





دانشگاه شهید بهشتی

دانشکده مهندسی برق و کامپیوتر

## نگاشت آشوبناک جدید برای رمزنگاری تصویر

رساله برای دریافت درجه دکتری

در رشته مهندسی کامپیوتر گرایش معماری کامپیوتر

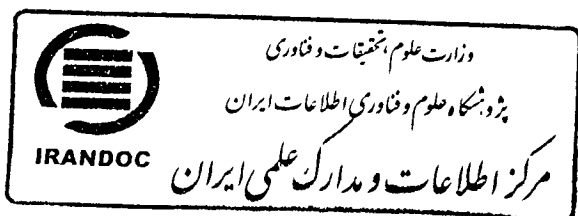
توسط:

شهرام اعتمادی بروجنی

استاد راهنما:

دکتر محمد عشقی

شهریورماه ۱۳۸۹



۱۴۹۲۲۱

۱۳۸۹/۱۰/۱۹



دانشگاه شهید بهشتی  
دانشکده مهندسی برق و کامپیوتر

رساله دکتری مهندسی کامپیوتر گرایش معماری کامپیوتر

تحت عنوان: نگاشت آشوبناک جدید برای رمزنگاری تصویر

در تاریخ ۲۴ شهریور ۱۳۸۹ رساله آقای شهرام اعتمادی بروجنی، توسط کمیته تخصصی داوران مورد بررسی و تصویب نهائی قرار گرفت.

- |  |                              |                                  |
|--|------------------------------|----------------------------------|
| امضاء:   | آقای دکتر محمد عشقی،         | ۱- استاد راهنما:                 |
| امضاء:  | آقای دکتر کیوان ناوی،        | ۲- استاد داور (از دانشگاه):      |
| امضاء:  | آقای دکتر علی ذاکرالحسینی،   | ۳- استاد داور (از دانشگاه)       |
| امضاء:  | آقای دکتر سیدمهدی فخرائی،    | ۴- استاد داور (خارج از دانشگاه): |
| امضاء:  | آقای دکتر محمدرضا جاهد مطلق، | ۵- استاد داور (خارج از دانشگاه)  |
| امضاء:  | آقای دکتر اسلام ناظمی،       | ۶- نماینده تحصیلات تکمیلی:       |
| امضاء:  | آقای دکتر امید هاشمی‌پور،    | ۷- ناظر تحصیلات تکمیلی:          |

## تشکر و قدردانی:

### بنام آنکه جان را فکرت آموخت چراغ دل ز نور جان برافروخت

وظیفه خود می‌دانم از از استاد عزیز و گرانقدرم، جناب آقای دکتر عشقی که با تلاش‌های بی‌شائبه خود مرا در طی مسیر تحقیق و حصول نتیجه و در تدوین رساله راهنمایی نمودند، کمال تشکر را بنمایم. ایشان در تمام دوره تحصیل همواره پشتیبان من بودند و از هیچ کمکی دریغ نورزیدند. برای ایشان آرزوی سلامتی و موفقیت روزافزون دارم.

همچنین از آقای دکتر ناوی، که علاوه بر قبول زحمت داوری این رساله، از رهنمودهای خود مرا بهره‌مند می‌کردند، نیز تشکر و قدردانی می‌نمایم. مناعت طبع ایشان در زمان تصدی معاونت تحصیلات تکمیلی دانشکده، زمینه توسعه دوره دکتری را فراهم نمود.

از آقایان دکتر ذاکرالحسینی، دکتر فخرائی، و دکتر جاهد مطلق که برای داوری این رساله قبول زحمت نمودند و وقت گرانبهای خود را در اختیار اینجانب قرار دادند، نیز متشکر و سپاسگزارم. بدیهی است، راهنمایی‌های ایشان نیز در تکمیل رساله تاثیر بسزائی داشت.

از کلیه همکاران و دوستان عزیزم به ویژه آقایان دکتر محمودی، دکتر گرگین و دکتر رشادی‌نژاد که در طول مدت تحصیل با اینجانب همکاری نمودند، تقدیر و تشکر می‌نمایم و برای همه آنها آرزوی سلامتی و موفقیت دارم.

از اینکه در دانشگاه شهید بهشتی این دوره تحصیلی را طی کردم، خوشحالم و از هیئت محترم رئیسه دانشکده، آقایان دکتر افجه‌ای، دکتر هاشمی‌پور و دکتر ناظمی و کلیه اساتید عزیز و کارکنان گرانقدر دانشکده، کمال تقدیر و تشکر را می‌نمایم.

در خاتمه از رؤسای محترم دانشکده فنی و مهندسی دانشگاه اصفهان، آقایان دکتر موسوی و دکتر آقامیری و همچنین مدیران محترم گروه کامپیوتر آقایان دکتر نقش‌نیلچی و دکتر جمشیدی، و تمام عزیزانی که در طی این دوره نهایت مساعدت را داشتند، سپاسگزاری و تشکر می‌نمایم.

