به نام خداوند جان و خرد

کزین برتر اندیشه برنگذرد

دانشگاه یزد

دانشکده مهندسی برق و کامپیوتر

گروه مهندسی کامپیوتر

پایان‌نامه

جهت دریافت درجه کارشناسی ارشد

مهندسی کامپیوتر

گرایش هوش مصنوعی و رباتیک

ارائه یک روش جدید رمزنگاری بصری رنگی با استفاده از الگوریتم ژنتیک

استاد راهنما:

دکتر علی‌محمد لطیف

استاد مشاور:

دکتر محمد قاسم‌زاده

پژوهش‌گر:

دانیال تقدس

تابستان ۱۳۹۲

تقدیم به

پدر و مادر عزیزم

که تمام زندگی خویش را مدیون آن‌ها هستم

و همه کسانی که درست اندیشیدن را به من آموختند.

سپاس‌گزاری

سپاس بی‌کران **پدر و مادرم** را که از ذره ذره‌ی جان خویش مرا پروراندند و در راه علم و انسانیت نهادند.

سپاس ویژه **جناب آقای دکتر لطیف** را که با صبر و دقتی مثال زدنی درست و نادرست را به من نشان دادند.

سپاس **جناب آقای دکتر قاسم‌زاده** را که راهنمایی‌های ایشان برای همیشه سرلوحه‌ی کار من است.

سپاس سایر اساتیدم را که شمع وجود خود را چراغ راه علم قرار داده‌اند.

سپاس همه‌ی دوستانم را که مرا یاری، همراهی و کمک کردند.

و سپاس همه‌ی پویندگان راه علم را که در تمامی تاریخ بشریت جز به بهتر کردن زندگی سایرین نیندیشیدند.

چکیده

با توجه به توسعه‌ی فناوری اطلاعات، امنیت بخشی جدا نشدنی از دنیای ارتباطات است. تاکنون روش‌های متعددی برای ارتباط امن بین مبدأ و مقصد ارائه شده‌اند که رمزنگاری یک دسته از این روش‌ها است. با توجه به استفاده فراوان از تصاویر دیجیتال در دنیای امروزی، رمزنگاری تصویر توسعه‌ی فراوانی یافته است. اغلب این روش‌ها با استفاده از کلید، تصویر محرمانه را به یک تصویر درهم‌ریخته تبدیل می‌کنند که اطلاعاتی به سایرین نمی‌دهد. گیرنده‌ی دارای صلاحیت، با داشتن کلید می‌تواند با محاسبات معکوس تصویر را رمزگشایی کند. نقطه ضعف این الگوریتم‌ها نیاز به محاسبات برای رمزگشایی است.

یکی از شاخه‌های نوین رمزنگاری تصویر، رمزنگاری بصری است. رمزنگاری بصری تبدیل یک تصویر به دو یا چند تصویر درهم‌ریخته است به طوری که تصویرهای تولید شده به تنهایی دارای اطلاعات خاصی نیستند اما اگر چاپ شده و برهم‌گذاشته شوند، نمایه‌ای قابل فهم از تصویر اصلی را تولید می‌کنند. خاصیت اصلی این روش عدم نیاز به دستگاه‌های پردازشگر برای بازیابی تصویر است و عملیات رمزگشایی توسط سیستم بینایی انسان انجام می‌پذیرد. اغلب روش‌های ارائه شده برای رمزنگاری بصری به رمزنگاری تصاویر دودویی محدود می‌شوند. هم‌چنین روش‌های رمزنگاری بصری تصاویر سطوح خاکستری و رنگی محتوای تصویر محرمانه را تغییر می‌دهند و تصاویر بازیابی شده در این روش‌ها دچار تغییر اندازه می‌شوند. با توجه به این مسئله در این پایان‌نامه یک روش جدید برای رمزنگاری تصاویر سطوح خاکستری و رنگی با استفاده از الگوریتم ژنتیک ارائه شده است. در این روش تصویر اول به صورت تصادفی تولید می‌شود. سپس با استفاده از الگوریتم ژنتیک و با تعریف یک تابع برازندگی مناسب، سعی شده تصویر دوم به گونه‌ای محاسبه گردد که در صورت برهم‌گذاری نمایه‌ای از تصویر اصلی را تولید نماید. از مزایای این روش می‌توان به هم‌اندازه بودن تصاویر رمز با تصویر اصلی اشاره کرد. نتایج حاصل از آزمایشات نشان می‌دهد تصاویر تولیدی از این روش از کیفیت بصری مناسبی برخوردار هستند.

