دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه کارشناسی ارشد

تاثیر قوانین اتوماتای سلولی روی اشتراک سرّ برای تصاویر

تهیه کننده

هدی ملکی

استاد راهنما

دکتر بابک صادقیان

۱۳۸۷

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)

بسمه تعالی

فرم اطلاعات پایان‌نامه
کارشناسی- ارشد و دکترا

تاریخ:
شماره:

معاونت پژوهشی
فرم پروژه تحصیلات تکمیلی ۷

مشخصات دانشجو:

نام و نام خانوادگی: هدی ملکی — دانشجوی آزاد ● — بورسیه ○ — معادل ○

شماره دانشجوئی: ۸۴۱۳۱۰۸۴ — دانشکده: مهندسی کامپیوتر و فناوری اطلاعات — رشته تحصیلی: امنیت اطلاعات

مشخصات استاد راهنما:

نام و نام خانوادگی: بابک صادقیان — درجه و رتبه: دانشیار

نام و نام خانوادگی: — درجه و رتبه:

مشخصات استاد مشاور:

نام و نام خانوادگی: — درجه و رتبه:

نام و نام خانوادگی: — درجه و رتبه:

عنوان پایان‌نامه به فارسی : تاثیر قوانین اتوماتای سلولی روی اشتراک سر برای تصاویر

عنوان پایان‌نامه به انگلیسی: The Effect of Rules for a Cellular Automata Based Secret Sharing Scheme for Images

نوع پروژه: کارشناسی○ — ارشد● — دکتر ا ○ — سال تحصیلی: ۱۳۸۵-۱۳۸۷

کاربردی ○ — بنیادی● — توسعه‌ای ● — نظری○

تاریخ شروع : مهر ۱۳۸۵ — تاریخ خاتمه : اردیبهشت ۱۳۸۷ — تعداد واحد : ۶ — سازمان تأمین کننده اعتبار :

واژه‌های کلیدی به فارسی: اتوماتای سلولی دو بعدی، قوانین بازگشت‌پذیر اتوماتای سلولی، خواص رمزنگاری

واژه‌های کلیدی به انگلیسی: Two dimensional cellular automata, Reversible cellular automata rule, Cryptographic property

مشخصات ظاهری	تعداد صفحات ۱۲۶	تصویر● جدول● نمودار ● نقشه○ واژه‌نامه ○		تعداد مراجع ۲۶	تعداد صفحات ضمائم ۲۶
زبان متن	فارسی ●	انگلیسی ○	چکیده	فارسی●	انگلیسی ●
یادداشت					

نظرها و پیشنهادها به منظور بهبود فعالیت‌های پژوهشی دانشگاه

استاد:

دانشجو:

امضاء استاد راهنما: **تاریخ:**

۱ : ارائه به معاونت پژوهشی به همراه یک نسخه الکترونیکی از پایان‌نامه و فرم اطلاعات پایان‌نامه بصورت PDF همراه چاپ چکیده (فارسی انگلیسی) و فرم اطلاعات پایان‌نامه

چکیده

شراکت سرّ روشی است که یک سرّ را بین شرکت کننده‌ها به شراکت می‌گذارد، بگونه‌ای که تنها زیر مجموعه‌های مجاز از شرکت کننده‌ها قادر به بازیابی سرّ باشند. می‌توان از اتوماتای سلولی در طراحی الگوریتم شراکت سِرّ استفاده نمود. طرح‌های مختلفی در این زمینه انجام گرفته است، یکی از این طرح‌ها توسط مارانون و دلری در سال ۲۰۰۵ انجام شده است.

جهت امکان بازیابی سِرّ لازم است تا الگوریتم طراحی شده بازگشت‌پذیر باشد. لذا چنانچه از اتوماتای سلولی در ساختار الگوریتم شراکت سِرّ استفاده نماییم، مساله بازگشت‌پذیری اتوماتای سلولی باید در نظر گرفته شود.

