



دانشگاه صنعتی امیرکبیر  
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه کارشناسی ارشد

# تأثیر قوانین اتوماتای سلولی روی اشتراک سر برای تصاویر

تهیه کننده

هدی ملکی

استاد راهنما

دکتر بابک صادقیان



دانشگاه صنعتی امیرکبیر  
(پلی تکنیک تهران)

بسمه تعالی

تاریخ:

شماره:

فرم اطلاعات پایان نامه

کارشناسی - ارشد و دکترا

معاونت پژوهشی

فرم پروژه تحصیلات تکمیلی ۷

مشخصات دانشجو:

معادل

بورسیه

دانشجوی آزاد

نام و نام خانوادگی: هدی ملکی

رشته تحصیلی: امنیت اطلاعات

دانشکده: مهندسی کامپیوتر و فناوری اطلاعات

شماره دانشجویی: ۸۴۱۳۱۰۸۴

مشخصات استاد راهنما:

درجه و رتبه: دانشیار

نام و نام خانوادگی: بابک صادقیان

درجه و رتبه:

نام و نام خانوادگی:

مشخصات استاد مشاور:

درجه و رتبه:

نام و نام خانوادگی:

درجه و رتبه:

نام و نام خانوادگی:

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

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

سال تحصیلی: ۱۳۸۵-۱۳۸۷

دکترا

ارشد

نوع پروژه: کارشناسی

نظری

توسعه‌ای

بنیادی

کاربردی

سازمان تأمین کننده اعتبار:

تعداد واحد: ۶

تاریخ خاتمه: اردیبهشت ۱۳۸۷

تاریخ شروع: مهر ۱۳۸۵

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

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

تعداد صفحات ضمیمه ۲۶	تعداد مراجع ۲۶	<input type="radio"/> واژه نامه	<input type="radio"/> نقشه	<input checked="" type="radio"/> نمودار	<input checked="" type="radio"/> جدول	<input checked="" type="radio"/> تصویر	تعداد صفحات ۱۲۶	مشخصات ظاهری
<input checked="" type="radio"/> انگلیسی	<input checked="" type="radio"/> فارسی	چکیده	<input type="radio"/> انگلیسی	<input checked="" type="radio"/> فارسی				زبان متن
یادداشت								

نظرها و پیشنهادهای به منظور بهبود فعالیت‌های پژوهشی دانشگاه

استاد:

دانشجو:

تاریخ:

امضاء استاد راهنما:

## 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 سرّ 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 سرّ لازم است تا الگوریتم طراحی شده بازگشت‌پذیر باشد. لذا چنانچه از اتوماتای سلولی در ساختار الگوریتم شراکت سرّ 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 پایان‌نامه 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 و لفرم 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 و لفرم 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 سرّ 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 هیچ کدام از این چهار ویژگی را ندارند. براین اساس می توان توابعی را یافت که هر چهار ویژگی مطلوب رمزنگاری را دارا هستند. تعداد توابعی که هیچیک از ویژگی ها را ندارند بسیار اندک هستند.

بررسی تاثیر قوانین بر امنیت طرح به دو روش تبدیل فوریه گسسته و همبستگی پیکسل های مجاور انجام گرفته است. بر اساس نتایج بدست آمده مشاهده می شود که استفاده از قوانین مطرح شده در الگوریتم شراکت سیر منجر به تولید سهم های کاملا تصادفی نمی شوند. در حالیکه بکارگیری قوانین تلفیقی مطلوب نوع (۱) و (۲) در ساختار الگوریتم منجر به بهبود سهم های بدست آمده از نظر رندم بودن، می شود.

## کلمات کلیدی

اتوماتای سلولی دو بعدی، قوانین بازگشت پذیر اتوماتای سلولی، خواص رمزنگاری.