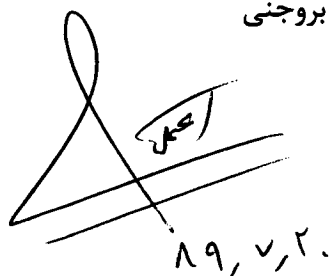
کلیه حقوق مادی مترتب بر نتایج مطالعات،  
ابتکارات و نوآوریهای ناشی از تحقیق موضوع  
این پایان نامه متعلق به دانشگاه شهید بهشتی  
می باشد.

به نام خدا

نام و نام خانوادگی: شهرام اعتمادی بروجنی  
عنوان پایان نامه: نگاشت آشوبناک جدید برای رمزنگاری تصویر  
استاد راهنما: دکتر محمد عشقی

اینجانب شهرام اعتمادی بروجنی تهیه کننده پایان نامه دکتری حاضر، خود را ملزم به حفظ امانت داری و قدردانی از زحمات سایر محققین و نویسندگان بنا بر قانون Copyright می دانم. بدین وسیله اعلام می نمایم که مسئولیت کلیه مطالب درج شده با اینجانب می باشد و در صورت استفاده از اشکال؛ جداول، و مطالب سایر منابع، بلافاصله مرجع آن ذکر شده و سایر مطالب از کار تحقیقاتی اینجانب استخراج گشته است و امانتداری را به صورت کامل رعایت نموده ام. در صورتی که خلاف این مطلب ثابت شود، مسئولیت کلیه عواقب قانونی با شخص اینجانب می باشد.

شهرام اعتمادی بروجنی



امضاء و تاریخ:  
۱۹، ۷، ۲۰

- همه آنان که به من آموختند چگونه بیاموزم و چگونه بیاموزانم،
- پدر بزرگوالم که چگونه زیستن را به من آموخت و عطر وجودش همچون سایه ای از صفا، محبت و صمیمیت بر زندگیم گسترده است،
- مادر مهربانم که عمر شریف خود صرف تربیت من نمود و والاترین تجلی گذشت، صداقت و عطوفت را در زندگی به من نشان داد،
- همسر عزیزم که همواره مشوق و تکیه گاه من در گذر از این مسیر دشوار بود و با بردباری عاشقانه، بار مسئولیت زندگی را بر دوش کشید،
- و فرزندان دلبندم، شکوفه های آرزو و امیدم، که کم توجهی ها و حضور کم مرا تحمل کردند.

## فهرست مطالب

۱	چکیده
۳	فصل ۱: مقدمه
۱۳	فصل ۲: تئوری آشوب و مفاهیم کاربردی آن
۱۴	۱-۲- مقدمه.....
۱۶	۲-۲- آشوب و مفاهیم اساسی.....
۱۷	۱-۲-۲- تعریف آشوب.....
۲۰	۲-۲-۲- نظریه آشوب و مفاهیم مرتبط.....
۲۰	۳-۲-۲- معادله و نمودار بازگشتی.....
۲۱	۳-۲- خصوصیات سیستمهای دینامیک آشوبناک.....
۲۱	۱-۳-۲- جذب کننده های عجیب و پیچیده.....
۲۲	۲-۳-۲- حساسیت بسیار زیاد به شرایط اولیه و نمای لیاپانوف.....
۲۴	۳-۳-۲- شکستگی های ناگهانی ساختاری در مسیر زمانی و دیاگرام دوشاخگی.....
۲۵	۴-۲- نداشت های آشوبناک گسسته یک بعدی.....
۲۶	۲-۴-۲- نداشت لوجستیک.....
۲۷	۳-۴-۲- نداشت خیمه.....
۲۹	۴-۴-۲- نداشت مثلث.....
۳۰	۵-۴-۲- نداشت چبی شف.....
۳۱	۶-۴-۲- نداشت برنولی.....
۳۲	۷-۴-۲- نداشت سینوسی.....
۳۳	۵-۲- نتیجه گیری.....
۳۵	فصل ۳: رمزنگاری تصویر و آشوب
۳۶	۱-۳- اصول رمزنگاری.....
۳۷	۲-۱-۳- رمزنگاری متقارن (با کلید خصوصی).....
۳۹	۱-۲-۱-۳- روش استاندارد رمزنگاری داده DES.....
۴۲	۲-۲-۱-۳- روش استاندارد رمزنگاری پیشرفته AES.....
۴۴	۳-۱-۳- رمزنگاری نامتقارن (با کلید عمومی).....
۴۵	۲-۳- رمزنگاری آشوبناک تصویر.....
۴۹	۳-۳- ارتباط بین سیستم های رمزنگار و تئوری آشوب.....