یکی از روش‌های ساختن اتوماتای سلولی بازگشت‌پذیر استفاده از قوانین بازگشت‌پذیر است. بازگشت‌پذیر بودن قوانین برای حالتی که اتوماتا دو بعدی باشد تا به حال بیان نشده است. یکی از معایب طرح مارانون و دلری استفاده از قانون خطی موسوم به ۱۶ برای بازگشت‌پذیر سازی اتوماتای سلولی است. از دیگر معایب آن استفاده از دسته خاصی از قوانین خطی و عدم بررسی تاثیر قوانین بر امنیت طرح مورد نظر است. در این پایان‌نامه هدف ما برطرف نمودن این عیوب با بکارگیری قوانین بازگشت‌پذیری است که دارای ویژگی‌های مطلوب رمزنگاری هستند.

در این پایان نامه با استفاده از روش اتوماتای سلولی مرتبه دوم، دو دسته قوانین بازگشت‌پذیر معرفی می‌کنیم، که آنها را قوانین تلفیقی نوع (۱) و قوانین تلفیقی نوع (۲) می‌نامیم. قوانین تلفیقی بر مبنای قوانین بازگشت‌پذیر یک بعدی ولفرم ایجاد می‌شوند. تعداد قوانین تلفیقی نوع (۱)، ۲۵۶ عدد و نوع (۲)، ۶۵۲۸۰ عدد است. مبنای عملیات جهت ایجاد قوانین تلفیقی اعمال قوانین بازگشت‌پذیر یک بعدی ولفرم به سطرها و ستون‌های اتوماتای سلولی دو بعدی بطور متناوب است. اگر قانون یک بعدی بازگشت‌پذیر مورد استفاده برای سطرها و ستون‌ها یکی باشد، قانون تلفیقی نوع (۱) ایجاد می‌شود. در حالیکه اگر از دو قانون یک بعدی بازگشت‌پذیر متفاوت برای سطرها و ستون‌ها استفاده شود، قانون تلفیقی را قانون تلفیقی نوع (۲) می‌نامیم.

بر روی قوانین، چهار ویژگی مطلوب رمزنگاری یعنی تمامیت، ویژگی بهمنی اکید، غیر خطی بودن و مسطح بودن تصویر تفاضلی بررسی قرار گرفته است. با انجام این آزمایش، مشاهده می‌شود که قوانین بکار رفته برای طرح شراکت سِرّ مارانون و دلری، فاقد ویژگی‌های مطلوب رمزنگاری هستند. با بررسی این چهار ویژگی بر روی قوانین تلفیقی نوع (۱) و (۲) مشاهده شده است که حدود ۲۶,۱۷٪ از قوانین تلفیقی نوع (۱) دارای هر چهار ویژگی هستند که به آنها قوانین تلفیقی مطلوب گوییم. در حالیکه تنها ۶,۲۵٪ از آنها فاقد هر یک از چهار ویژگی نام برده هستند. برای

قوانین تلفیقی نوع (۲) حدود ۱۴٫۵٪ از قوانین شامل هر چهار ویژگی هستند، در حالیکه تنها ۰٫۷۸٪ از آنها هیچ‌کدام از این چهار ویژگی را ندارند. براین اساس می‌توان توابعی را یافت که هر چهار ویژگی مطلوب رمزنگاری را دارا هستند. تعداد توابعی که هیچیک از ویژگی‌ها را ندارند بسیار اندک هستند.

بررسی تاثیر قوانین بر امنیت طرح به دو روش تبدیل فوریه گسسته و همبستگی پیکسل‌های مجاور انجام گرفته است. بر اساس نتایج بدست آمده مشاهده می‌شود که استفاده از قوانین مطرح شده در الگوریتم شراکت سِرّ منجر به تولید سهم‌های کاملا تصادفی نمی‌شوند. در حالیکه بکارگیری قوانین تلفیقی مطلوب نوع (۱) و (۲) در ساختار الگوریتم منجر به بهبود سهم‌های بدست آمده از نظر رندم بودن، می‌شود.