## فهرست مطالب

صفحه	عنوان
۱	۱- مقدمه.....
۲	۱-۱- مقدمه.....
۸	۲- اتوماتای سلولی و انواع آن.....
۹	۱-۲- مقدمه.....
۹	۲-۲- تعریف نظری از اتوماتای سلولی.....
۱۱	۲-۳- تعریف محاسباتی اتوماتای سلولی.....
۱۳	۲-۳-۱- ویژگی های قانون.....
۱۵	۲-۳-۲- تکامل اتوماتای سلولی.....
۲۰	۲-۳-۳- اتوماتای سلولی غیر خود گردان.....
۲۱	۲-۴- اتوماتای سلولی قابل برنامه نویسی.....
۲۳	۲-۵- اتوماتای سلولی دو بعدی.....
۲۴	۲-۶- اتوماتای سلولی بازگشت پذیر.....
۲۵	۲-۷- اتوماتای سلولی حافظه ای.....
۲۸	۲-۸- جمع بندی.....
۲۹	۳- اتوماتای سلولی و معمانگاری.....
۳۰	۳-۱- مقدمه.....
۳۰	۳-۲- رمز قطعه ای مبتنی بر اتوماتای سلولی بازگشت پذیر.....
۳۳	۳-۳- اتوماتای سلولی و توابع درهم سازی.....
۳۴	۳-۳-۱- تابع درهم سازی بر مبنای اتوماتای سلولی.....
۳۵	۳-۳-۲- تابع فشرده ساز $h(.)$ .....
۳۶	۳-۳-۳- تابع خروجی $g^*(.)$ .....
۳۷	۳-۳-۴- تابع درهم سازی $hash^*(.)$ .....
۳۸	۳-۴- رمز کردن شکل ها و اتوماتای سلولی.....
۳۸	۳-۴-۱- مولد شبه تصادفی بیتی.....
۳۸	۳-۴-۲- سیستم رمز کردن شکل ها.....
۴۲	۳-۵- جمع بندی.....

## فهرست مطالب

صفحه	عنوان
۴۳	۴- شراکت سرّ با استفاده از اتوماتای سلولی
۴۴	۴-۱- مقدمه
۴۵	۴-۲- شراکت سرّ آستانه ای
۴۶	۴-۳- شراکت سرّ مبتنی بر اتوماتای سلولی
۴۶	۴-۳-۱- طرح شراکت سرّ مبتنی بر LMCA
۴۸	۴-۳-۲- تحلیل امنیتی
۴۹	۴-۴- جمع بندی
۵۰	۵- شراکت سرّ تصاویر با استفاده از اتوماتای سلولی
۵۱	۵-۱- مقدمه
۵۲	۵-۲- طرح شراکت سرّ تصاویر رنگی با استفاده از اتوماتای سلولی حافظه دار
۵۳	۵-۲-۱- فاز برپایی
۵۴	۵-۲-۲- فاز محاسبه سهم ها
۵۴	۵-۲-۳- فاز بازیابی
۵۵	۵-۲-۴- یک مثال
۵۵	۵-۳- تحلیل امنیتی
۵۷	۵-۴- بررسی امنیت قوانین شراکت سرّ تصاویر رنگی با استفاده از اتوماتای سلولی حافظه دار
۵۸	۵-۴-۱- ویژگی های رمزنگاری
۵۹	۵-۴-۲- نداشتن ویژگی کامل بودن و بهمنی اکید قوانین خطی
۶۱	۵-۴-۳- جدول نمایه تفاضلی برای قوانین خطی
۶۵	۵-۵- جمع بندی
۶۶	۶- قانون تلفیقی
۶۷	۶-۱- مقدمه
۶۷	۶-۲- دامنه پروژه
۶۸	۶-۳- قوانین بازگشت پذیر یک بعدی و لفرم
۶۸	۶-۴- قوانین تلفیقی
۶۹	۶-۴-۱- قانون تلفیقی نوع (۱)
۸۴	۶-۴-۲- قانون تلفیقی نوع (۲)

## فهرست مطالب

صفحه	عنوان
۹۳	۵-۶- بررسی آماری.....
۹۷	۶-۶- جمع بندی.....
۹۹	۷- تبدیل فوریه گسسته و همبستگی.....
۱۰۰	۱-۷- مقدمه.....
۱۰۰	۲-۷- تبدیل فوریه گسسته.....
۱۰۶	۳-۷- شرح آزمایش برای قوانین خطی.....
۱۰۹	۴-۷- شرح آزمایش برای قوانین تلفیقی نوع (۱).....
۱۱۳	۵-۷- شرح آزمایش برای قوانین تلفیقی نوع (۲).....
۱۱۵	۶-۷- همبستگی تصاویر.....
۱۲۰	۷-۷- جمع بندی.....
۱۲۲	۸- نتیجه گیری.....
۱۲۴	۹- منابع.....

