
بسم الله الرحمن الرحيم

دانشگاه ارومیه

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد شبکه‌های کامپیوتری

ارائه‌ی یک الگوریتم جدید برای رمزنگاری بصری در تصاویر سیاه و سفید

دانشجو

احمدشهاب ارکان

استاد راهنما

دکتر جمشید باقرزاده

استاد مشاور

دکتر علی‌محمد لطیف

آذرماه ۱۳۹۲

دانشگاه ارومیه

دانشکده فنی و مهندسی

ارائه‌ی یک الگوریتم جدید برای رمزنگاری بصری در تصاویر سیاه و سفید

دانشجو:

احمدشهاب ارکان

این پایان‌نامه به عنوان بخشی از فعالیتهای علمی - پژوهشی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش شبکه‌های کامپیوتری در تاریخ آذرماه ۱۳۹۲ توسط هیئت داوران ذیل مورد پذیرش قرار گرفت.

استاد راهنمای اول: دکتر جمشید باقرزاده

استاد مشاور: دکتر علی‌محمد لطیف

داور خارجی: دکتر مهدی چهل امیرانی

داور داخلی: دکتر صالح یوسفی

تقدیم با بوسه بر دستان مادرم

آن فرشته معصومی که الف قامت خویش را دال گرداند تا نهال بی‌سایبان بوستان لبریز صفای خویش را به دستان بخشنده دریایی و عشق لایزالی، پاسبان باشد.

به پاس تعبیر عظیم و انسانی از کلمه ایثار و از خودگذشتگی

به پاس عاطفه سرشار و گرمای امیدبخش وجودش که در سردترین روزگاران بهترین حامی بوده است

به پاس قلب بی‌ریایش که فریادرس است و سرگردانی و ترس در پناهش به شجاعت می‌گراید

و به پاس محبت‌های بی‌دریغش که هرگز فروکش نمی‌کند

این مجموعه را به مادر عزیزم گرانقدرم می‌کنم.

تشکر و قدردانی

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و دورد بر جمیع انبیاء و خاندان پاکشان، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

بدون شک جایگاه و منزلت استاد، اجّل از آن است که در مقام قدردانی از زحمات بی شائبه‌ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم.

اما از آنجایی که تجلیل از استاد، سپاس از انسانی است که هدف و غایت آفرینش را تامین می‌کند و سلامت امانت-هایی را که به دستش سپرده‌اند، تضمین؛ بر حسب وظیفه و از باب ″ من لم یشکر المنعم من المخلوقین لم یشکر اللّه عزّ و جلّ:"

از اساتید با تقوا، صبور، با کمالات و شایسته؛ آقایان دکتر جمشید باقرزاده و دکتر علی‌محمد لطیف که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی و مشاوره‌ی این پایان‌نامه را بر عهده گرفتند؛

هم چنین از اساتید فرزانه و دلسوز؛ آقایان دکتر چهل امیرانی و دکتر یوسفی که زحمت داوری این پایان‌نامه را متقبل شدند؛ کمال تشکر و قدردانی را دارم

به پیشگاه دوستان گرانقدر جنابان دکتر عماد رضایی، حامد صالحی، محمد خضری یزدان، جواد محتاجعلی، احمدخضری، دکتر رضا طلایی، علیرضا حسین پور، مهدی نیکخواه، علیرضا ولی زاده، مرتضی گل زاده، فرشاد رحمانی و بزرگوارانی که از قلم نگذشتند، که در نشیب و فراز روزهای خاطره ساز، هم‌دل، همراه، استوار و ثابت قول بودند سر تعظیم به رسم رفاقت و ادب ، فرود آورده و از ایزد منان توفیق تعالی درجات و مکارم اخلاق را برای این عزیزان خواستارم.

چکیده:

تصویر یکی از مهم‌ترین داده در سیستم‌های اطلاعاتی می‌باشد. به علت سرعت انتقال بالای اطلاعات در شبکه تصاویر نیز برای مخابره شدن از این بستر استفاده می‌کنند. نا امنی در بستر شبکه علت اصلی رمزنگاری اطلاعات پیش از مخابره شدن می‌باشد. الگوریتم‌های کلاسیک رمزنگاری اطلاعات در بستر شبکه در کدگذاری تصاویر دچار ضعف می‌باشد؛ به همین علت تصاویر قبل از مخابره شدن توسط تکنیک‌ها متنوع رمزنگاری تصویر، کدگذاری شده و سپس ارسال می‌شوند. تکنیک‌های جابه‌جایی و جای‌گزینی از مرسوم‌ترین روش‌های رمزنگاری تصویر می‌باشند. هم‌چنین رمزنگاری بصری نیز برای کد کردن سندهای چاپی به کار می‌رود؛ که توسط الگوریتم‌های رمز، سند به دو یا چند اشتراک تقسیم می‌شود. سپس رمزگشایی بدون نیاز به محاسبات ریاضی و توسط سیستم بینایی انسان با قرار گرفتن اشتراک‌های رمز روی یک‌دیگر انجام می‌شود. در این پایان‌نامه الگوریتم‌های نوینی برای رمزنگاری تصویر با تکنیک جابه‌جایی در تصاویر سیاه سفید، خاکستری و رنگی با تمرکز استفاده‌ی تصاویر در سیستم‌های بلادرنگ، و نیز یک روش جدید رمزنگاری بصری برای تصاویر سیاه و سفید بدون استفاده از گسترده کردن پیکسل‌ها ارائه می‌شود. در روش پیشنهادی برای رمزنگاری بصری از اشتراک‌های بامفهوم و بلاک‌های با اندازه‌ی متفاوت به منظور حفظ وضوح مفاهیم و هم چنین تنظیم کنتراست تصویر استفاده می‌شود. نتایج آزمایش‌ها نشان می‌دهد روش‌های پیشنهادی برای رمزکردن تصویر از کارایی مناسب و کیفیت رمزنگاری بالایی برخوردار است.