کلمات کلیدی

اتوماتای سلولی دو بعدی، قوانین بازگشت‌پذیر اتوماتای سلولی، خواص رمزنگاری.

فهرست مطالب

عنوان صفحه

فهرست مطالب

عنوان صفحه

فهرست مطالب

عنوان صفحه

فهرست اشکال

عنوان صفحه

فهرست اشکال

عنوان صفحه

فهرست اشکال

عنوان صفحه

فهرست اشکال

عنوان صفحه

فهرست اشکال

عنوان صفحه

فهرست جداول

عنوان صفحه

۱- مقدمه

۱-۱- مقدمه

معماشناسی شامل شاخه‌های مختلفی است که هرکدام بسته به کاربرد، به نوعی در صدد محافظت از اطلاعات هستند. یکی از مباحث مهم معماشناسی[1]، رمزنگاری است. رمزنگاری عبارت است از تبدیل کردن اطلاعات مورد نظر به یک سری داده به ظاهر نامفهوم (درهم)، که تبدیل تحت یک دنباله دلخواه به نام کلید انجام می‌شود، بطوریکه کلید بطور مخفی بین فرستنده و گیرنده مجاز اطلاعات قرارداد می‌شود و تنها این دو فرد از آن با خبر می‌شوند و دنباله کلید اجرایی بر اساس کلید اصلی تولید می‌شود. انجام عملیات ترجمه رمز بدون داشتن کلید مخفی بسیار پیچیده و وقت‌گیر است، در حالیکه ترجمه رمز با داشتن کلید مخفی با سرعت و به سهولت امکان‌پذیر است. برای رمز داده‌ها از دو الگوریتم رمز قطعه‌ای و دنباله‌ای می‌توان استفاده نمود. در رمز قطعه‌ای، متن مورد نظر جهت رمز شدن به قطعات تقسیم و الگوریتم رمز قطعه‌ای به هر قطعه اعمال می‌شود. در الگوریتم رمز دنباله‌ای، متن مورد نظر بصورت یک دنباله در نظر گرفته می‌شود و الگوریتم به آن اعمال می‌شود.

از آنجا که ساختار الگوریتم‌های رمز قطعه‌ای/دنباله‌ای بر همگان معلوم و مشخص است و قوت سیستم رمز مبتنی بر پیچیدگی بین ورودی/خروجی و کلید می‌باشد، نگهداری و مخفی نگه داشتن کلید اهمیت قابل توجهی دارد.

شراکت سِرّ، روشی است که سهم‌های متناظر با یک سِرّ (مثلا کلید) را با استفاده از محاسبات خاصی بدست آورده و بین کاربران تقسیم می‌نماید و تنها در صورتی امکان کشف سِرّ وجود دارد که تعداد معینی

---

[1] Cryptology

از کاربران مجاز سهم‌های خود را به شراکت بگذارند. هدف از شراکت سِرّ جلوگیری از فاش شدن کلید (یا سِرّ مورد نظر) در رمزنگاری است. معمولا شراکت سِرّ برای داده‌ها بکار می‌رود، اما تصاویر نیز می‌توانند به عنوان سِرّ در طرح شراکت سِرّ مورد استفاده قرار گیرند.

طرح شراکت سِرّ می‌تواند مبتنی بر اتوماتای سلولی باشد. اتوماتای سلولی، نوع خاصّی ازماشین حالت متناهی است که در کاربردهایی مانند شبیه‌سازی سیستم‌های فیزیکی، فرآیندهای زیستی، سیر تکاملی گونه‌ها ، مدل‌های اقتصادی اجتماعی، تولید طرح‌های آزمایشی و تولید کدهای تصحیح خطا استفاده می‌شوند.

در واقع ساختار ساده و رفتار پیچیده اتوماتای سلولی موجب شده است که از آن برای بسیاری از کاربردهای معمّاشناسی استفاده شود، از جمله در طرح‌های شراکت سِرّ.

