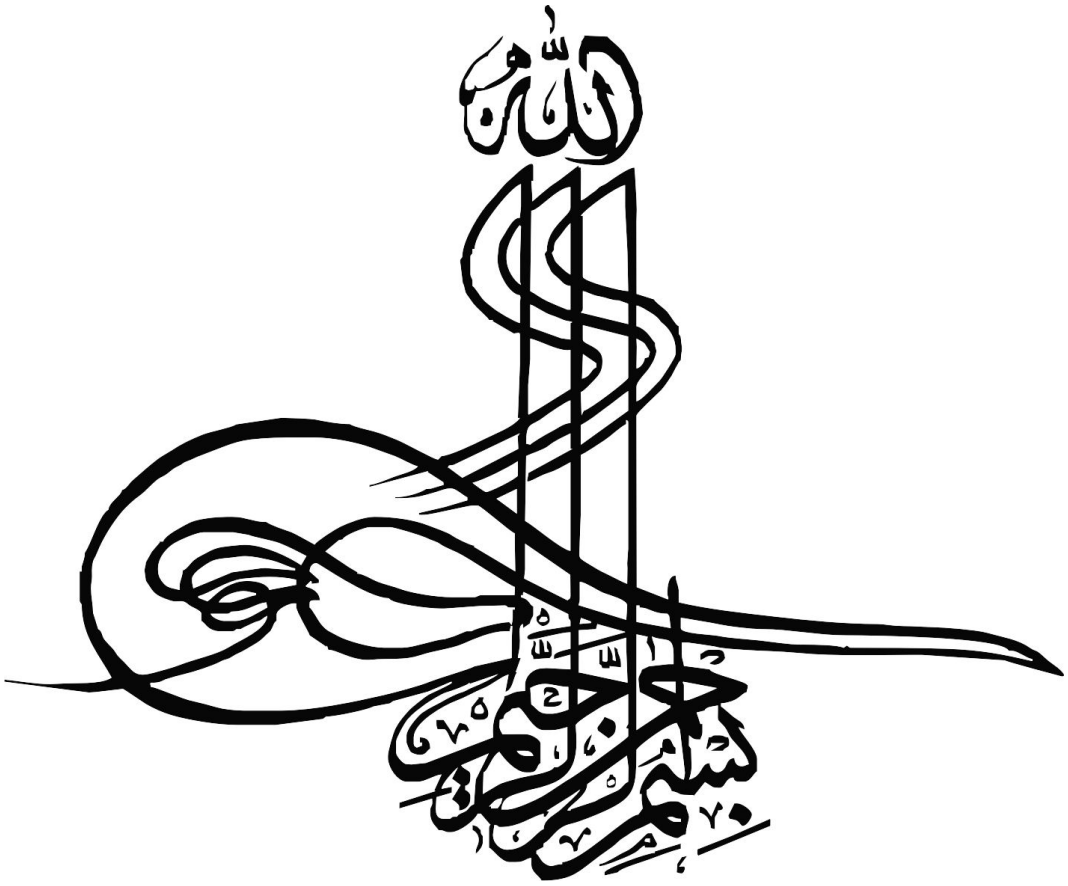

دانشکده علوم

گروه ریاضی

پایان نامه جهت اخذ درجه کارشناسی ارشد رشته ی ریاضی محض

عنوان پایان نامه:

تحلیل رمز یک روش رمزنگاری تصویر مبتنی بر تابع آشوب

استاد راهنما:

نگارش:

شهریور

دانشکده علوم

گروه ریاضی

پایان نامه جهت اخذ درجه کارشناسی ارشد رشته ی ریاضی محض

نگارش:

عنوان پایان نامه:

تحلیل رمز یک روش رمزنگاری تصویر مبتنی بر تابع آشوب

در تاریخ توسط هیات داوران زیر بررسی و با درجه به تصویب نهایی رسید.