کلید واژه: رمزنگاری، رمزنگاری بصری، تصویر، درهم‌ریزی.

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست علایم و نشانه‌ها و مخفف‌ها

عنوان	علامت اختصاری
تصویر اصلی	SI
ماتریس رمز برای پیکسل سفید	S_0
ماتریس رمز برای پیکسل مشکی	S_1
مجموعه ماتریس رمز برای پیکسل سفید	C_0
مجموعه ماتریس رمز برای پیکسل مشکی	C_1
رمزنگاری بصری	VC
اشتراک‌های رمز	SH

۱ فصل اول: مقدمه

پیشرفت سریع علم ارتباطات و شبکه‌های کامپیوتری و توسعه‌ی فراوان سیستم‌های چندرسانه‌ای دیجیتالی، باعث تحول بزرگی در زندگی بشر شده است. این تحول، ضمن دارا بودن مزایای فراوان دارای معایبی نیز می‌باشد. جعل و سوء استفاده‌ی عمدی و یا غیرعمدی از مشکل‌های موجود در استفاده از محصول‌های دیجیتالی است. لذا حفاظت و تامین امنیت این محصول‌ها همواره مورد توجه محققین بوده است. یکی از روش‌های متداول حفاظت اطلاعات رمزنگاری می‌باشد.

رمزنگاری علم تبادل و نگهداری محرمانه‌ی اطلاعات با استفاده از توابع ریاضی است که زیرساخت پروتکل‌های امنیت در شبکه‌های کامپیوتری می‌باشد. استفاده از رمزنگاری دارای سابقه‌ی طولانی و تاریخی است. سابقه رمزنگاری اطلاعات به دوران امپراطوری روم بر می‌گردد. امروزه اغلب روش‌ها و مدل‌های رمزنگاری اطلاعات توسط کامپیوتر انجام می‌پذیرد. از این رو رمزنگاری با توجه به پیشرفت‌های اخیر تحول یافته است و در این راستا الگوریتم‌های فراوانی ارائه شده است.

در رمزنگاری رسانه‌های دیجیتالی ابتدا رسانه توسط یک تابع ریاضی با استفاده از کلید درهم‌ریخته می‌شود و سپس توسط کاربران مجاز با داشتن کلید صحیح، رمزگشایی انجام می‌شود[۱]. با توجه به کاربرد روزافزون تصاویر دیجیتال در کامپیوتر، مسئله امنیت برای این داده اهمیت ویژه‌ای یافته است. به علت سرعت بالای انتقال داده توسط شبکه‌های کامپیوتری تصاویر نیز برای مخابره شدن از این بستر بهره می‌گیرند. محتوای تصاویر مخابره شده می‌تواند کاربردهای نظامی، سیاسی، پزشکی و غیره داشته باشد؛ در نتیجه حفظ محرمانگی اطلاعات تصویر توسط رمزنگاری اهمیت بسیاری دارد. به دلیل ویژگی‌های تصویر و زمان‌گیر بودن الگوریتم‌های کلاسیک رمزنگاری داده استفاده از این الگوریتم‌ها برای رمزنگاری تصویر، کارآمد نیست[۲].

رمزنگاری تصویر با استفاده از دو تکنیک جایگزینی[۱] و جابه‌جایی پیکسل[۲] تصویر انجام می‌شود. در روش جایگزینی، سطح روشنایی پیکسل توسط عملیات محاسباتی و منطقی با استفاده از یک تابع ریاضی تغییر می‌کند و سپس معکوس عملیات رمزنگاری در مقصد انجام می‌شود و مقادیر پیکسل‌ها بازیابی می‌شوند. روش جابه‌جایی با تغییر چیدمان پیکسل‌ها در تصویر انجام می‌شود. در این تکنیک ابتدا مکان قرار گرفتن پیکسل‌ها در تصویر توسط یک رابطه‌ی برگشت‌پذیر تغییر می‌یابد و سپس در مقصد چیدمان اولیه‌ی پیکسل‌ها بازیابی می‌شوند.

در درهم‌ریزی تصویر جابه‌جایی چیدمان پیکسل‌ها باید به گونه‌ای انجام شود که تصویر رمزشده هیچ‌گونه اطلاعاتی از تصویر اصلی را به کاربر غیرمجاز ندهد. درهم‌ریزی تصویر در حوزه‌ی مکان با جابه‌جایی مستقیم سطح روشنایی پیکسل‌ها انجام می‌شود؛ اما برای درهم‌ریزی تصویر در حوزه‌ی فرکانس، ابتدا تصویر با یک

[1] Replacing
[2] Substituting

تبدیل مناسب به حوزه‌ی فرکانس انتقال داده می‌شود و سپس درهم‌ریزی روی تبدیل تصویر انجام می‌گیرد. در پایان توسط معکوس تبدیل، تصویر به حوزه‌ی مکان انتقال داده می‌شود.