اتوماتای سلولی، سیستم پویایی است که در آن فضا و زمان گسسته است. یک اتوماتای سلولی، از یک آرایه از سلّولها تشکیل شده است. هر یک از این سلّولها قادر به نگهداری یکی از مقادیر متناهی (حالت) ممکن است. تمامی سلّولها در فواصل زمانی گسسته به صورت همگام بر طبق یک قانون محلّی بهنگام می‌شوند. به مجموعه حالات سلّولها در هر لحظه، پیکربندی اتوماتای سلولی گفته می‌شود. حالت جدید هر سلّول، تنها از حالات فعلی سلّول‌های همسایه تأثیر می‌پذیرد. همسایه‌های یک سلّول، شامل خود سلّول و سلّولهای مجاور یا نزدیک هستند. آرایه سلّولها می‌تواند دارای d بعد باشد.

قانون مشابهی که برای هر سلّول استفاده می‌شود بر طبق همسایه‌های آن تعریف می‌شود. هر قانون، اساساً یک ماشین حالت متناهی است که در قالب یک تابع گذر مشخّص می‌شود. بدین منظور، یک جدول قانون وجود دارد که برای هر پیکربندی ممکن از حالات، دارای یک مدخل است.

برای یک اتوماتای سلّولی m حالتی با n همسایه، تعداد m^n پیکربندی همسایگی مجزّا وجود دارد و تعداد m^{m^n} نگاشت مختلف از این پیکربندی‌های همسایگی به حالت دیگر وجود دارد. هر نگاشت، مشخّص کننده یک قانون اتوماتای سلولی است.

قانون در اتوماتای سلولی نقش اساسی ایفا می‌کند. به عنوان مثال معمولا از قانون ۳۰ برای تولید اعداد تصادفی استفاده می‌شود. آیا انتخاب قانون مناسب در کیفیت نتایج بدست آمده در کاربردهای معماشناسی موثر است؟ چنانچه پاسخ این پرسش مثبت باشد، می‌تواند کاربران چنین قوانین را به انتخاب راحت‌تر و موثرتر رهنمون سازد. این سوال برای زمانیکه از اتوماتای سلولی در طرح شراکت سِرّ تصاویر استفاده می‌شود، نیز مطرح است.

اتوماتای سلولی مورد نیاز برای شراکت سِرّ تصاویر، اتوماتای سلولی دو بعدی است. قوانین موجود برای اتوماتای سلولی دو بعدی بازگشت‌پذیر نیستند، در حالیکه الگوریتم مورد نیاز برای شراکت سِرّ تصاویر باید

بازگشت‌پذیر باشد. در این صورت دو حالت وجود خواهد داشت: ۱- الگوریتم مورد استفاده بازگشت‌پذیر باشد. ۲- اتوماتای سلولی بکار رفته بازگشت‌پذیر باشد. اگر هدف، استفاده از اتوماتای سلولی بازگشت‌پذیر است؛ لازم است از قوانین دو بعدی بازگشت‌پذیر در اتوماتای سلولی استفاده شود.

مجموعه اتوماتای سلولی دو بعدی بازگشت‌پذیر زیر مجموعه‌ای از مجموعه همه اتوماتاهای سلولی دو بعدی است که تعداد اعضای آن در مقایسه با تعداد اعضای مجموعه بسیار ناچیز است. هیچ تابع کارا برای تشخیص آنکه آیا یک اتوماتای سلولی دو بعدی بازگشت‌پذیر است وجود ندارد. حتی اگر بخواهید جستجوی جامع انجام دهید، با صرف زمان بسیار زیادی برای جستجو تنها تعداد معدودی را می‌توان بدست آورد. اما منطقی‌تر آن است که سعی در ترکیب موارد خاصی که دارای ویژگی‌های مطلوب هستند، باشیم.

تعدادی از تکنیک‌های ترکیبی که منجر به تعداد قابل توجهی از اتوماتای سلولی بازگشت‌پذیر می‌شوند عبارتند از:

حالات جزیی: حالت جزیی به اتوماتای سلولی گویند که همسایگی آن حداکثر شامل یک سلول باشد.