۳-۴- فضای کلید و حملات مرتبط ..... ۵۰

## فصل ۴: طراحی رمزنگار آشوبناک تصویر در حوزه زمان

۴-۱- مقدمه ..... ۵۴

۴-۲- اصول رمزنگاری آشوبناک ..... ۵۵

۴-۲-۱- نگاشت‌های آشوبناک ..... ۵۶

۴-۲-۲- طرح رمزنگاری آشوبناک ..... ۵۸

۴-۲-۲-۱- جایگشت آشوبناک ..... ۵۸

۴-۲-۲-۲- جانشینی آشوبناک ..... ۶۰

۴-۳- طراحی یک سیستم رمزنگار آشوبناک تصویر ..... ۶۱

۴-۳-۱- واحد جایگشت پیکسل‌ها به صورت آشوبناک ..... ۶۲

۴-۳-۱-۱- مولد رشته بیت‌های باینری تصادفی آشوبناک ..... ۶۴

۴-۳-۱-۲- مولد (محاسب) اعداد صحیح تصادفی ..... ۶۵

۴-۳-۱-۳- الگوریتم Tompkins-Paige ..... ۶۶

۴-۳-۱-۴- جایگشت پیکسل‌ها در یک بعد به کمک نگاشت آشوبناک ..... ۶۷

۴-۳-۱-۵- جایگشت پیکسل‌ها در دو بعد به کمک نگاشت آشوبناک ..... ۶۸

۴-۳-۲- واحد جانشینی پیکسل‌ها به صورت آشوبناک ..... ۶۹

۴-۳-۲-۲- مولد تصویر شبه تصادفی توسط نگاشت خیمه (TPRI) ..... ۷۰

۴-۳-۲-۳- جمع مدولار برای جانشینی پیکسل‌ها به وسیله نگاشت آشوبناک ..... ۷۱

۴-۳-۲-۴- شبیه‌سازی سیستم رمز تصویر به وسیله نگاشت‌های آشوبناک ..... ۷۲

۴-۳-۵- تجزیه و تحلیل امنیت روش ارائه شده ..... ۸۲

۴-۳-۵-۱- هیستوگرام و تست چی دو ..... ۸۲

۴-۳-۵-۲- ضریب همبستگی ..... ۸۳

۴-۳-۵-۳- تفاوت بین تصویر رمز شده و تصویر اصلی ..... ۸۵

۴-۳-۵-۴- بررسی فضای کلید ..... ۸۸

۴-۳-۶- نتیجه‌گیری ..... ۸۹

## فصل ۵: طراحی مولد تصویر شبه تصادفی آشوبناک

۵-۱- مقدمه ..... ۹۲

۵-۲- نگاشت‌های یک بعدی آشوبناک ..... ۹۳

۵-۳- طراحی مولد تصویر شبه تصادفی به وسیله آشوب ..... ۹۶

۵-۳-۱- تولید تصویر شبه تصادفی توسط مولد بیت‌های تصادفی آشوبناک ..... ۹۷

- ۹۸-۳-۲- توليد تصوير شبه تصادفي به وسيله مولد اعداد تصادفي آشوبناک ..... ۹۸
- ۹۸-۵-۴- شبیه سازی مولد تصوير شبه تصادفي به وسيله آشوب ..... ۹۸
- ۱۰۱-۵-۵- محاسبه معيارهاي سنجش و تجزيه و تحليل آنها ..... ۱۰۱
- ۱۰۲-۵-۱- ضريب همبستگي ..... ۱۰۲
- ۱۰۳-۵-۲- هيستوگرام و تست چي دو ..... ۱۰۳
- ۱۰۳-۵-۳- مقايسه تصوير تصادفي واقعي و تصاویر شبه تصادفي آشوبناک ..... ۱۰۳
- ۱۰۵-۵-۴- مقايسه سرعت بوسيله تاخير CPU ..... ۱۰۵
- ۱۰۵-۵-۵- بررسی فضای کلید ..... ۱۰۵
- ۱۰۶-۵-۶- نتیجه گیری ..... ۱۰۶

