Pegueroles et al., A practical solution for distribution rights protection in multicast environments computational science and its applications, in: ICCSA, LNCS, 3982, Springer-Verlag, Berlin Heidelberg, 2006, pp. 527–536.
[11] J. Anderson, C. Manifavas, Chameleon-a new kind of stream cipher, Proc. FSE, 1267, Springer-Verlag, 1997, pp. 107–113.
[12] A.N. Lemma et al., Secure watermark embedding through partial encryption, in: Proc. IWDW, LNCS, 4283, Springer-Verlag, Berlin Heidelberg, 2006, pp. 433–445.
[13] S. Lian, Z. Wang, Collusion-traceable secure multimedia distribution based on controllable modulation, IEEE Trans. Circuits Syst. Video Technol. 18 (10) (2008) 1462–1467.
[14] S. Lian, X. Chen, Secure and traceable multimedia distribution for convergent mobile TV services, Comput. Commun. 33 (2010) 1664–1673, http://dx.doi.org/10.1016/j.comcom.2010.03.015.
[15] B. Mobasseri, R. Berger, M. Marcinak, Y. NaikRaikar, Data embedding in JPEG bitstream by code mapping, IEEE Trans. Image Process. 19 (4) (2010) 958–966.
[16] S. Lian, Z. Liu, Z. Ren, H. Wang, Secure distribution scheme for compressed data streams, Proc. IEEE ICIP 1953–1956 (2006) 2006.
[17] Tosun A S, Feng W C. On error preserving encryption algorithms for wireless video transmission. Proceedings of the ACM International Multimedia Conference and Exhibition. Ottawa, Ont, 2001, 302–308.
[18] Wu C P, Kuo C C J. Fast encryption methods for audiovisual data confidentiality. Proc. of SPIE International Symposia on Information Technologies 2000. Boston, USA, 2000. 284–295.
[19] Wu C P, Kuo C CJ. Efficient multimedia encryption via entropy codec design. SPIE International Symposium on Electronic Imaging 2001. San Jose, USA, 2001, 128–138.
[20] A. Boho, G. Wallendael, A. Dooms, J. Cock, G. Braeckman, P. Schelkens, B. Preneel, R. Walle, End-To-End security for video distribution, the combination of encryption, watermarking, and video adaptation, IEEE Signal Process. Mag. 30 (2) (2013) 97–107.
[21] Int. Telecommunication Union, CCITT Recommendation T.81, Information Technology-Digital Compression and Coding of Continuous tone Still Images-Requirements and Guidelines 1992.
[22] Shan. He, Wu. Min, Joint coding and embedding techniques for multimedia fingerprinting, IEEE Trans. Inf. Secur. 1 (2) (2006) 231–247.
[23] I. Brown, C. Perkins, J. Crowcroft, Watercasting: Distributed watermarking of multicast media, in: In Proc. NGC, LNCS, 1736, Springer, Heidelberg, 1999, pp. 286–300.
[24] H.V. Zhao, K.J. Liu, Fingerprint multicast in secure video streaming, IEEE Trans Image Process. 15 (1) (2006) 12–29.

[25] M.U. Celik, A.N. Lemma, S. Katzenbeisser, M.V.D. Veen, Lookup-table-based secure client-side embedding for spread-spectrum watermarks, IEEE Trans. Inf. Forensics Secur. 3 (3) (2008) 475–487.
[26] C.-Y. Lin, P. Prangjarote, L.-W. Kang, W.-L. Huang, T.-H. Chen, Joint fingerprinting and decryption with noise-resistant for vector quantization images, Signal Process. 92 (9) (2012) 2159–2171.
[27] Jordi. Serra-Ruiz, David. Megias, A novel semi-fragile forensic watermarking scheme for remote sensing images, Int. J. Remote Sens. 32 (19) (2011) 5583–5606.

[28] Joan. Serra-Sagristà, Francesc. Aulí-Llinàs, Remote sensing data compression, Comput. Intell. Remote Sens., SCI 133 (2008) 27–61.
[29] Jiangtao Wen, M. Severa, Wenjun Zheng, M.H. Luttrell, Wenyin Jin, A format-compliant configurable encryption framework for access control of video, IEEE Trans. Circuits Syst. Video Technol. 12 (6) (2002) 545–557.