داشتن رابطه بازگشت‌پذیر: به مفهوم آنکه تابع انتقال بکار گرفته در اتوماتای سلولی بگونه‌ای باشد که معکوس آن امکان بازگشت به پیکربندی قبل را داشته باشد.

جایگشت فضای خاص محافظت شده: در این حالت تابع انتقال محلی به صورتی است که با تغییر حالت سلول مرکزی در فضای خاص، دیگر رخدادهای آن فضای خاص، ایجاد نمی‌شود یا از بین نمی‌روند. در این حالت گوییم فضای خاص محافظت شده است.

اتوماتای سلولی مرتبه دوم: در این اتوماتا بجای استفاده از یک پیکربندی، از دو پیکربندی فعلی و قبلی در ساخت پیکربندی جدید استفاده می‌شود.

افراز اتوماتای سلولی: در این حالت اتوماتا به ناحیه‌هایی تقسیم می‌شود که در هر ناحیه امکان اعمال قانون بازگشت‌پذیر راحت است. تابع انتقال محلی در واقع به این ناحیه‌ها اعمال می‌شود [۹].

در اتوماتای سلولی جزیی زمانیکه همسایه‌های موثر آن شامل دقیقا یک عضو باشد و جدول قانون آن بازگشت‌پذیر یا به عبارتی بصورت جایگشتی از مقادیر قبل باشد، بازگشت‌پذیر خواهد بود.

زمانیکه تعداد همسایه‌ها بیش از یک عضو باشد، جدول قانون نمی‌تواند بازگشت‌پذیر باشد. چرا که دو مجموعه ظاهر شده در پیکربندی‌های قبل و بعد از اعمال قانون دارای کاردینالیتی متفاوت هستند. در این حالت، همچنانکه وضعیت سلول جدید کاملا با توجه به وضعیت سلول‌های همسایه زمان قبل بدست می‌آید، مقدار سلول قبلی نمی‌تواند کاملا با توجه به سلول‌های پیکربندی زمان جدید بدست آید. تنها راه ساخت اتوماتای سلولی بازگشت‌پذیر در این مورد آن است که بتوان تابع انتقال محلی آن را به نحوی که

جایگشتی از پیکربندی قبلی باشد، بیان نمود. راه‌های مختلفی برای حصول به اتوماتای سلولی بازگشت-پذیر دو بعدی وجود دارد.

یکی از این راه‌ها استفاده از جایگشت فضای خاص محافظت شده است. در این محیط اگر کسی بخواهد یکی از گام‌های پیش رفته را لغو کند، به راحتی می‌تواند بفهمد کدامین سلول تغییر کرده است. زیرا زمانی یک تغییر مجاز است که آن فضای خاص محافظت شده باشد. نحوه لغو تغییر، با مکمل کردن مجدد مقدار همان سلول صورت می‌پذیرد. در واقع وارون تابع انتقال محلی در این حالت با خود تابع انتقال محلی برابر است.

از دیگر راه‌ها، استفاده از اتوماتای سلولی مرتبه دوم است. بدین مفهوم که پیکربندی بعدی تابعی از پیکربندی فعلی و پیکربندی قبلی باشد. به این ترتیب نیازی نیست تا تابع محلی بازگشت‌پذیر باشد. بلکه تنها با داشتن دو پیکربندی بعدی و فعلی می‌توان به راحتی پیکربندی قبلی را بدست آورد و با این کار در واقع مسیر حرکتی عکس را بازسازی نمود.

افراز اتوماتای سلولی نیز از دیگر روش‌های ممکن در ساخت اتوماتای سلولی دو بعدی بازگشت‌پذیر است.

طرح‌های مختلفی در زمینه شراکت سرّ تصاویر با استفاده از اتوماتای سلولی انجام گرفته است، یکی از این طرح‌ها توسط آقایان مارانون و دِلری در سال ۲۰۰۵ انجام شده است.