## فصل ۶: طراحی رمزنگاری آشوبناک تصوير با استفاده از تبدیل فوريه و جایگزینی

- ۱۰۹ پیکسل ها
- ۱۱۰-۱-۶- مقدمه ..... ۱۱۰
- ۱۱۰-۲-۶- مروری بر تبدیل فوريه گسسته و نگاشت های آشوبناک ..... ۱۱۰
- ۱۱۱-۲-۶-۱- تبدیل فوريه گسسته (۲ بعدی) ..... ۱۱۱
- ۱۱۲-۲-۶-۲- توابع آشوبناک ..... ۱۱۲
- ۱۱۲-۲-۶-۲- تابع خيمه ..... ۱۱۲
- ۱۱۳-۲-۶-۳- تابع برنولی ..... ۱۱۳
- ۱۱۳-۳-۶- سیستم رمزنگاری تصوير به وسيله تبدیل فوريه گسسته و جانشینی پیکسل ها ..... ۱۱۳
- ۱۱۵-۳-۶-۲- واحد تبدیل دامنه- فاز با استفاده از نگاشت آشوبناک خيمه ..... ۱۱۵
- ۱۱۶-۳-۶-۳- واحد جانشینی پیکسل ها به وسيله نگاشت آشوبناک برنولی ..... ۱۱۶
- ۱۱۷-۴-۶-۴- شبیه سازی سیستم رمزنگار (آشوبناک) ارائه شده ..... ۱۱۷
- ۱۲۶-۵-۶-۵- تجزيه و تحليل امنيت سیستم ..... ۱۲۶
- ۱۲۶-۵-۶-۱- هيستوگرام و تست چي دو ..... ۱۲۶
- ۱۲۸-۵-۶-۲- میانگین مجذورخطا (MSE) ..... ۱۲۸
- ۱۲۸-۵-۶-۳- ضريب همبستگي ..... ۱۲۸
- ۱۳۰-۵-۶-۴- مقايسه حساسيت به تغيير کلید و تغيير تصوير ..... ۱۳۰
- ۱۳۰-۵-۶-۵- بررسی فضای کلید ..... ۱۳۰
- ۱۳۱-۶-۶-۶- نتیجه گیری ..... ۱۳۱

## فصل ۷: معرفی تابع محراب: یک نگاشت آشوبناک جدید برای رمزنگاری تصوير ۱۳۳

- ۱۳۴-۱-۶-۱- مقدمه ..... ۱۳۴

۱۳۵	۲-۷- تئوری.....
۱۳۶	۳-۷- معرفی نگاشت جدید(نگاشت محراب).....
۱۳۷	۲-۳-۷- معرفی نگاشت محراب مثلثی.....
۱۳۸	۲-۲-۳-۷- بررسی خواص نگاشت محراب مثلثی ۱.....
۱۴۱	۳-۲-۳-۷- بررسی خواص نگاشت محراب مثلثی ۲.....
۱۴۴	۴-۲-۳-۷- بررسی خواص نگاشت محراب مثلثی ۳.....
۱۴۷	۳-۳-۷- معرفی نگاشت محراب خیمه.....
۱۴۹	۲-۳-۳-۷- بررسی خواص نگاشت محراب خیمه ۱.....
۱۵۲	۳-۳-۳-۷- بررسی خواص نگاشت محراب خیمه ۲.....
۱۵۵	۴-۳-۳-۷- بررسی خواص نگاشت محراب خیمه ۳.....
۱۵۷	۴-۳-۷- معرفی نگاشت محراب نهایی.....

## فصل ۸: بررسی عملکرد نگاشت جدید (محراب) در رمزنگار آشوبناک تصویر ۱۶۱

۱۶۲	۱-۸- مقدمه.....
۱۶۲	۲-۸- طراحی مولد تصویر شبه تصادفی آشوبناک با نگاشت محراب.....
۱۶۳	۲-۲-۸- شبیه سازی مولد تصویر شبه تصادفی به وسیله‌ی آشوب.....
۱۶۳	۳-۲-۸- محاسبه معیارهای سنجش و تجزیه و تحلیل آن‌ها.....
۱۶۵	۳-۸- طراحی رمزنگار آشوبناک تصویر در حوزه زمان با نگاشت محراب.....
۱۶۶	۱-۳-۸- بلوک دیاگرام رمزنگار آشوبناک تصویر در حوزه زمان با نگاشت محراب.....
۱۶۷	۲-۳-۸- شبیه سازی رمزنگار آشوبناک تصویر در حوزه زمان با نگاشت محراب.....
۱۷۴	۳-۳-۸- تجزیه و تحلیل امنیت روش ارائه شده.....
۱۷۶	۴-۸- طراحی رمزنگاری آشوبناک تصویر با تبدیل فوریه و جایگزینی پیکسل‌ها بکمک نگاشت محراب.....
۱۷۷	۱-۴-۸- رمزنگاری آشوبناک تصویر با تبدیل فوریه و جایگزینی پیکسل‌ها بکمک نگاشت محراب.....
۱۷۹	۲-۴-۸- شبیه سازی سیستم رمزنگار تصویر با تبدیل فوریه و جایگزینی پیکسل‌ها بکمک نگاشت محراب.....
۱۸۷	۳-۴-۸- تجزیه و تحلیل امنیت سیستم.....

## فصل ۹: نتیجه گیری ۱۹۱

۱۹۲	۱-۹- جمع بندی.....
۱۹۳	۲-۹- نتیجه گیری.....