## فهرست اشکال

عنوان	صفحه
شکل ۱-۲) نمایش همسایه های سلول میانی.....	۱۱
شکل ۲-۲) نحوه محاسبه شماره قانون در اتوماتای سلولی، رنگ سفید به معنی حالت صفر و رنگ سیاه به معنی حالت یک برای سلول است. ....	۱۲
شکل ۳-۲) یک قانون محلی برای اتوماتای سلولی مقدماتی، در آن ۸ حالت ممکن برای ۳ سلول همسایگی را نشان داده و در هر حالت مقدار سلول میانی را در واحد زمانی بعد نشان می دهد. ....	۱۲
شکل ۴-۲) روند تکامل اتوماتای سلولی مقدماتی را با توجه به قانون محلی بیان شده در شکل (۳-۲).....	۱۳
شکل ۵-۲) اتوماتای سلولی ترکیبی.....	۱۴
شکل ۶-۲) تکامل اتوماتای سلولی را برای ۳۲ قانون مجاز با یک پیکربندی اولیه ای که در آن، فقط یک سلول دارای مقدار ۱ است و بقیه آنها مقدار صفر دارند.....	۱۶
شکل ۷-۲) مثلث پاسکال.....	۱۷
شکل ۸-۲) ساختمان هندسی بازگشتی.....	۱۷
شکل ۹-۲) تکامل اتوماتای سلولی در واحد زمان را برای حالت اولیه تصادفی در ۳۲ قانون مجاز.....	۱۸
شکل ۱۰-۲) شمای یک اتوماتای سلولی یک بعدی الف) با شرایط مرزی تهی ب) با شرایط مرزی دوری.....	۱۹
شکل ۱۱-۲) الف) شرایط مرزی دوری. ب) شرایط مرزی تهی.....	۲۰
شکل ۱۳-۲) ساختار PCA با سه سلول و ساختار داخلی یک سلول PCA.....	۲۲
شکل ۱۴-۲) یک PCA عمومی (غیر مکمل شده) با سه خط کنترلی.....	۲۲
شکل ۱۵-۲) یک PCA مکمل شده با سه خط کنترلی.....	۲۲
شکل ۱۶-۲) قانون بازگشت پذیر ۱۹/۲۳۶.....	۲۵
شکل ۱-۳) رمز کردن یک قطعه با استفاده از اتوماتای سلولی بازگشت پذیر.....	۳۱
شکل ۲-۳) ترجمه رمز یک قطعه با استفاده از اتوماتای سلولی بازگشت پذیر.....	۳۲
شکل ۳-۳) طرح رمز کردن چندین قطعه.....	۳۳
شکل ۱-۴) نمایش شراکت سرّ برای سه شرکت کننده.....	۴۴
شکل ۱-۵) تصویر اصلی و دو سهم آن.....	۵۵
شکل ۲-۵) هیستوگرام تصویر اصلی و دو سرّ جزئی بدست آمده.....	۵۶
شکل ۳-۵) همبستگی بین پیکسل های مجاور مورب.....	۵۷
شکل ۴-۵) نمودار ویژگی کامل بودن. مقادیر سطرها شامل تفاضل خروجی تصویر اصلی با تصاویر تغییر	