در طرح مذکور بیان قوانین اتوماتای سلولی بسیار ضعیف انجام گرفته است؛ بدین مفهوم که در این طرح حالت‌های مختلفی که قوانین می‌توانند داشته باشند و اثر آنها روی طرح دیده نشده است. هدف از انجام این پروژه بررسی اثر اعمال قوانین مختلف روی طرح است. با توجه به نامحدود بودن شرایط و محدود بودن زمان انجام پروژه و حجم کاری پیش‌بینی شده، بررسی بر روی دو دسته از قوانین انجام خواهد گرفت: اول قوانین از نوعی که در طرح مذکور در نظر گرفته شده است، ولی بررسی روی آنها انجام نشده است. دوم قوانینی که وضعیت سلول‌ها در دو واحد زمانی قبل بر وضعیت فعلی سلول تاثیر می-گذارد. برای هر دو دسته شعاع همسایگی برابر با یک و اتوماتای سلولی دو بعدی است. در نتیجه هر سلول حداکثر ۹ همسایه دارد. پس از تعریف قوانین، بررسی‌هایی همچون بازگشت‌پذیری قانون، ویژگی بهمنی، ویژگی کامل بودن، نمایه خطی و نمایه تفاضلی انجام می‌گیرد. برای بررسی هر کدام از این پنج ویژگی، نیاز به دنبال کردن گام‌ها و انجام آزمون‌های مختلف روی هر قانون است. سپس از میان قوانین آزمایش شده، قوانینی که مشخصه آنها برای عملیات رمزنگاری مناسب است یعنی دارای ویژگی بازگشت‌پذیر بودن، بهمنی، کامل بودن است و مشخصه‌های نمایه خطی و نمایه تفاضلی خوبی دارند انتخاب می‌شود. ارزیابی در راستای بررسی تاثیر چنین قوانینی بر روی طرح مورد نظر صورت می‌پذیرد. ارزیابی مورد نظر

در واقع بررسی ارتباط بین اجزای سر جزیی و سر اصلی در دامنه فرکانس بر روی تصاویر آزمایشی با استفاده از DFT است.

تعداد قوانین دسته اول برابر با ۵۱۲ قانون است. اما تعداد قوانین دسته دوم برابر با $۲^{۱۸}$ است که بررسی این تعداد قانون، در محدوده زمانی پروژه امکان‌پذیر نیست. به همین دلیل، روشی پیشنهاد کردیم که بر اساس آن قوانین بازگشت‌پذیر قابل ایجاد است. این قوانین را قوانین تلفیقی نامیدیم. قوانین تلفیقی بازگشت‌پذیر پیشنهادی در دسته اتوماتای سلولی مرتبه دوم جای دارند. این قوانین دو بعدی و بازگشت-پذیر هستند و با تلفیق یک دسته خاص از قوانین یک بعدی بازگشت‌پذیر ایجاد می‌شوند. تعداد این قوانین $۲^{۱۶}$ است. از این قوانین می‌توان در الگوریتم شراکت سِرّ استفاده نمود. البته کاربرد این قوانین به الگوریتم شراکت سِرّ محدود نمی‌شود، بلکه در هر الگوریتمی که نیازمند اتوماتای سلولی دو بعدی بازگشت‌پذیر باشد، می‌توان از آن استفاده نمود. قوانین تلفیقی مذکور را به لحاظ دارا بودن ویژگی‌های مطلوب رمزنگاری بررسی نمودیم و از میان آنها، قوانین با ویژگی‌های مطلوب رمزنگاری (قوانین مطلوب)، قوانین فاقد این ویژگی‌ها و قوانین میانی را استخراج نموده، در قالب جدولی بیان کردیم. سپس الگوریتم شراکت سِرّ تصاویر مارانون و دِلری را با استفاده از قوانین تلفیقی مطلوب اجرا نموده و تصاویر سهم‌های حاصله را با استفاده از تبدیل فوریه گسسته[۲] (DFT) بررسی کردیم. نتایج آن را با نتایج بدست آمده از قوانین معمول مورد استفاده در الگوریتم مقایسه نمودیم.