۱.استاد راهنما: با مرتبه علمی استادیار امضا

۲.استاد داور داخل گروه: با مرتبه علمی امضا

۳.استاد داور خارج گروه: دکتر با مرتبه علمی امضا

ای خدای من...

ای آفریدگار من، ای همه ی هستیم، بر من این نعمت را ارزانی دار که:

بیشتر در پی تسلا دادن باشم تا تسلا یافتن
بیشتر در پی فهمیدن باشم تا فهمیده شدن
بیشتر پی دوست داشتن باشم تا دوست داشته شدن

زیرا در بخشیدن است که می یابیم
و در عفو کردن است که بخشیده می شویم
و در مردن است که حیات جاوید می یابیم

سپاس گزاری...

سپاس خداوندگار حکیم را که با لطف بی‌کران خود، آدمی را زیور عقل آراست.

در آغاز وظیفه خود می‌دانم از زحمات بی‌دریغ پدر و مادرم که از ابتدای عمر همراه با من، همگام با من، برای رسیدن به مدارج بالای انسانی برایم تلاش کردند. از استاد راهنمای خوبم، ه صمیمانه تشکر و قدردانی می کنم چرا که قطعاً بدون تلاش و راهنمایی های ارزنده ایشان، در طی این مدت، این مجموعه به انجام نمی‌رسید.

در پایان، بوسه می‌زنم بر دستان خداوندگاران مهر و مهربانی، پدر و مادر عزیزم و بعد از خدا، ستایش می‌کنم وجود مقدس‌شان را و تشکر می‌کنم از برادران و خواهر عزیزم به پاس عاطفه سرشار و گرمای امیدبخش وجودشان، که در این سردترین روزگاران، بهترین پشتیبان من بودند.

تقدیم به همه آنهایی که

برای سرفرازی این مرز و بوم تلاش

کرده و می کنند.

چکیده

در این نوشتار روش رمزنگاری تصویر با استفاده از روش ارائه شده توسط $Huang$ و همکاران را مورد تحلیل و بررسی قرار می دهیم و نقایص آن را یافته و آنها را برطرف می نماییم. در ادامه به بررسی الکوریتم اصلاح شده از لحاظ امنیت و کارایی می پردازیم. سرانجام، الگوریتم رمزنگاری نوینی را مبتنی بر نگاشت آشوب لجستیک پیشنهاد داده و با استفاده از آزمونهای مختلف نشان می دهیم که از لحاظ امنیت و کارایی دارای مولفه های بسیار مطلوبی است.

واژه های کلیدی: رمزنگاری تصویر، تابع چی بیشف، آشوب، انتشار، مولد کلید جاری، تحلیل رمز

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فصل ۱

مقدماتی در رمزنگاری

۱.۱ مقدمه

در دنیای امروز، با رشد اینترنت و امکانات ارتباطی دیگر، نقش امنیت و تضمین صحت اطلاعات بیشتر و بیشتر می گردد. از طرفی چون پیچیدگی های روابط انسانی مانند اعتماد متقابل در روابط الکترونیکی وجود ندارند، از این رو بایستی یک علم شرایط را آماده و این روابط را تضمین نماید. یکی از متداولترین روشهای حفاظت اطلاعات، رمز نمودن آنها است، طوری که دستیابی به اطلاعات رمز شده برای افرادِ غیر مجاز، امکان پذیر نبوده و صرفا افرادی مشخص قادر به باز نمودن رمز و استفاده از اطلاعات باشند. در طول تاریخ، رمزنگاری، جزئی از جنگ، سیاست و حکومت اداری بوده است. برای مثال در قرن شانزدهم ملکه اسکاتلند به خاطر رمزگشایی پیغامی رمزی که در زندان و اسارت به شاه فرستاده بود، جانش را از دست داد.