رمزنگاری بصری یکی از مدل‌های رمزنگاری تصویر مربوط به اشتراک‌های رمز بصری می‌باشد. در رمزنگاری بصری به روش سنتی تصویر مورد نظر به n اشتراک متفاوت تقسیم می‌شود. هر اشتراک، به صورت توزیعی از نویز خواهد بود که هیچ اطلاعاتی در مورد تصویر اصلی ارائه نخواهد کرد. پس از روی هم قرار دادن k تعداد از n اشتراک، تصویر اصلی توسط سیستم بینایی انسان قابل مشاهده خواهد بود[۳]. در فصل دوم پایان‌نامه، رمزنگاری بصری به روش سنتی بررسی خواهد شد.

در رمزنگاری بصری به روش سنتی از تکنیک گسترده کردن پیکسل‌ها برای پنهان کردن تصاویر باینری(مشکی و سفید) بهره می‌بردند. بنابراین اشتراک‌های رمز، حداقل دو برابر تصویر اصلی دچار تغییر ابعاد می‌شد؛ همین تغییر ابعاد در تصویر نهایی بازیابی شده نیز اتفاق می‌افتاد. برای حل این مشکل، روش‌های رمزنگاری پیشرفته‌ی متنوعی عرضه شد. توسط روش‌های ارائه شده در این زمینه، عملیات رمزنگاری را با ضریب اطمینان خوب و بدون ایجاد تغییر ابعاد نسبت به تصویر اصلی انجام شد[۵-۴]. علاوه بر ایجاد اشتراک‌های رمز برای تصاویر مشکی و سفید، مدل‌های رمزنگاری دیگری نیز با هدف رمزکردن تصاویر رنگی یا ایجاد چندین رمز هم‌زمان برای تصاویر مشکی و سفید ارائه شدند.

در فصل سوم پایان‌نامه، مدل جدیدی برای رمزنگاری بصری در حوزه‌ی تصاویر مشکی و سفید، با تکنیک گسترده نکردن پیکسل‌های تصویر اصلی ارائه خواهد شد. با استفاده از مولفه‌های کنتراست، کاربر به راحتی قادر خواهد بود کنتراست مورد نظر خود را در تولید اشتراک‌های رمز و هم چنین تصویر نهایی بازیابی شده، به دست آورد. از دیگر مزیت‌های مدل جدید می‌توان به کنترل کردن کیفیت و شفافیت تصویر نهایی(تصویر رمزگشایی شده) توسط تغییر اندازه‌ی بلاک‌های ایجاد رمز، نام برد. در این پایان‌نامه، مدل‌های(۲، ۲)، (۲، n) و(n، n) با رویکرد مدل جدید ارائه شده، بسط داده خواهند شد. برای هر مدل، نتایج عملی و آزمایشگاهی در فصل چهارم پایان نامه آورده خواهد شد. در نهایت، استنتاج و نتیجه‌گیری در فصل پنجم پایان نامه، ارائه می‌شود.

۱-۱ تاریخچه

رمزنگاری تصویر از دیرباز یکی از متداول‌ترین شیوه‌های پنهان‌سازی اطلاعات بوده است. از تکنیک‌های متداول رمزنگاری تصویر، می‌توان به جابه‌جایی و جایگزینی اشاره کرد. در روش جابه‌جایی سطوح روشنایی در ماتریس تصویر توسط توابع ریاضی یک به یک و برگشت‌پذیر، جابه‌جا می‌شوند. این تکنیک در تصاویر سیاه و سفید، خاکستری و رنگی مورد استفاده قرار می‌گیرد. تصاویر سیاه و سفید گسترده‌ای از صفر و یک می‌باشند در حالی‌که سطوح روشنایی در تصاویر خاکستری مقادیری بین صفر تا ۲۵۵ (طیف خاکستری) را دارا می‌باشند. تصاویر رنگی از سه ماتریس برای نمایش رنگ‌های قرمز، آبی و سبز تشکیل می‌شوند که هر پیکسل از

تصویر نهایی، ترکیبی از مقادیر این سه ماتریس می‌باشد. توسط روش جابه‌جایی محل قرار گرفتن پیکسل در ماتریس تصویر، تغییر می‌کند و بدین صورت مفهوم تصویر از بین خواهد رفت. سپس در مقصد توسط الگوریتم رمزگشایی، سطوح روشنایی به محل اولیه‌ی خود در ماتریس تصویر برخواهند گشت و تصویر اصلی بازیابی می‌شود.

همانند بقیه انواع داده، تصویر نیز برای منتقل شدن از بستر شبکه(اینترنت) بهره می‌گیرد. سرعت بالا و امکانات ویژه‌ی بستر شبکه باعث شده است تا اکثر اطلاعات از این محیط برای مخابره شدن استفاده کنند؛ ولی شبکه محیط ناامن می‌باشد و خطرات سرقت اطلاعات، شنود و دستکاری اطلاعات همواره در فضای سایبری وجود دارد. لذا اطلاعات، قبل از مخابره شدن در بستر شبکه لازم است به رمز تبدیل شده و سپس ارسال شوند. تصویر نیز از همین قانون پیروی کرده و قبل از ارسال، به رمز تبدیل شده و منتقل می‌شود. تکنیک‌های جابه‌جایی و جای‌گزینی از جمله روش‌های شناخته شده در رمزنگاری تصویر می‌باشد.