## فهرست اشکال

عنوان	صفحه
یافته و مقادیر ستون شامل شماره بیت ها است.....	۵۸
شکل ۶-۱) قانون بازگشت پذیر ۲۱۴/۴۱.....	۶۸
شکل ۶-۲) اتوماتای سلولی دو بعدی .....	۶۹
شکل ۶-۳) تبدیل اتوماتای سلولی دو بعدی به $m$ اتوماتای سلولی یک بعدی و اعمال قانون بازگشت پذیر $f$ به آنها.....	۷۰
شکل ۶-۴) تبدیل اتوماتای سلولی دو بعدی به $n$ اتوماتای سلولی یک بعدی و اعمال قانون بازگشت پذیر $f$ به آن.....	۷۰
شکل ۶-۵) الف) تبدیل اتوماتای سلولی دو بعدی به اتوماتای سلولی یک بعدی، با کنار هم قرار دادن سطرهاى اتوماتای سلولی دو بعدی و اعمال قانون بازگشت پذیر $f$ به آن. ب) اتوماتای سلولی یک بعدی جدید پس از اعمال قانون $f$ .....	۷۱
شکل ۶-۶) تبدیل اتوماتای سلولی یک بعدی به اتوماتای سلولی دو بعدی، با جدا نمودن هر $n$ سلول به عنوان سطرهاى مجزا.....	۷۱
شکل ۶-۷) الف) تبدیل اتوماتای سلولی دو بعدی به اتوماتای سلولی یک بعدی، با کنار هم قرار دادن ستون های اتوماتای سلولی دو بعدی و اعمال قانون $f$ . ب) اتوماتای سلولی یک بعدی جدید پس از اعمال قانون $f$ .....	۷۲
شکل ۶-۸) تبدیل اتوماتای سلولی یک بعدی به اتوماتای سلولی دو بعدی، با جدا نمودن $n$ سلول به عنوان ستون های مجزا.....	۷۲
شکل ۶-۹) اعمال قانون تلفیقی نوع (۱) به اتوماتای سلولی دو بعدی .....	۷۳
شکل ۶-۱۰) اعمال وارون قانون تلفیقی نوع (۱) به اتوماتای سلولی دو بعدی .....	۷۴
شکل ۶-۱۱) نمودار ویژگی کامل بودن برای قانون ۵۷/۱۹۸. مشاهده می شود که هیچکدام از اعداد این نمودار برابر صفر نمی باشد.....	۷۵
شکل ۶-۱۲) نمودار ویژگی بهمنی با بازه ۵٪ برای قانون ۵۷/۱۹۸. مشاهده می شود که تعداد ۲۲۵ عدد از ۲۵۶ عدد موجود در نمودار در بازه ۴۷۵-۵۲۵ قرار دارد.....	۷۶
شکل ۶-۱۳) نمودار ویژگی کامل بودن برای قانون ۱۵/۲۴۰. مشاهده می شود که مقدار صفر در نمودار وجود دارد.....	۷۷
شکل ۶-۱۴) نمودار ویژگی بهمنی با بازه ۱۰٪ برای قانون ۱۱/۲۴۴. مشاهده می شود که تعداد ۲۲۰ عدد از ۲۵۶ عدد موجود در بازه ۴۵۰-۵۵۰ قرار دارند.....	۷۹
شکل ۶-۱۵) تبدیل اتوماتای سلولی دو بعدی به $m$ اتوماتای سلولی یک بعدی و اعمال قانون بازگشت	