رمزنگاری یکی از شاخه های ریاضی و علوم کامپیوتر دانسته می شود. همچنین این علم دارای رابطه تنگاتنگی با علوم نظریه اطلاعات ، امنیت رایانه ای و مهندسی است. رمزنگاری و ابزارهای مربوط به آن در طی قرن ها رشد کرده و در الگوریتم های کامپیوتری و سیستم های مدرن امروزی به اوج خود رسیدند. رمزنگاری مدرن علاوه بر رمزنگاری ، شاخه های مهم دیگری را نیز در بر می گیرد که از جمله آنها رمزنگاری نامتقارن ، توابع فشرده ساز، اهراز هویت پیام و افراد، اعداد تصادفی، امضاهای دیجیتال و ... می توان نام برد. علم رمزنگاری علاوه بر جذابیت و ویژگی های منحصر بفرد خود که آنها را از هویت رمزگونه خویش که با ریاضیات نیز در تعامل است بدست آورده، پیچیدگی بسیار زیادی نیز داراست؛ تا حدی که بسیاری از بزرگان ریاضی و رمزنگاری روز، این علم را از دشوارترین علوم شمرده اند. برای مثال برای تسلط کافی به مباحث رمزنگاری از جمله آنتروپی اطلاعات، تلاش بسیار کافی نیست بلکه فرد باید تفکر رمزنگاری داشته باشد.

امروزه رمزنگاری با جذب پرتلاش ترین دانشمندان و نوابغ جهان، با رشدی باور نکردنی روند رسیدن به پرکاربردترین علوم را طی می کند. بطور کلی روند تکامل رمزنگاری را می توان به چهار مرحله ریز تقسیم کرد:

مرحله اول: از سیستم های ساده جانشینی و جابجایی برای رمزنگاری استفاده شد. در این مرحله بیشتر قلم و کاغذ و ماشین های ساده مکانیکی مورد استفاده قرار گرفتند(مانند سیستم سزار و سیستم اسپارتان)

مرحله دوم: از آغاز قرن بیستم شروع و تا دهه ۱۹۵۰ ادامه می یابد. در این مرحله از سیستم های پیچیده مکانیکی و الکترو مکانیکی استفاده شد و به تبع آن سیستم های رمزنگاری پیچیده تری ابداع گردید.(مانند سیستم H۲۰۹ و یا ماشین Haglin)

مرحله سوم: که با انتشار مقالات بسیار مهم شانون[۱] در سالهای ۱۹۴۸ و ۱۹۴۹ پیشرفت سریع در صنایع

[۱] Shannon

میکروالکترونیک در دهه ۱۹۶۰ شروع می شود و هنر رمزنگاری به علم رمزنگاری مبدل می گردد.

مرحله چهارم: که از اواخر دهه ۱۹۷۰ با پیشنهاد سیستم های رمزنگاری با کلید همگانی شروع می شود و تا امروز ادامه دارد.

۲.۱ تعاریف اساسی

رمزنگاری[۱] از دو واژه رمز [۲] و نگارش [۳] پدید آمده است. هدف این علم بررسی و مطالعه اطلاعات رمزی و مخفی می باشد. این علم همانند هر علمی دیگر اصطلاحات پایه ای و بخصوصی دارد که در ادامه با آنها آشنا خواهیم شد.

تعریف ۱.۲.۱. به هر گونه محاسبه و عملی که منجر به مخفی و پنهان شدن متن یا اطلاعات شود، رمزگذاری[۴] گفته می شود.

تعریف ۲.۲.۱. به هر گونه سعی و تلاش برای کشف رمز و خواندن اطلاعات مخفی شده رمزگشایی[۵] گویند.

تعریف ۳.۲.۱. به متنی که قصد پنهان و مخفی کردن آن را داریم، متن آشکار[۶] گویند.

تعریف ۴.۲.۱. متن رمز[۷] به متن پنهان و مخفی گویند که پس از عملیات رمزنگاری بدست می آید و توسط انسان قابل فهم نیست.

تعریف ۵.۲.۱. روشی که برای رمز کردن متن آشکار بکار گرفته می شود را الگوریتم[۸] می نامند.