توابع متعددی برای رمزنگاری تصویر در سالیان متمادی ارائه شده است که هر کدام از ویژگی‌ها و ضعف-های مختص به خود بهره مند می‌باشد. پاره‌ای از این توابع رمزنگاری دارای محاسبات ریاضی پیچیده و زمان-گیری می‌باشند که با هدف ارائه‌ی بهینه‌ترین الگوریتم رمز و ایجاد فاصله‌ی مناسب بین تصویر رمزشده و تصویر اصلی شناخته شده می‌باشند. در حالی که پاره‌ای دیگر از الگوریتم‌های رمز تصویر برای سیستم‌های بلادرنگ مورد استفاده قرار می‌گیرند. این دسته از الگوریتم‌های رمزنگاری دارای محاسبات ریاضی با پیچیدگی کم و سرعت بالا می‌باشند و در حالی که سرعت بالایی دارند از فاصله‌ی مناسبی بین تصویر رمزشده و تصویر اصلی برخوردار می‌باشند.

رمزنگاری بصری اولین بار برای اهداف علمی توسط Naor , Shamir در سال ۱۹۹۴ در اجلاس EuroCrypt '94 ارائه شد[۶]. EuroCrypt همانند اجلاس Crypto و AsianCrypt هر سال با پشتیبانی IACR[1](دستیاران بین‌المللی برای تحقیقات رمزنگاری) برگزار می‌شود. هدف اصلی این نشست‌ها، پیش‌برد تحقیقات رمزنگاری و موارد وابسته به آن است. در نشست یاد شده، روش رمزنگاری جدید که توسط آن بتوان تصویر مشکی و سفیدی را به اشتراک‌های متعددی تقسیم کرد، ارائه شد. برای رمزگشایی تصویر رمز شده، اشتراک‌های ایجاد شده را روی صفحات شفاف چاپ کرده و آنها را روی هم قرار می‌دادند.

از سال ۱۹۹۴، مقاله‌ها و پایان‌نامه‌های زیادی در مورد گسترش انواع رمزنگاری بصری ارائه شده است. در سال ۱۹۹۵ گروهی از دانشجویان دانشگاه لوون[2] بلژیک، مدل مناسبی برای رمزنگاری بصری تصاویر رنگی ارائه کردند. در سال ۱۹۹۸ در هفتمین کنفرانس بین المللی پیتون (International Python Conference)، فرانک استجانو[3] ابزاری برای رمزنگاری بصری ارائه کرد که به کاربران این اجازه را می‌داد تا اشتراک‌های رمزی دلخواه خود را ایجاد کنند و علاوه بر تصاویر مشکی و سفید، تصاویر خاکستری را نیز پشتیبانی می‌کرد[۷]. تا

[1] International Association for Cryptological Research
[2] Leuven
[3] Frank Stajano

امروز، تحقیقات برای رمزنگاری بصری ادامه دارد. مقاله‌های زیادی شامل مباحث وضوح تصویر، گسترش مدل‌های رمزنگاری و آستانه‌گذاری برای رمز کردن، به انتشار رسیده است.

۱-۲ تئوری پایه

برای رمزنگاری و رمزگشایی به کمک تکنیک جابه‌جایی، برای تصاویر سیاه و سفید و خاکستری، ابتدا ماتریس تصویر به برداری از مولفه‌های روشنایی که با عنوان پیکسل‌ها شناخته می‌شوند، تبدیل می‌شود. سپس توسط محاسبات ریاضی و با استفاده از توابع برگشت‌پذیر، محل قرار گرفتن سطوح روشنایی در بردار تصویر اصلی جابه‌جا می‌شوند و تصویر ماهیت اصلی خود را از دست خواهد داد. رمزنگاری برای سطوح روشنایی تصویر یا به صورت جریانی از بیت‌ها(هر بیت) و یا به صورت بلوک(مجموعه‌ای از چند بیت) صورت می‌گیرد. سپس تصویر رمزشده در بستر شبکه مخابره می‌شود. در مقصد توسط محاسبه‌ی تابع معکوس توسط کلید یا کلیدهای رمز، پیکسل‌ها به محل اولیه‌ی خود در بردار تصویر باز می‌گردند و مفهوم تصویر اصلی بازیابی می‌شود.

در تکنیک جای‌گزینی مقدار واقعی سطح روشنایی توسط توابع ریاضی تغییر می‌کند. در این روش پیکسل‌های تصویر اصلی قبل از مخابره شدن، مقدار حقیقی خود را از دست می‌دهند و در مقصد توسط تابع معکوس رمزنگاری و کلید رمز، مقدار واقعی آن‌ها بازیابی می‌شود.