- ۱۹۸..... ۳-۹- پیشنهاد برای کارهای بعدی
- ۱۹۹..... لیست مقالات مستخرج از رساله

۲۰۱ **مراجع**

۲۰۷ **پیوست‌ها**

۲۰۸..... پیوست الف: واژه‌نامه فارسی به انگلیسی

۲۱۱..... پیوست ب: واژه‌نامه انگلیسی به فارسی

۲۱۴..... پیوست ج: مخفف‌ها

۲۱۶..... پیوست د

## فهرست اشکال

- شکل (۱-۲) نمودار بازگشتی نگاشت لوجستیک ..... ۲۶
- شکل (۲-۲) نمودار مسیر حرکت نگاشت لوجستیک ..... ۲۷
- شکل (۳-۲) دیاگرام دوشاخگی نگاشت لوجستیک ..... ۲۷
- شکل (۴-۲) نمودار بازگشتی نگاشت خیمه ..... ۲۸
- شکل (۵-۲) دیاگرام دوشاخگی نگاشت خیمه ..... ۲۹
- شکل (۶-۲) نمودار بازگشتی نگاشت مثلث ..... ۳۰
- شکل (۷-۲) دیاگرام دوشاخگی نگاشت مثلث ..... ۳۰
- شکل (۸-۲) نمودار بازگشتی نگاشت چپی شف ..... ۳۱
- شکل (۹-۲) دیاگرام دوشاخگی نگاشت چپی شف ..... ۳۱
- شکل (۱۰-۲) نمودار بازگشتی نگاشت برنولی ..... ۳۲
- شکل (۱۱-۲) دیاگرام دوشاخگی نگاشت برنولی ..... ۳۲
- شکل (۱۲-۲) نمودار بازگشتی نگاشت سینوسی ..... ۳۳
- شکل (۱۳-۲) دیاگرام دوشاخگی نگاشت سینوس ..... ۳۳
- شکل (۱-۳) بلوک دیاگرام کلی رمزنگاری متقارن ..... ۳۸
- شکل (۲-۳) بلوک دیاگرام کلی رمزنگار DES ..... ۴۱
- شکل (۳-۳) نمودار گردشی الگوریتم AES ..... ۴۳
- شکل (۴-۳) ساختار کلی رمزنگاری نامتقارن ..... ۴۵
- شکل (۵-۳) رمزنگاری تصویر توسط الگوریتم AES [۳۹] ..... ۴۷
- شکل (۶-۳) رمزنگاری تصویر توسط الگوریتم AES [۴۰] ..... ۴۷
- شکل (۱-۴) نمودارهای بازگشتی نگاشت لوجستیک و خیمه ..... ۵۷
- شکل (۲-۴) بلوک دیاگرام سیستم رمزنگار آشوبناک تصویر ..... ۶۲
- شکل (۳-۴) بلوک دیاگرام واحد جایگشت آشوبناک ..... ۶۴
- شکل (۴-۴) هیستوگرام تابع لوجستیک بر حسب مقدار اولیه  $x_0 = 0.5$  و پارامتر کنترل  $a = 3.9$  ..... ۶۵
- شکل (۵-۴) بلوک دیاگرام واحد جانشینی آشوبناک ..... ۷۰
- شکل (۶-۴) تصویر Peppers به همراه هیستوگرام آن ..... ۷۳
- شکل (۷-۴) یک نمونه از (a) ماتریس واحد و (b) ماتریس جایگشت ..... ۷۴

- شکل (۸-۴) جایگشت سطری تصویر Peppers ..... ۷۵
- شکل (۹-۴) جایگشت ستونی تصویر Peppers ..... ۷۵
- شکل (۱۰-۴) جایگشت دو بعدی تصویر Peppers با کلیدهای یکسان ..... ۷۶
- شکل (۱۱-۴) جایگشت دو بعدی تصویر Peppers با کلیدهای متفاوت ..... ۷۶
- شکل (۱۲-۴) نمونه یک تصویر شبه تصادفی و هیستوگرام آن ..... ۷۷
- شکل (۱۳-۴) نمونه یک تصویر رمز شده و هیستوگرام آن ..... ۷۷
- شکل (۱۴-۴) (a) تصویر Peppers (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۷۸
- شکل (۱۵-۴) (a) تصویر Lake (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۷۸
- شکل (۱۶-۴) (a) تصویر Airplane (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۷۹
- شکل (۱۷-۴) (a) تصویر Baboon (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۷۹
- شکل (۱۸-۴) (a) تصویر Cameraman (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۸۰
- شکل (۱۹-۴) (a) تصویر House (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۸۰
- شکل (۲۰-۴) (a) تصویر Splash (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۸۱
- شکل (۲۱-۴) (a) تصویر صورت (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۸۱
- شکل (۱-۵) دیاگرام دوشاخگی نگاشت تعمیم یافته لوجستیک ..... ۹۵
- شکل (۲-۵) دیاگرام دوشاخگی نگاشت تعمیم یافته خیمه ..... ۹۶
- شکل (۳-۵) بلوک دیاگرام تولید تصویر شبه تصادفی با استفاده از مولد بیت‌های تصادفی آشوبناک ..... ۹۷
- شکل (۴-۵) بلوک دیاگرام تولید تصویر شبه تصادفی به وسیله ی مولد اعداد تصادفی آشوبناک ..... ۹۸
- شکل (۵-۵) a- تصویر شبه تصادفی توسط نگاشت لوجستیک b- هیستوگرام آن ..... ۹۹
- شکل (۶-۵) a- تصویر شبه تصادفی توسط نگاشت خیمه b- هیستوگرام آن ..... ۹۹