## فهرست اشکال

عنوان	صفحه
پذیر $f_1$ به آن.....	۸۵
شکل ۶-۱۶) تبدیل اتوماتای سلولی دو بعدی به $n$ اتوماتای سلولی یک بعدی و اعمال قانون بازگشت پذیر $f_2$ به آن.....	۸۶
شکل ۶-۱۷) اعمال قانون تلفیقی نوع (۲) به اتوماتای سلولی دو بعدی.....	۸۷
شکل ۶-۱۸) اعمال وارون قانون تلفیقی نوع (۲) به اتوماتای سلولی دو بعدی.....	۸۸
شکل ۶-۱۹) نمودار ویژگی کامل بودن برای قانون ۱۰۶/۱۴۹-۱۰۱/۱۵۴. مشاهده می شود که هیچکدام از اعداد این نمودار برابر صفر نمی باشد.....	۸۹
شکل ۶-۲۰) نمودار ویژگی بهمنی با بازه ۵% برای قانون ۱۰۶/۱۴۹-۱۰۱/۱۵۴.....	۹۰
شکل ۶-۲۱) نمودار ویژگی کامل بودن برای قانون ۱۳۱/۱۲۴-۰/۲۵۵. مشاهده می شود که مقدار صفر در نمودار وجود دارد.....	۹۱
شکل ۶-۲۲) نمودار ویژگی بهمنی با بازه ۱۰% برای قانون ۱۱/۲۴۴-۲۰۷/۴۸.....	۹۲
شکل ۶-۲۳) شکل سمت چپ، اعمال قانون تلفیقی نوع (۱)، شکل سمت راست، اعمال قانون تلفیقی نوع (۲).....	۹۳
شکل ۶-۲۴) اعمال دو قانون تلفیقی نوع (۱) یا نوع (۲).....	۹۴
شکل ۶-۲۵) اعمال سه قانون تلفیقی نوع (۱) یا نوع (۲).....	۹۴
شکل ۶-۲۶) اعمال چهار قانون تلفیقی نوع (۱) یا نوع (۲).....	۹۵
شکل ۶-۲۷) اعمال پنج قانون تلفیقی نوع (۱) یا نوع (۲).....	۹۵
شکل ۶-۲۸) اعمال شش قانون تلفیقی نوع (۱) یا نوع (۲).....	۹۶
شکل ۶-۲۹) اعمال هفت قانون تلفیقی نوع (۱) یا نوع (۲).....	۹۶
شکل ۶-۳۰) ساختار قوانین بازگشت پذیر دو بعدی، با تعمیم ایده آقای ولفرم.....	۹۷
شکل ۷-۱) تصویری از فرکانسهای تصویر دو بعدی.....	۱۰۱
شکل ۷-۲) تصویر اصلی و نتایج حاصل از اعمال تبدیل فوریه به آن.....	۱۰۲
شکل ۷-۳) تصویر (الف) تصویری از خطوط راه راه عمودی است. تصویر (ب) تصویر حاصل از اعمال تبدیل فوریه گسسته روی تصویر (الف) است.....	۱۰۳
شکل ۷-۴) تصویر (الف) تصویری از خطوط راه راه مورب است. تصویر (ب) تصویر حاصل از اعمال تبدیل فوریه گسسته روی تصویر (الف) است.....	۱۰۴
شکل ۷-۵) موج تصادفی در امتداد بردار زمان.....	۱۰۵
شکل ۷-۶) نمودار حاصل از اعمال تبدیل فوریه بر روی موج تصادفی.....	۱۰۵