به عنوان مثال بردار تصویر مفروض به صورت زیر برای مخابره شدن آماده می‌شود:

$$image : \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$$

$$Scrambling\_Method : \{11,8,1,12,9,2,10,13,4,5,14,7,15,3,6\}$$

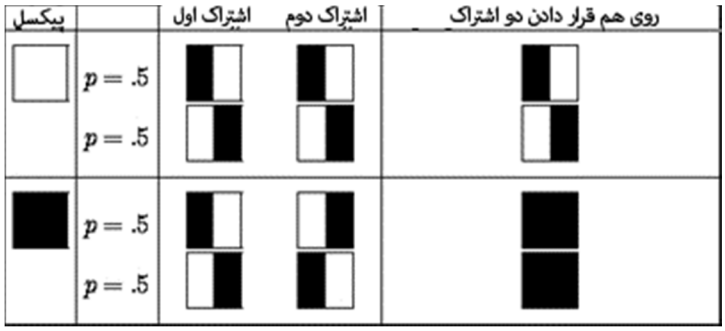
$$Substituting\_Method : \{23,8,250,100,44,7,32,87,90,2,18,1,136,76,45\}$$

همان‌طور که ملاحظه می‌شود توسط کلید رمز مفروض در روش جابه‌جایی، جای قرار گرفتن سطوح روشنایی در بردار رمز نسبت به بردار تصویر اصلی تغییر کرده است و در روش جای‌گزینی، مقدار واقعی پیکسل‌های تصویر اصلی به صورت متناوب تغییر می‌کند. در نتیجه ماهیت تصویر اصلی از دست می‌رود و تصویر به اصطلاح رمز می‌شود. لازم به توضیح است که از ترکیب هر دو روش فوق نیز می‌توان برای رمزنگاری تصویر بهره گرفت. بدیهی است ترکیب این دو تکنیک با یک‌دیگر باعث بالارفتن پیچیدگی محاسبات رمزنگاری و زمان‌بر بودن پروسه‌ی رمزنگاری می‌شود.

به چه شکلی یک تصویر به روش بصری رمزنگاری و کدگشایی می‌شود؟ این بخش روی توضیح تئوری پایه رمزنگاری بصری تاکید دارد. پایان‌نامه حاضر، مربوط به تصاویر باینری است که از گروهی پیکسل‌های مشکی و سفید تشکیل شده است. برای رمز کردن این گونه تصاویر، هر پیکسل در تصویر اصلی به دو یا چندین زیرپیکسل تقسیم می‌شود.

رمزنگاری بصری در سال ۱۹۹۴ توسط Naor و Shamir معرفی شد. ایده‌ی این نوع رمزنگاری از سوال هوشمندانه‌ی زیر جرقه خورد: آیا می‌توان مدل اشتراکی از رمزنگاری ابداع کرد که در آن، تصویر اصلی تنها با روی هم قراردادن نسخه‌ای رمز شده، توسط چشم انسان قابل بازیابی باشد. به عبارتی دیگر برای انجام عملیات رمزگشایی نیازی به محاسبات ریاضی نباشد. هر نسخه(اشتراک) از رمز، یک صفحه با ضریب شفافیت خاص است که از پیکسل‌های مشکی و سفید تشکیل می‌شود. به صورتی که در اختیار داشتن هر کدام از نسخه‌ها، اطلاعات خاصی از تصویر اصلی به دارنده اعطاء نمی‌کند.

Naor و Shamir برای دست یافتن به این هدف، مدل زیر را ارائه کردند. الگوریتم زیر مشخص می‌کند که چطور یک پیکسل در تصویر به صورت رمز در می‌آید.



شکل ۱-۱: تئوری پایه مربوط به رمزنگاری بصری

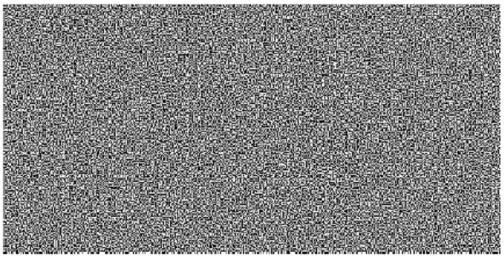
هر پیکسل P به دو زیرپیکسل، در هر دو اشتراک از رمز تقسیم می‌شود. برای رمزکردن پیکسل P از تصویر اصلی در صورتی که سفید باشد، یکی از دو حالت تصویر از سطر اول جدول شکل ۱-۱ به صورت تصادفی انتخاب می‌شود و اگر پیکسل P مشکی بود، به صورت تصادفی یکی از دو حالت تصویر بالا(سطر دوم جدول شکل ۱-۱) انتخاب می‌شود. در نتیجه، پیکسل مورد نظر به صورت رمزشده بر اساس سطور جدول فوق، در نسخ اشتراکی وارد می‌شود. هر پیکسل در تصویر اصلی تا انتهای تصویر به صورت تصادفی بر همین اساس رمز می‌شود.