- شکل (۵-۷a) - تصویر شبه تصادفی توسط نگاشت چپی شف b- هیستوگرام آن ..... ۱۰۰
- شکل (۵-۸a) - تصویر شبه تصادفی توسط نگاشت دندانان اره‌ای (برنولی) b- هیستوگرام آن ..... ۱۰۰
- شکل (۵-۹a) - تصویر شبه تصادفی توسط نگاشت سینوسی b- هیستوگرام آن ..... ۱۰۰
- شکل (۵-۱۰a) - تصویر شبه تصادفی توسط نگاشت تعمیم یافته لوجستیک b- هیستوگرام آن ..... ۱۰۱
- شکل (۵-۱۱a) - تصویر شبه تصادفی توسط نگاشت تعمیم یافته خیمه b- هیستوگرام آن ..... ۱۰۱
- شکل (۵-۱۲) تصویر تصادفی واقعی ..... ۱۰۴
- شکل (۶-۱) بلوک دیاگرام رمزنگار تصویر به وسیله‌ی تبدیل فوریه گسسته و جانشینی پیکسل‌ها. ۱۱۴
- شکل (۶-۲) بلوک دیاگرام واحد تبدیل دامنه- فاز با استفاده از نگاشت آشوبناک خیمه ..... ۱۱۶
- شکل (۶-۳) بلوک دیاگرام واحد جانشینی پیکسل‌ها به وسیله‌ی نگاشت آشوبناک برنولی ..... ۱۱۷
- شکل (۶-۴a) ( تصویر Peppers b) هیستوگرام، c) فاز d) دامنه ..... ۱۱۸
- شکل (۶-۵a) ( تصویر شبه تصادفی خیمه b) هیستوگرام آن، c) فاز آن d) دامنه آن ..... ۱۱۹
- شکل (۶-۶a) (فاز جدید b) دامنه جدید c) تصویر رمز شده I d) هیستوگرام آن ..... ۱۲۰
- شکل (۶-۷a) ( تصویر شبه تصادفی برنولی b) هیستوگرام c) تصویر رمز شده II d) هیستوگرام ..... ۱۲۱
- شکل (۶-۸a) ( تصویر Peppers b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۲
- شکل (۶-۹a) ( تصویر Lake b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر .. ۱۲۲
- شکل (۶-۱۰a) ( تصویر Airplane b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۳
- شکل (۶-۱۱a) ( تصویر Baboon b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۳
- شکل (۶-۱۲a) ( تصویر Cameraman b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۴
- شکل (۶-۱۳a) ( تصویر House b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۴
- شکل (۶-۱۴a) ( تصویر Splash b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۵
- شکل (۶-۱۵a) ( تصویر صورت b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۲۵