## فهرست اشکال

عنوان	صفحه
شکل ۷-۷) نمودار موج تصادفی دو بعدی پس از اعمال تبدیل فوریه دو بعدی.....	۱۰۶
شکل ۷-۸) تصویر سمت چپ تصویر Lena است و تصویر سمت راست تصویر Pepper است.....	۱۰۷
شکل ۷-۹) تصویر سهم های بدست آمده از اعمال قانون مطلوب ۱۲۳ در الگوریتم شراکت سرّ تصاویر. سرّ مورد نظر تصویر Pepper است. ....	۱۰۷
شکل ۷-۱۰) تصویر سهم های بدست آمده از اعمال قانون مطلوب ۱۲۳ روی تصویر Pepper پس از اعمال تبدیل فوریه گسسته به هر یک از آنها. ....	۱۰۸
شکل ۷-۱۱) تصویر سهم های بدست آمده از اعمال قانون مطلوب ۱۲۳ در الگوریتم شراکت سرّ تصاویر. سرّ مورد نظر تصویر Lena است.....	۱۰۸
شکل ۷-۱۲) تصویر سهم های بدست آمده از اعمال قانون مطلوب ۱۲۳ روی تصویر Lena پس از اعمال تبدیل فوریه گسسته به هر یک از آنها. ....	۱۰۹
شکل ۷-۱۳) تصویر سهم های بدست آمده از اعمال قانون مطلوب ۹/۲۴۶ در الگوریتم شراکت سرّ تصاویر. سرّ مورد نظر Pepper است. ....	۱۱۱
شکل ۷-۱۴) تصویر سهم ها پس از اعمال تبدیل فوریه گسسته به هر یک از آنها. ....	۱۱۱
شکل ۷-۱۵) سهم های بدست آمده از اعمال قانون ۹/۲۴۶ در الگوریتم شراکت سرّ تصاویر. سرّ مورد نظر Lena است. ....	۱۱۲
شکل ۷-۱۶) تصویر سهم ها پس از اعمال تبدیل فوریه گسسته به هر یک از آنها. ....	۱۱۲
شکل ۷-۱۷) تصویر سهم های بدست آمده از اعمال قانون مطلوب ۱۰۶/۱۴۹-۱۰۱/۱۵۴ در الگوریتم شراکت سرّ تصاویر. سرّ مورد نظر Pepper است.....	۱۱۳
شکل ۷-۱۸) تصویر سهم ها پس از اعمال تبدیل فوریه گسسته به هر یک از آنها. ....	۱۱۳
شکل ۷-۱۹) سهم های بدست آمده از اعمال قانون ۱۰۶/۱۴۹-۱۰۱/۱۵۴ در الگوریتم شراکت سرّ تصاویر. سرّ مورد نظر Lena است. ....	۱۱۴
شکل ۷-۲۰) تصویر سهم ها پس از اعمال تبدیل فوریه گسسته به هر یک از آنها. ....	۱۱۴
شکل ۷-۲۱) سهم های بدست آمده برای پیکربندی اولیه تصایر Lena, Pepper و قانون ۵. ....	۱۱۶
شکل ۷-۲۲) توزیع همبستگی سهم ها برای قانون ۵.....	۱۱۶
شکل ۷-۲۳) سهم های بدست آمده برای پیکربندی اولیه تصایر Lena, Pepper و قانون ۱۳۶/۱۱۹...۱۱۷	۱۱۷
شکل ۷-۲۴) توزیع همبستگی سهم ها برای قانون ۱۳۶/۱۱۹.....	۱۱۸
شکل ۷-۲۵) سهم های بدست آمده برای پیکربندی اولیه تصایر Lena, Pepper و قانون ۲۴۹/۵۶-.....	۱۱۹
.....	۲۲۶/۲۹

فهرست اشکال

صفحه

عنوان

شکل ۷-۲۶) توزیع همبستگی سهم ها برای قانون ۱۹۹/۵۶-۲۲۶/۲۹ ..... ۱۲۰

## فهرست جداول

عنوان	صفحه
جدول ۵-۱) ضریب همبستگی بین دو پیکسل مجاور	۵۶
جدول ۶-۱) جداول نمایه خطی و نمایه تفاضلی قانون ۵۷/۱۹۸	۷۶
جدول ۶-۲) جداول نمایه خطی و نمایه تفاضلی قانون ۱۵/۲۴۰	۷۸
جدول ۶-۳) جداول نمایه خطی و نمایه تفاضلی قانون ۱۱/۲۴۴	۷۹
جدول ۶-۴) مشخصات قوانین تلفیقی نوع (۱)	۸۰
جدول ۶-۵) قوانین مطلوب و نامطلوب تلفیقی با توجه به نتایج حاصل از آزمایش های انجام شده	۸۴
جدول ۶-۶) تعداد و درصد قوانین که دارای هر کدام از ویژگی کامل بودن، ویژگی بهمندی اکید، نمایه خطی و نمایه تفاضلی است	۸۴
جدول ۶-۷) تعداد و درصد قوانین که دارای هر کدام از ویژگی کامل بودن، ویژگی بهمندی اکید، نمایه خطی و نمایه تفاضلی است	۹۳

١- مقدمه

## ۱-۱- مقدمه

معماشناسی شامل شاخه‌های مختلفی است که هر کدام بسته به کاربرد، به نوعی در صدد محافظت از اطلاعات هستند. یکی از مباحث مهم معماشناسی<sup>۱</sup>، 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

---

<sup>۱</sup> Cryptology

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

طرح شراکت سیرّ می‌تواند مبتنی بر اتوماتای سلولی باشد. اتوماتای سلولی، نوع خاصی از ماشین 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 معماشناسی استفاده شود، از جمله در طرح‌های شراکت سیرّ.