پیکسل P(دلخواه) در نسخه اول را در نظر بگیرید. یکی از زیرپیکسل‌ها، مشکی و زیرپیکسل دیگری به صورت سفید در نظر گرفته می‌شود. علاوه بر این، وضعیت‌های موجود در هر نسخه می‌تواند به صورت ((مشکی – سفید)) و ((سفید – مشکی)) اتفاق بیافتد و مستقل از پیکسل موجود در زمینه‌ی تصویر اصلی ایجاد شود. بدین معنی که اشتراک اول هیچ راهنمایی در مورد مشکی یا سفید بودن پیکسل در تصویر اصلی ارائه نمی‌کند. شرایط فوق برای نسخه دوم نیز پیاده‌سازی می‌شود و به همین صورت تا آخرین پیکسل موجود در تصویر اصلی عملیات رمز انجام می‌شود. پیکسل دلخواه P را در تصویر اصلی در نظر بگیرید، اگر مشکی باشد در این صورت دو زیرپیکسل مشکی و مشکی در دو نسخه رمز شده وجود دارد و اگر پیکسل P سفید باشد، یک زیرپیکسل مشکی و یک زیرپیکسل سفید وجود خواهد داشت، بدیهی است زمانی که این دو

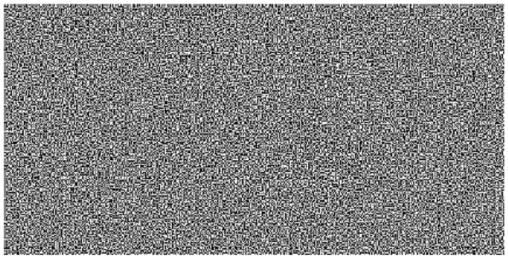
اشتراک روی هم قرار می‌گیرند نتیجه برای پیکسل مشکی، ضریب ۱ و برای پیکسل سفید، ضریب ۰/۵(تقریبا رنگی در طیف خاکستری) خواهد داشت. در این روش ۵۰٪ از وضوح و شفافیت تصویر اصلی را از دست خواهد رفت ولی تصویر اصلی قابل رویت و شناسایی خواهد بود.

۱-۳ مثال برای رمزنگاری بصری

برای اینکه به خوانندگان محترم برای درک بهتر از مفهوم رمزنگاری بصری کمک شده باشد، در این قسمت مثال عملی از بحث، ارائه می‌شود. تصویر اصلی با استاندارد(۲، ۲) (در فصل بعد توضیح داده خواهد شد) به ۲ اشتراک با صفحات شفاف، تسهیم شده است(شکل ۱-۲). اشتراک‌های ایجاد شده، هیچ گونه اطلاعاتی از تصویر اصلی ارائه نمی‌کنند. بهر شکل، هرگاه یکی از اشتراک‌ها روی اشتراک دیگری قرار بگیرد، نتیجه همانند قسمت ج شکل ۱-۲ خواهد شد. پیکسل‌های سفید تصویر اصلی، به صورت خاکستری دیده خواهند شد و پیکسل‌های مشکی تصویر اصلی، به صورت خاکستری پررنگ یا مشکی، ظاهر خواهند شد. پیشنهاد می‌شود دو اشتراک مثال فوق را روی صفحات شفاف پرینت کرده و روی هم قرار بدهید و یا اینکه اشتراک‌ها را در یک شاخه ذخیره کرده و با نرم افزارهای مدیریت تصاویر، بین اشتراک‌ها سوییچ کنید. به یکی از این دو روش، تصویر اصلی قابل رویت خواهد بود.



الف) اشتراک اول مثال ۱-۳



ب) اشتراک دوم از مثال ۱-۳

ج) روی هم قرارداده شده‌ی اشتراک‌های الف و ب

شکل ۱-۲: اشتراک‌ها و نتیجه‌ی روی هم قرار دادن آن‌ها از مثال ۱-۳

۲ فصل دوم: فعالیت‌های مرتبط در رمزنگاری تصویر

از روش‌های متعددی که برای رمزنگاری بصری با تکنیک جابه‌جایی ارائه شده است، در این بخش به چند مورد اشاره می‌گردد.

در سال ۲۰۰۴ میلادی، توسط ژیانچنگ ژو و همکاران[۱۳] یک روش مبتنی بر دنباله‌ی فیبوناچی ارائه شد. آن‌ها در این روش با استفاده از دنباله‌ی فیبوناچی و اندازه‌ی تصویر ابتدا اعداد متباین و پیش ضرایب تابع درهم‌ریزی تصویر را تولید می‌کردند. یکی از مشکل‌های این روش تولید ضرایب یکسان تابع درهم‌ریزی برای تصاویر با اندازه‌های یکسان بود.

در سال ۲۰۰۹ میلادی، توسط وانگ و همکاران[۱۴] روش بهبود یافته‌ی دنباله‌ی آشوب با استفاده از ویژگی مقدار اولیه ارائه شد. در این روش ابتدا یک دنباله‌ی بی‌نظمی با استفاده از کلید تولید و سپس این دنباله به صورت منطقی با پیکسل‌های تصویر ترکیب فصلی منطقی می‌شد. در پایان تصویر رمزشده با استفاده از نقشه‌ی چیدمان پیکسل‌ها، درهم‌ریخته می‌شد. روش پیشنهادی وانگ، علاوه بر درهم‌ریختن محل قرار گرفتن پیکسل‌های تصویر، مقادیر آن‌ها را نیز تغییر می‌داد. این روش دارای کارایی خوبی بود ولی از پیچیدگی محاسبات ریاضی بالایی برخوردار بود.