امکان مقایسه نتایج به دلیل ساختار خاصی که الگوریتم اشتراک سِرّ دارد، وجود ندارد. زیرا بخش عمده تصادفی بودن سهم‌ها به دلیل بکارگیری تصاویر تصادفی در پیکربندی اولیه است. لذا جهت امکان مقایسه تاثیر قوانین بر تصادفی بودن سهم‌ها، تصاویر تصادفی را از پیکربندی اولیه حذف نمودیم و بجای آن از تصاویر با معنا استفاده نمودیم. سپس نتایج بدست آمده را با بررسی توزیع همبستگی پیکسل‌های سهم‌ها مقایسه نمودیم. مشاهده شد که استفاده از قوانین تلفیقی مطلوب نوع (۱) یا (۲) منجر به افطایش امنیت طرح می‌گردد. زیرا سهم‌های بدست آمده تصادفی هستند در حالیکه استفاده از قوانین مورد استفاده در طرح منجر به ایجاد سهم‌های تصادفی نمی‌گردد.

رئوس مطالب پایان نامه بدین شرح است: فصل دوم، به بیان ساختار اتوماتای سلولی و انواع آن پرداخته است. در این فصل ساختار اتوماتای سلولی و نحوه تکامل آن بیان شده است. در فصل دوم به بیان انواع اتوماتای سلولی که برای کاربردهای رمزنگاری مورد استفاده قرار می‌گیرند پرداخته شده است. فصل سوم به تشریح کاربردهای اتوماتای سلولی در رمزنگاری برای هر نوع از اتوماتای سلولی تشریح شده در فصل دوم پرداخته است. فصل چهارم مختص بیان شراکت سِرّ با استفاده از اتوماتای سلولی است. در این

[2] Discrete Fourier transform

فصل ساختار کلی شراکت سِرّ توضیح داده شده است و نمونه‌ای از طرح‌های شراکت سِرّ با استفاده از اتوماتای سلولی آورده شده است. در فصل پنجم حالت خاصی از شراکت سِرّ با استفاده از اتوماتای سلولی، یعنی شراکت سِرّ تصاویر تشریح شده است. طرح شراکت سِرّ مارانون ودِلری نیز در این فصل آورده شده است. تحلیل امنیتی که در مقاله مذکور آمده بیان شده است. در این فصل به تشریح چهار ویژگی مطلوب رمزنگاری پرداختیم. هر یک از این چهار ویژگی مطلوب رمزنگاری را بر روی قوانین مورد استفاده در طرح شراکت سِرّ مارانون ودِلری مورد بررسی قرار دادیم. قوانین تلفیقی در فصل ششم آورده شده است. در این فصل نحوه ایجاد دو دسته قوانین تلفیقی، یعنی قوانین تلفیقی نوع (۱) و نوع (۲) آورده شده است. هر یک از این قوانین از نظر دارا بودن چهار ویژگی مطلوب رمزنگاری مورد بررسی وارزیابی قرار گرفته‌اند. قوانین دارای هر چهار ویژگی مطلوب رمزنگاری آورده شده است. در فصل هفتم تبدیل فوریه گسسته بیان شده است. نتایج بدست آمده از اعمال تبدیل فوریه بر روی سهم‌های حاصل از اعمال قوانین مذکور در طرح مارانون ودِلری و قوانین تلفیقی بر الگوریتم شراکت سِرّ بیان شده است. مقایسه‌ای بین نتایج بدست آمده از اعمال تبدیل فوریه روی هر دو دسته صورت پذیرفته است. سپس توزیع همبستگی روی سهم‌های بدست آمده از الگوریتم تغییر یافته را بررسی نمودیم. نهایتا در فصل هشتم جمع‌بندی از مطالب بیان شده در پایان نامه آورده شده است. مسائل باز و کارهای آتی نیز در این فصل آمده است.