کلید واژه‌ها: رمزنگاری تصاویر، رمزنگاری بصری، تصاویر سطوح خاکستری، تصاویر رنگی، الگوریتم ژنتیک، جستجوی هوشمند

فهرست مطالب

فهرست تصاویر

فهرست جداول

فصل ۱

مقدمه

۱.۱ مقدمه

امنیت یکی از مهم‌ترین مسائل در ارتباطات است. از دیر باز تاکنون رمزنگاری اصلی‌ترین روش امن کردن ارتباط بوده است. ارتباطات دیجیتال نیز از این امر مستثنی نیستند. افزایش روزافزون امکانات تولید و انتشار تصاویر، محافظت و مکانیزم‌های جدید اشتراک‌گذاری[۱] و کنترل دسترسی[۲] را برای تصاویر منتشر شده می‌طلبد.

تاکنون روش‌های مختلفی برای رمزنگاری تصویر ارائه شده‌اند که هر کدام مزایا و معایب خاص خود را دارند. تکنیک‌های اشتراک‌گذاری امن تصاویر با ارائه راه حل‌های نوین، برای توسعه کاربردهای تصویرپردازی امن نسبت به روش‌های سنتی رمزنگاری ارجحیت دارند. یکی از این تکنیک‌ها رمزنگاری بصری[۳] است؛ که به صاحب رمز این امکان را می‌دهد تا اطلاعات تصویر را از طریق کانال‌های ارتباطی عمومی بین مشترکان توزیع کند. این تکنیک از تصویر محرمانه، چند تصویر به ظاهر درهم‌ریخته تولید می‌کند؛ و تا زمانی که تصویرهای درهم‌ریخته تولید شده به طور صحیح ترکیب نشوند هیچ اطلاعاتی را به دارنده‌ی آن‌ها نخواهند داد.

۲.۱ انواع روش‌های رمزنگاری تصاویر

تاکنون روش‌های گوناگونی برای تأمین امنیت در ارتباطات تصویری ارائه شده است. اولین ایده ایجاد یک تصویر رمز شده توسط یک کلید و ارسال آن کلید به صورت مخفی، همراه عکس رمز شده به مقصد است. این روش‌ها رمزنگاری کلید مخفی[۴] نام دارند. گیرنده با استفاده از کلید و با اطلاع از روش رمزنگاری، محاسبات معکوس را انجام می‌دهد و اقدام به رمزگشایی[۵] تصویر می‌کند. این روش‌ها

---

[۱] Sharing

[۲] Access Control

[۳] Visual Cryptography

[۴] Secret Key Cryptography

[۵] Decryption

دو زیر مجموعه عمده دارند: درهم‌ریزی[۶] و تعویض مقادیر[۷].

در روش‌های درهم‌ریزی، مقادیر پیکسل[۸]ها تغییری نمی‌کند و فقط از نظر مکانی جابه‌جا می‌شوند. رمزنگاری آشوبی[۹] یکی از انواع این روش‌ها است. در رمزنگاری آشوبی با استفاده از یک فرایند مولد عدد شبه تصادفی[۱۰] و با داشتن هسته[۱۱] شروع به عنوان کلید الگوریتم، یک آرایه از اعداد تصادفی به اندازه تصویر تولید می‌شود. سپس آرایه اعداد تصادفی، مرتب شده و بر اساس این ترتیب محل قرار گرفتن پیکسل‌های تصویر تغییر می‌کند که یک تصویر درهم‌ریخته به دست می‌آید. گیرنده‌ی تصویر درهم‌ریخته با داشتن هسته شروع می‌تواند همان دنباله اولیه اعداد را تولید کرده، سپس ترتیب معکوس درهم‌ریختگی تصویر را به دست آورد. تصویر اصلی با تغییر مکان پیکسل‌ها با ترتیب معکوس رمزگشایی می‌شود.

در روش‌های تعویض مقادیر با استفاده از مولد اعداد تصادفی و همراهی یک تابع، مقدار هر پیکسل به ازای عدد تصادفی، متناسب با مقدار تابع تغییر می‌کند. در نهایت تصویر رمزگذاری[۱۲] شده در هر پیکسل روشنایی متفاوتی دارد و هیچ اطلاعاتی را از محتوای تصویر اصلی به دشمن نخواهد داد.

مولد اعداد تصادفی مورد استفاده در این روش‌ها می‌تواند انواع مختلفی داشته باشد. توابع بازگشتی آشوبی[۱۳] و اتوماتای سلولی[۱۴] نمونه‌هایی از تولید کننده‌های معروف اعداد شبه تصادفی هستند. هم‌چنین پس از رمزگذاری، معیارهای متفاوتی برای آگاهی از کارآمدی روش رمزنگاری (غیر بصری)

---

[۶] Scrambling

[۷] Substitution

[۸] Pixel

[۹] Chaotic Encryption

[۱۰] Pseudo Random Number Generator

[۱۱] Seed

[۱۲] Encrypt

[۱۳] Chaotic Recursive Function

[۱۴] Cellular Automata

مورد استفاده قرار می‌گیرند. از جمله این معیارها می‌توان به انواع خطا[۱۵]، آنتروپی[۱۶] و یا همبستگی[۱۷] اشاره کرد.