در سال ۲۰۱۰ میلادی، توسط ژانگ رویهانگ و همکارانش[۱۵] روش مبتنی بر دامنه‌ی محدود اعداد صحیح ارائه شد. در این روش عملیات درهم‌ریزی تصویر با استفاده از کد گری و دامنه‌ی محدود اعداد صحیح انجام می‌شد که علاوه بر این‌که پارامترهای ساده‌ای برای تولید تابع درهم‌ریزی تصویر داشت، از کارایی قابل قبولی روی تصویر برخوردار بود؛ ولی همانند روش رمزنگاری تصویر مبتنی بر دنباله‌ی فیبوناچی، مشکل تولید ضرایب یکسان برای تصاویر با اندازه‌های مشابه، در این روش نیز وجود داشت.

در سال ۲۰۱۰ میلادی، ژیاندانگ لیو و همکاران[۱۶] روش مبتنی بر جابه‌جایی مرتب شده در مدل Chaotic را ارائه کردند. در این روش برای درهم‌ریزی تصویر یک جای‌گشت کد آدرس در دنباله‌ی بی‌نظمی ایجاد و سپس برای تولید تابع رمز از چگالی دنباله‌ی بی‌نظمی استفاده می‌شد. سادگی سیستم تولید تابع رمز در این روش، باعث کاهش پیچیدگی محاسبات ریاضی می‌شد؛ ولی حساسیت استفاده از مقدار اولیه مناسب در نگاشت دنباله‌ی بی‌نظمی، افزایش یافت.

وانگ پیژن و همکارانش[۱۷] در سال ۲۰۱۰ میلادی با بهبود روش Hyper-chaotic، یک الگوریتم درهم‌ریزی تصویر را ارائه کردند. در روش پیشنهادی، ابتدا بر اساس دنباله‌ی بی‌نظمی با قانون Rossler تابع درهم‌ریزی تولید و سپس روی پیکسل‌های تصویر اعمال می‌شد؛ در پایان سطرها و ستون‌های تصویر تحت نگاشت دنباله‌ی منطقی، درهم ریخته می‌شدند. برای بازیابی تصویر باید معکوس نگاشت دنباله‌ی رمزنگاری انجام می‌شد. روش پیژن از کارایی خوب و طول مناسب کلید رمز برخوردار بود ولی پیچدگی بالای محاسبات ریاضی، از ضعف‌های این روش به حساب می‌آمد.

در سال ۲۰۱۱ میلادی، توسط ژانگ لی و همکارانش[۱۸]، روش مبتنی بر چرخش مکعب روبیک ارائه شد. وی در روش پیشنهادی خود ابتدا تصویر مورد نظر را به چندین بلوک مجزا تقسیم می‌کرد که از این طریق چندین مکعب تولید می‌شد. سپس مکعب‌های تولید شده بر اساس قانون دنباله‌ی منطقی و قانون حل مسئله‌ی مکعب روبیک، چرخش داده می‌شدند. از ویژگی‌های این روش، سرعت بالا و پیچیدگی محاسبات تولید تصویر رمزشده و نیز آگاهی از پارامترهای دنباله‌ی منطقی بود لازم به ذکر است در این روش کلید تابع از طول مناسبی برخوردار است.

توسط ژانگ ون هوا و همکاران[۱۹] در سال ۲۰۱۱ میلادی هم چنین روش مبتنی بر جابه‌جایی موجی ارائه شد. در روش پیشنهادی او، از نظریه اعداد اول به عنوان یک مولفه‌ی دیگر محاسبه تابع رمز استفاده می‌شد. برای تابع درهم‌ریزی تصویر ضریب عامل فرکانس پایین در تصویر کاهش می‌یافت که باعث افزایش فضای کلید رمز می‌شد. با افزایش ابعاد کلید، محرمانگی تصویر افزایش پیدا می‌کرد. کارایی قابل قبول روی تصویر برای درهم‌ریزی و هم چنین طول مناسب کلید رمز از نقاط برجسته در روش پیشنهادی ژانگ ون هوا بود.

مدل‌های متفاوتی نیز برای رمزنگاری بصری توسعه داده شده است. مدل، در اینجا به معنی روش رمزنگاری و کدگشایی تصویر می‌باشد. برای مثال، مدل(n ،k) که در آن n اشتراک برای رمزکردن یک تصویر ایجاد می‌شود و تنها در صورتی که k تعداد از اشتراک‌ها روی هم قرار بگیرند، تصویر اصلی بازیابی خواهد شد. اگر تعداد اشتراک‌های پشته شده کم‌تر از k باشد، تصویر اصلی قابل بازیابی نخواهد بود. مدل دیگری از رمزنگاری وجود دارد که در آن باید مجموعه‌ی مشخصی از نسخ اشتراک روی هم قرار بگیرند تا تصویر اصلی قابل بازیابی باشد. فرض کنید اشتراک‌های A,B,C,D تولید شده باشند. مدل مورد نظر طوری طراحی شده است که تنها در حالتی که اشتراک‌های B و C روی هم قرار گرفتند؛ تصویر اصلی قابل رویت باشد و هر ترکیب دیگری از اشتراک‌ها، تصویری بی‌معنی باشد[۸].