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

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

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

قانون در اتوماتای سلولی نقش اساسی ایفا می‌کند. به عنوان مثال معمولاً 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 سیرّ تصاویر استفاده می‌شود، نیز مطرح است.

اتوماتای سلولی مورد نیاز برای شراکت سیرّ تصاویر، اتوماتای سلولی دو بعدی است. قوانین موجود برای اتوماتای سلولی دو بعدی بازگشت‌پذیر نیستند، در حالیکه الگوریتم مورد نیاز برای شراکت سیرّ 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 جزئی: حالت جزئی 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 جزئی زمانیکه همسایه‌های موثر آن شامل دقیقاً 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 کاردینالیته متفاوت هستند. در این حالت، همچنانکه وضعیت سلول جدید کاملاً با توجه به وضعیت سلول‌های همسایه زمان قبل بدست می‌آید، مقدار سلول قبلی نمی‌تواند کاملاً 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 دلری 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 می‌گذارد. 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 پنچ 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  $2^{18}$  است که بررسی این تعداد قانون، در محدوده زمانی پروژه امکان پذیر نیست. به همین دلیل، روشی پیشنهاد کردیم که بر اساس آن قوانین بازگشت پذیر قابل ایجاد است. این قوانین را قوانین تلفیقی نامیدیم. قوانین تلفیقی بازگشت پذیر 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 بازگشت پذیر ایجاد می شوند. تعداد این قوانین  $2^{16}$  است. از این قوانین می توان در الگوریتم شراکت سیر استفاده نمود. البته کاربرد این قوانین به الگوریتم شراکت سیر محدود نمی شود، بلکه در هر الگوریتمی که نیازمند اتوماتای سلولی دو بعدی بازگشت پذیر باشد، می توان از آن استفاده نمود. قوانین تلفیقی مذکور را به لحاظ دارا بودن ویژگی های مطلوب رمزنگاری بررسی نمودیم و از میان آنها، قوانین با ویژگی های مطلوب رمزنگاری (قوانین مطلوب)، قوانین فاقد این ویژگی ها و قوانین میانی را استخراج نموده، در قالب جدولی بیان کردیم. سپس الگوریتم شراکت سیر تصاویر مارانون و دلری را با استفاده از قوانین تلفیقی مطلوب اجرا نموده و تصاویر سهم های حاصله را با استفاده از تبدیل فوریه گسسته<sup>۲</sup> (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 سیر دارد، وجود ندارد. زیرا بخش عمده تصادفی بودن سهم ها به دلیل بکارگیری تصاویر تصادفی در پیکربندی اولیه است. لذا جهت امکان مقایسه تاثیر قوانین بر تصادفی بودن سهم ها، 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 پیکسل های سهم ها مقایسه نمودیم. مشاهده شد که استفاده از قوانین تلفیقی مطلوب نوع (۱) یا (۲) منجر به افضایش امنیت طرح می گردد. زیرا سهم های بدست آمده تصادفی هستند در حالیکه استفاده از قوانین مورد استفاده در طرح منجر به ایجاد سهم های تصادفی نمی گردد.

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 می گیرند 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 سیر با استفاده از اتوماتای سلولی است. در این

---

<sup>2</sup> Discrete Fourier transform

فصل ساختار کلی شراکت سیر توضیح داده شده است و نمونه‌ای از طرح‌های شراکت سیر با استفاده از اتوماتای سلولی آورده شده است. در فصل پنجم حالت خاصی از شراکت سیر با استفاده از اتوماتای سلولی، یعنی شراکت سیر تصاویر تشریح شده است. طرح شراکت سیر مارانون و دلری 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 سیر مارانون و دلری 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 و ارزیابی 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 و دلری و قوانین تلفیقی بر الگوریتم شراکت سیر 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. نهایتاً 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.