تعریف ۶.۲.۱. کلید رمز[۹] اطلاعاتی معمولاً عددی است که به عنوان پارامتر ورودی به الگوریتم رمز داده می‌شود و عملیات رمزنگاری و رمزگشایی با استفاده از آن انجام می‌گیرد. انواع مختلفی از کلیدهای رمز در رمزنگاری تعریف و استفاده می‌شود.

---

۱ Cryptography
۲ Crypt
۳ Graphy
۴ Encryption
۵ Decryption
۶ Plaintext
۷ Ciphertext
۸ Algorithm
۹ Key

تعریف ۷.۲.۱. به قوانین و قرار دادهای مورد توافق دو طرف در نحوه تبادل اطلاعات پروتکل گفته می شود. ولی وقتی در علم رمزنگاری بحث از پروتکل ها رمزنگاری می شود، منظور نحوه تبادل اطلاعات رمز شده می باشد.

تعریف ۸.۲.۱. به هنر شکستن متن رمز بدون استفاده از کلید، تحلیل رمز[۱] گفته می شود.

تعریف ۹.۲.۱. یک سیستم رمزنگاری دارای پنج مولفه $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \xi, \mathcal{D})$ است که به آنها پارامترهای رمزنگاری گفته می شود:

الف_ فضای متناهی از متن آشکار[۲] که معمولا با $\mathcal{P}$ نمایش می دهند.

ب_ فضای متناهی از متن رمز شده[۳] که این نیز با $\mathcal{C}$ نمایش داده می شود.

ج_ فضای کلید[۴]مجموعه از کلید های ممکن است و با $\mathcal{K}$ نمایش داده می شود.

د_ برای هر $k \in K$ یک تابع رمزگذاری e_k و متناظر با آن تابع رمزگشایی d_k وجود دارد بطوری که:

$$e_k : \mathcal{P} \longrightarrow \mathcal{C}$$

$$d_k : \mathcal{C} \longrightarrow \mathcal{P}$$

و داریم:

$$\forall x \in \mathcal{P} : d_k(e_k(x)) = x.$$

[۱] cryptanalysis
[۲] Plaintext space
[۳] ciphertext space
[۴] Key space

فصل ۲

الگوریتم رمزنگاری تصویر مبتنی بر توابع آشوب

که x_i و y_i، iـامین جفت پیکسل همجوار عمودی یا افقی یا قطری است و N تعداد کل جفت پیکسل ها در هر قسمت است و $E(x)$ و $E(y)$ میانگین ارزش پیکسل های تصویر اصلی و تصویر رمز شده است. برای یک تصویر مقدار همبستگی به عدد ۱ نزدیک و برای یک تصویر رمزشده توسط سیستم رمزنگاری ایده آل این کمیت باید نزدیک به صفر باشد.

در تصاویر مختلف رمزنگاری شده ما بطور تصادفی ۳۶۰۰ جفت از پیکسل های همجوار به صورت عمودی، افقی و قطری انتخاب نموده و نتایج را در جدول زیر ارائه داده ایم.

تصویر	اندازه تصویر	همبستگی افقی	همبستگی عمودی	همبستگی قطری
برنج	۱۲۸×۱۲۸	۰,۰۱۵۶	۰,۰۱۰۴	۰,۰۰۹۵
مرد عکاس	۲۵۶×۲۵۶	۰,۰۰۷۶	۰,۰۰۷۹	۰,۰۰۶۰
لنا	۵۱۲×۵۱۲	۰,۰۱۳۴	۰,۰۱۶۶	۰,۰۰۷۴