مدل زیر تشریح کننده‌ی روش استفاده از ماتریس‌هاست. در این مدل دو مجموعه از ماتریس موجود است. C_0 برای رمزکردن پیکسل‌های سفید و C_1 برای رمزکردن پیکسل‌های مشکی در نظر گرفته شده است. ماتریس‌های درنظر گرفته شده $n \times m$ می‌باشند. هر پیکسل در تصویر اصلی به m زیرپیکسل برای رمزکردن تقسیم می‌شود و n اشتراک برای رمز وجود دارد. ماتریس‌ها از قانون جای‌گشت ستون‌ها ساخته می‌شوند. به عنوان مثال مجموعه‌ی زیر را برای مدل(۲، ۲) در نظر بگیرید.

$$C_0 = \{\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}\}$$

$$C_1 = \{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\}$$

در این حالت n = 2 , m = 2 می‌باشد. زمانی که یک پیکسل سفید رمز می‌شود، یکی از ماتریس‌های C_0 به صورت تصادفی انتخاب می‌شود. هیچ تفاوتی در انتخاب ماتریس نیست زیرا نتیجه‌ی OR کردن تمامی ستون-ها، یک زیرپیکسل مشکی و m-1 زیرپیکسل سفید می‌شود. بدین صورت ضریبی از ۱ به دست می‌آید که در

چشم انسان خاکستری دیده می‌شود. با انتخاب ماتریس در هر اشتراک یکی از سطرهای زیرپیکسل برای رمزنگاری بکار می‌رود. همین ایده برای رمزکردن پیکسل مشکی نیز مورد استفاده قرار می‌گیرد. یکی از ماتریس‌های C_1 به صورت تصادفی انتخاب می‌شود، هر انتخابی از ماتریس بعد از OR منطقی شدن با هم، ۲ زیرپیکسل مشکی و m-2 زیرپیکسل سفید نتیجه می‌دهد که باعث تولید ضریب سنگین‌تری از مشکی(تیره-تر) می‌شود. مانند قبل، هر اشتراک یک سطر از ماتریس را توزیع می‌کند. پس از توزیع زیرپیکسل‌ها در اشتراک‌های رمز با روی هم قرار دادن اشتراک‌ها، زیرپیکسل‌ها ترکیب می‌شوند تا خاکستری روشن و تیره را نمایش دهند و تصویر اصلی ظاهر شود. هیچ اطلاعاتی از تصویر اصلی در هیچ‌کدام از اشتراک‌ها قابل مشاهده نیست زیرا هر پیکسل از تصویر اصلی به صورت تصادفی به دو زیرپیکسل رمز شده است. یکی سفید و دیگری مشکی.

۲–۱ مدل آستانه‌گذاری (k، k) در رمزنگاری بصری

در این قسمت به بررسی مدل‌های متفاوت از آستانه‌گذاری پرداخته خواهد شد. در ادامه نمونه‌هایی از مدل آستانه‌گذاری بررسی می‌شود.

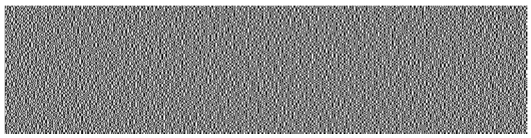
۲–۱–۱ مدل (۲، ۲)

مدل(۲، ۲) روش توضیح داده شده در قبل را نمایش می‌دهد به صورتی که هر دو اشتراک تولید شده برای رمزگشایی مورد نیاز است. پیاده‌سازی مدل(۲، ۲) و دیگر تک تولیدی‌ها، یک شرایط ویژه را ایجاد می‌کند. امکان پیاده‌سازی روش(۲، ۲) توسط دو لایه از زیرپیکسل(شکل ۲.۱) وجود دارد.

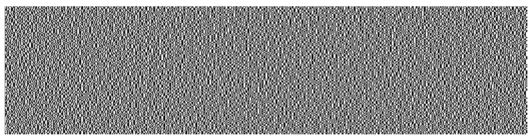
شکل ۲-۱: لایه‌گذاری کردن برای زیرپیکسل در روش(۲، ۲)

در این پایان‌نامه از نرم افزار متلب برای پیاده‌سازی رمزنگاری بصری استفاده شده است. برنامه مربوط به مدل رمزنگاری(۲، ۲) به نام VisCryp.m برای انجام عملیات ماتریس و هم چنین تابع generateshare.m برای تولید اشتراک‌ها در بخش ضمایم ارائه شده است. خروجی توابع نامبرده شده در شکل ۲-۲ نمایش داده شده است. هم چنین نتیجه‌ی روی هم قراردادن اشتراک‌ها نیز مشاهده می‌شود.

الف) تصویر ورودی به تابع تولید اشتراک‌های رمز به مدل(۲، ۲)



ب) اشتراک اول ایجاد شده توسط تابع رمزنگار



ج) اشتراک دوم ایجاد شده توسط تابع رمزنگار

د) روی هم قرار گرفتن اشتراک‌های ایجاد شده

شکل ۲-۲: خروجی توابع رمزنگاری بصری به روش(۲، ۲)

نمونه کد متلب که از ۳ ماتریس برای رمز کردن تصویر اصلی بهره می‌گیرد نیز با عنوان Patrec.m در بخش ضمایم ارائه شده است. مشکل این روش توزیع دو زیرپیکسل به ازای هر پیکسل تصویر اصلی در اشتراک‌های رمز به صورت افقی یا عمودی می‌باشد. بدین صورت تصویر دچار تحریف[1] می‌شود. مثال این روش در شکل ۲-۳ مشاهده می‌شود.

[1] Distort