- شکل (۶-۱۶) هیستوگرام تصاویر رمز شده‌ی مقالات (a) Prasanna و سایرین (b) Wang و سایرین  
 ۱۲۷ .....Sinha و Singh(c)
- شکل (۷-۱) حالت‌های مختلف نمودار بازگشتی نگاشت محراب مثلثی برای  $r=1$  و  $r=0.5$  ..... ۱۳۸
- شکل (۷-۲) ، نمودار مسیر حرکت برای دو مقدار اولیه  $0.750$  و  $0.751$  به ازای  $r=0.95$  ..... ۱۳۹
- شکل (۷-۳) دیاگرام دوشاخگی برحسب پارامتر  $r$  ..... ۱۳۹
- شکل (۷-۴) نمودار نمای لپایانوف برحسب پارامتر  $r$  ..... ۱۴۰
- شکل (۷-۵) هیستوگرام / تابع توزیع احتمال به ازای  $r=0.95$  ..... ۱۴۱
- شکل (۷-۶) ، نمودار مسیر حرکت برای دو مقدار اولیه  $0.750$  و  $0.751$  به ازای  $r=0.95$  ..... ۱۴۲
- شکل (۷-۷) دیاگرام دوشاخگی برحسب پارامتر  $r$  ..... ۱۴۳
- شکل (۷-۸) نمودار نمای لپایانوف برحسب پارامتر  $r$  ..... ۱۴۳
- شکل (۷-۹) هیستوگرام / تابع توزیع احتمال به ازای  $r=0.95$  ..... ۱۴۴
- شکل (۷-۱۰) ، نمودار مسیر حرکت برای دو مقدار اولیه  $0.750$  و  $0.751$  به ازای  $r=0.95$  ..... ۱۴۵
- شکل (۷-۱۱) دیاگرام دوشاخگی برحسب پارامتر  $r$  ..... ۱۴۵
- شکل (۷-۱۲) نمودار نمای لپایانوف برحسب پارامتر  $r$  ..... ۱۴۶
- شکل (۷-۱۳) هیستوگرام / تابع توزیع احتمال به ازای  $r=0.95$  ..... ۱۴۶
- شکل (۷-۱۴) حالت‌های ممکن نگاشت محراب خیمه  $a=0.3$  ..... ۱۴۸
- شکل (۷-۱۵) حالت‌های ممکن نگاشت محراب خیمه  $a=0.5$  ..... ۱۴۸
- شکل (۷-۱۶) حالت‌های ممکن نگاشت محراب خیمه  $a=0.7$  ..... ۱۴۹
- شکل (۷-۱۷) ، نمودار مسیر حرکت برای دو مقدار اولیه  $0.750$  و  $0.751$  به ازای  $a=0.45$  ..... ۱۵۰
- شکل (۷-۱۸) دیاگرام دوشاخگی برحسب پارامتر  $a$  ..... ۱۵۱
- شکل (۷-۱۹) نمودار نمای لپایانوف برحسب پارامتر  $a$  ..... ۱۵۱
- شکل (۷-۲۰) هیستوگرام / تابع توزیع احتمال به ازای  $a=0.45$  ..... ۱۵۲
- شکل (۷-۲۱) نمودار مسیر حرکت برای دو مقدار اولیه  $0.750$  و  $0.751$  به ازای  $a=0.45$  ..... ۱۵۳
- شکل (۷-۲۲) دیاگرام دوشاخگی برحسب پارامتر  $a$  ..... ۱۵۳
- شکل (۷-۲۳) نمودار نمای لپایانوف برحسب پارامتر  $a$  ..... ۱۵۴
- شکل (۷-۲۴) هیستوگرام / تابع توزیع احتمال به ازای  $a=0.45$  ..... ۱۵۴
- شکل (۷-۲۵) نمودار مسیر حرکت برای دو مقدار اولیه  $0.750$  و  $0.751$  به ازای  $a=0.45$  ..... ۱۵۵
- شکل (۷-۲۶) دیاگرام دوشاخگی برحسب پارامتر  $a$  ..... ۱۵۶



- شکل (۷-۲۷) نمودار نمای لپایانوف برحسب پارامتر  $a$  ..... ۱۵۶
- شکل (۷-۲۸) هیستوگرام / تابع توزیع احتمال به ازای  $a=0.45$  ..... ۱۵۷
- شکل (۷-۲۹) دیاگرام دوشاخگی برحسب پارامترهای  $a$  و  $r$  ..... ۱۵۸
- شکل (۷-۳۰) نمودار نمای لپایانوف برحسب پارامترهای  $a$  و  $r$  ..... ۱۵۹
- شکل (۸-۳) بلوک دیاگرام واحد جانشینی آشوبناک ..... ۱۶۷
- شکل (۸-۴) جایگشت دو بعدی تصویر Peppers ..... ۱۶۸
- شکل (۸-۵) نمونه یک تصویر شبه تصادفی با نگاشت محراب و هیستوگرام آن ..... ۱۶۸
- شکل (۸-۶) نمونه یک تصویر رمز شده و هیستوگرام آن ..... ۱۶۹
- شکل (۸-۷) (a) تصویر Peppers (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۰
- شکل (۸-۸) (a) تصویر Lake (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۰
- شکل (۸-۹) (a) تصویر Airplane (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۱
- شکل (۸-۱۰) (a) تصویر Baboon (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۱
- شکل (۸-۱۱) (a) تصویر Cameraman (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۲
- شکل (۸-۱۲) (a) تصویر House (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۲
- شکل (۸-۱۳) (a) تصویر Splash (b) تصویر جایگشت شده (c) تصویر رمز شده نهائی (d,e,f) هیستوگرام تصاویر ..... ۱۷۳
- شکل (۸-۱۴) (a) تصویر صورت (b) تصویر رمز شده (c) تصویر رمز شده II (d,e,f) هیستوگرام تصاویر ..... ۱۷۳
- شکل (۸-۱۵) بلوک دیاگرام رمزنگاری آشوبناک تصویر با تبدیل فوریه و جایگزینی پیکسل ها بکمک نگاشت محراب ..... ۱۷۷
- شکل (۸-۱۶) بلوک دیاگرام واحد تبدیل دامنه- فاز با استفاده از نگاشت آشوبناک محراب ..... ۱۷۸
- شکل (۸-۱۷) بلوک دیاگرام واحد جانشینی پیکسل ها به وسیله نگاشت آشوبناک محراب ..... ۱۷۹
- شکل (۸-۱۸) (a) تصویر شبه تصادفی محراب (b) هیستوگرام آن، (c) فاز آن (d) دامنه آن ..... ۱۸۰