جدول ۱.۲: مقادیر همبستگی پیکسل های همجوار برای تصاویر مختلف رمز شده

۱.۰.۲ آنتروپی

یکی دیگر از مولفه های یک سیستم رمزنگاری میزان پیش بینی ناپذیری تصاویر رمزشده حاصل از آن است. این میزان توسط مفهومی به نام آنتروپی[۱] سنجیده می شود. در حالت کلی آنتروپی، میزان تصادفی بودن یک رخداد را نشان می دهد. آنتروپی اطلاعات یک نظریه ریاضی است که بر مبنای آن ارتباط داده ای و ذخیره سازی اطلاعات توسط آن آزمایش می شود که در سال ۱۹۴۹توسط کلود شانون معرفی شده است]۱۷[. یکی از راه های دست آوردن آنتروپی استفاده از رابطه زیر است: پس در یک سیستم رمزنگاری مناسب تصاویر ایجاد شده باید مقدار آنتروپی ای نزدیک به ۸ داشته باشند. همانطور که در جدول ۲,۲ می بینید مقدار آنتروپی برای تصاویر مختلف محاسبه شده است. نتایج جدول ۲,۲ نشان می دهد که روش پیشنهادی تصاویری کاملا تصادفی و غیر قابل پیش بینی ایجاد می کند که نشان دهنده امنیت بسیار بالایی برای این سنجش است.

[۱] Entropy

تصویر	اندازه تصویر	مقدار آنتروپی
مرد عکاس	۲۵۶×۲۵۶	۷,۹۹
شامپانزه	۱۷۵×۱۷۹	۷,۹۹۳
فلفل	۲۵۵×۲۵۲	۷,۹۹۷

جدول ۲.۲: مقادیر آنتروپی برای تصاویر مختلف رمز شده

۲.۰.۲ مقایسه با روش های مشابه

در روش رمزنگاری که در مراجع ذکر شده اند و مبتنی بر روش DNA انجام می پذیرند، چون در هر راند از رمزنگاری ابتدا باید پیکسل ها را به $ASCII$ تبدیل کرده و سپس عملیات رمزنگاری را برای اعداد ۰۰ ،۰۱ ،۱۰ ،۱۱ انجام داد و دوباره پیکسل ها را به اعداد اعشاری تبدیل کرد. این پروسه مدت زمان بسیاری می طلبد. همچنین ترتیب عادی معادلات نیز می تواند زمان زیادی برای سیستم های آشوب با بعد بالا مهم باشد مراجع ۱۱و ۶. در این روش، سیستم رمزنگاری از یک تابع ساده بهره برده در نتیجه مدت زمان رمزنگاری برای یک تصویر ۲۵۶×۲۵۶ برابر با ۰,۶۵۶ ثانیه می باشد. جدول ۳,۲ مدت زمان رمزنگاری تصاویر مختلف را در یک راند با مراجع ۱۱ و ۶ نشان می دهد. مقادیر نشان می دهد از این روش می توان برای کاربرد های بلادرنگ تصویری استفاده کرد.

اندازه تصویر	روش پیشنهادی	مرجع [۱۱]	مرجع [۶]
۲۵۶×۲۵۶	۰,۶۵۶s	>۱,۶۰۹s	>۰,۶۷۲s
۵۱۲×۵۱۲	۱,۱۴۴s	>۴,۰۷۸s	>۲,۶۸۸s
۱۰۲۴×۰۲۴	۵,۰۹۷s	>۲۸,۷۵۰s	>۱۰,۷۹۷s

جدول ۳.۲: مدت زمان رمزنگاری برای تصاویر مختلف

مرجع [؟] یک نمونه پروژه دکترا و مرجع [؟] یک نمونه مقاله مجله فارسی است. مرجع [؟] یک نمونه مقاله کنفرانس فارسی و مرجع [؟] یک نمونه کتاب فارسی با ذکر مترجمان و ویراستاران فارسی است. مرجع [؟] یک نمونه پروژه کارشناسی ارشد انگلیسی و [؟] هم یک نمونه متفرقه می‌باشند.

مرجع [؟] یک نمونه کتاب لاتین است که از آنجا که دارای فیلد authorfa است، نام نویسندگان آن در استیلهای asa-fa، plainnat-fa و chicago-fa به فارسی دیده می‌شود. مرجع [؟] مقاله انگلیسی است که معادل فارسی نام نویسندگان آن ذکر نشده بوده است.