- شکل (۸-۱۹) a) فاز جدید b) دامنه جدید c) تصویر رمز شده d) هیستوگرام آن ..... ۱۸۱
- شکل (۸-۲۰) a) تصویر شبه تصادفی محراب b) هیستوگرام c) تصویر رمز شده II d) هیستوگرام ... ۱۸۲
- شکل (۸-۲۱) a) تصویر Peppers b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۳
- شکل (۸-۲۲) a) تصویر Lake b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۳
- شکل (۸-۲۳) a) تصویر Airplane b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۴
- شکل (۸-۲۴) a) تصویر Baboon b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۴
- شکل (۸-۲۵) a) تصویر Cameraman b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۵
- شکل (۸-۲۶) a) تصویر House b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۵
- شکل (۸-۲۷) a) تصویر Splash b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۶
- شکل (۸-۲۸) a) تصویر صورت b) تصویر رمز شده c) تصویر رمز شده II d,e,f) هیستوگرام تصاویر ..... ۱۸۶
- شکل (۹-۱) نمودار مقایسه مقدار تست چی دو هیستوگرام تصاویر رمز شده در روشهای مختلف ..... ۱۹۵
- شکل (۹-۲) نمودار مقایسه MSE تصاویر رمز شده در روشهای مختلف ..... ۱۹۵
- شکل (۹-۳) نمودار مقایسه ضریب همبستگی تصاویر رمز شده در روشهای مختلف ..... ۱۹۶
- شکل (۹-۴) نمودار مقایسه تاخیر عملکرد در روشهای مختلف ..... ۱۹۷
- شکل (۹-۵) نمودار مقایسه طول کلید در روشهای مختلف ..... ۱۹۷

## فهرست جداول

- جدول (۱-۳) ارتباط بین سیستم های رمزنگار و تئوری آشوب ..... ۴۹
- جدول (۱-۴) ضریب همبستگی پیکسل های تصویر در سه جهت افقی، عمودی و مورب ..... ۸۴
- جدول (۲-۴) مقایسه ضرایب همبستگی روش ارائه شده با روشهای مشابه ..... ۸۵
- جدول (۳-۴) مقایسه MAE جایگشت و جایگشت+جانشینی ..... ۸۶
- جدول (۴-۴) مقایسه NPCR , UACI روش ارائه شده با چند روشهای مشابه ..... ۸۷
- جدول (۵-۴) مقایسه فضای کلید ..... ۸۸
- جدول (۱-۵) ضرایب همبستگی افقی، عمودی و مورب تصاویر شبه تصادفی ..... ۱۰۲
- جدول (۲-۵) مقادیر تست چی دو برای هیستوگرام تصاویر شبه تصادفی آشوبناک ..... ۱۰۳
- جدول (۳-۵) مقایسه تصویر تصادفی واقعی و تصاویر شبه تصادفی آشوبناک ..... ۱۰۴
- جدول (۴-۵) مقایسه زمان تلف شده CPU بر حسب ثانیه ..... ۱۰۵
- جدول (۵-۵) طول و فضای کلید نگاشتهای مختلف ..... ۱۰۶
- جدول (۱-۶) ضریب همبستگی و تست چی دو تصویر اصلی ..... ۱۲۹
- جدول (۲-۶) مقایسه ضریب همبستگی, MSE و تست چی دو تصاویر رمز شده با الگوریتم ارائه شده ..... ۱۲۹
- جدول (۳-۶) مقایسه تست چی دو, MSE و ضریب همبستگی تصویر رمز شده در روشهای مختلف ..... ۱۲۹
- جدول (۴-۶) مقایسه حساسیت به تغییر کلید و تغییر تصویر ..... ۱۳۰
- جدول (۱-۸) ضرایب همبستگی افقی، عمودی و مورب تصویر شبه تصادفی محراب ..... ۱۶۴
- جدول (۲-۸) مقادیر تست چی دو برای هیستوگرام تصویر شبه تصادفی محراب ..... ۱۶۴
- جدول (۳-۸) مقایسه زمان تلف شده CPU برای تصویر شبه تصادفی محراب ..... ۱۶۵
- جدول (۴-۸) مقایسه ضرایب همبستگی روش ارائه شده با فصل ۴ ..... ۱۷۵
- جدول (۵-۸) مقایسه MAE روش ارائه شده با فصل ۴ ..... ۱۷۵
- جدول (۶-۸) مقایسه NPCR , UACI روش ارائه شده با چند روش فصل ۴ ..... ۱۷۶
- جدول (۷-۸) مقایسه تست چی دو, MSE و ضریب همبستگی تصویر رمز شده با روش فصل ۶ ..... ۱۸۸
- جدول (۸-۸) مقایسه حساسیت به تغییر کلید و تغییر تصویر ..... ۱۸۸
- جدول (۹-۸) مقایسه تست چی دو, MSE و ضریب همبستگی تصویر رمز شده در روشهای مختلف ..... ۱۸۹
- جدول (۱۰-۸) مقایسه سرعت عملکرد و طول کلید ..... ۱۹۰