خطا مجموع میزان تفاوت مقادیر پیکسل‌های تصویر رمزگذاری شده با تصویر اصلی است. خطا می‌تواند مجذور مربعات تفاضل هر مقدار از مقدار اصلی و یا حتی براساس اهمیت مقادیر، تفاضل با ضریب باشد. به عنوان مثال خطای میانگین مربعات[۱۸] دو تصویر با ابعاد $M \times N$ از رابطه‌ی ۱-۱ محاسبه می‌شود:

$$MSE(f,g) = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(f(x,y) - g(x,y)) \qquad (۱-۱)$$

که در این جا f تصویر اصلی و g تصویر تغییر یافته است.

در تصاویر عادی پیکسل‌های هم‌جوار (افقی، عمودی و مورب) به غیر از لبه‌ها، مقادیر نزدیک به یکدیگر و مرتبط دارند که این مسئله همبستگی بین پیکسلی نام دارد. این در صورتی است که در تصویر رمزگذاری شده پیکسل‌های هم‌جوار باید مقادیر متفاوت و نامرتبطی داشته باشند به گونه‌ای که تصویر رمزگذاری شده مفهومی نداشته باشد. همبستگی بین دو تصویر از رابطه‌ی ۱-۲ به دست می‌آید:

$$Corr(x,y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \qquad (۱-۲)$$

که x مجموعه‌ی پیکسل‌های تصویر و y مجموعه‌ی پیکسل‌های هم‌جوار متناظر با x است. در رمزنگاری تصویر، برای محاسبه‌ی همبستگی بین پیکسل‌های یک تصویر، تعدادی از پیکسل‌ها به صورت تصادفی به عنوان x و پیکسل‌های هم‌جوار آن‌ها به عنوان y در نظر گرفته می‌شوند. هر چه این مقدار همبستگی کم‌تر شود، الگوریتم رمزنگاری امن‌تر به حساب می‌آید.

آنتروپی معیار عدم قطعیت یک متغیر تصادفی است. هرچه آنتروپی یک تصویر رمزگذاری شده بیش‌تر باشد، تصویر رمزگذاری شده درهم‌ریخته‌تر و قدرت رمزگذاری بیش‌تر است. آنتروپی از رابطه‌ی ۱-۳

---

[۱۵] Error

[۱۶] Entropy

[۱۷] Correlation

[۱۸] Mean Square Error

بدست می‌آید:

$$H(X) = \sum_{i=۰}^{N} P(x_i) \times log(\frac{۱}{P(x_i)}) \qquad (۳-۱)$$

که N تعداد سطوح خاکستری تصویر و $P(x_i)$ احتمال رخداد (فراوانی نسبی) مقدار x_i در پیکسل‌های تصویر است.

مخفی‌نگاری[۱۹] از دیگر انواع روش‌های ارتباط امن است [۱۰]. در این روش یک پیام (یا تصویر) در یک تصویر معمولی مخفی می‌شود که به آن تصویر پوشش[۲۰] گفته می‌شود. این روش‌ها طوری طراحی می‌شوند که تصویر محرمانه حتی در صورت اعمال تغییراتی مثل اعمال فیلترها و یا فشرده‌سازی در تصاویر پوشش، قابل بازیابی باشد [۱۱].

یک روش بسیار شبیه به مخفی‌نگاری، واترمارکینگ[۲۱] است [۱۲]. هدف اصلی واترمارکینگ جاسازی یک تصویر واترمارک به منظور تایید صحت، در تصویر اصلی است. تفاوت واترمارکینگ و مخفی‌نگاری در این است که در مخفی‌نگاری تصویر پوشش اهمیتی ندارد ولی هدف واترمارکینگ حفظ مالکیت تصویر پوشش است و سلامت آن مهم است.

در این روش‌ها دو خاصیت شفافیت[۲۲] و مقاومت[۲۳] اهمیت دارند. نخست اینکه واترمارک نباید به صورت محسوسی در تصویر اصلی آشکار باشد. معیار سنجش کارایی این روش‌ها PSNR[۲۴] تصویر پوشش بعد از مخفی‌نگاری و یا واترمارکینگ نسبت به تصویر بدون پیام است. به این دلیل این معیار از اهمیت برخوردار است که افراد فاقد صلاحیت به تفاوت‌های تصویر قبل و بعد از واترمارکینگ و یا مخفی‌نگاری پی نبرند. دومین خاصیت قدرت بازیابی واترمارک و یا تصویر مخفی شده است. به این ترتیب اگر تصویر با حمله فشرده‌سازی و یا اعمال فیلترهای میان‌گذر یا تارکننده تغییر داده شد، هم‌چنان تصویر مخفی و یا واترمارک از تصویر پوشش قابل استخراج باشد. در بعضی روش‌ها برای

[۱۹] Steganography

[۲۰] Camouflage Image

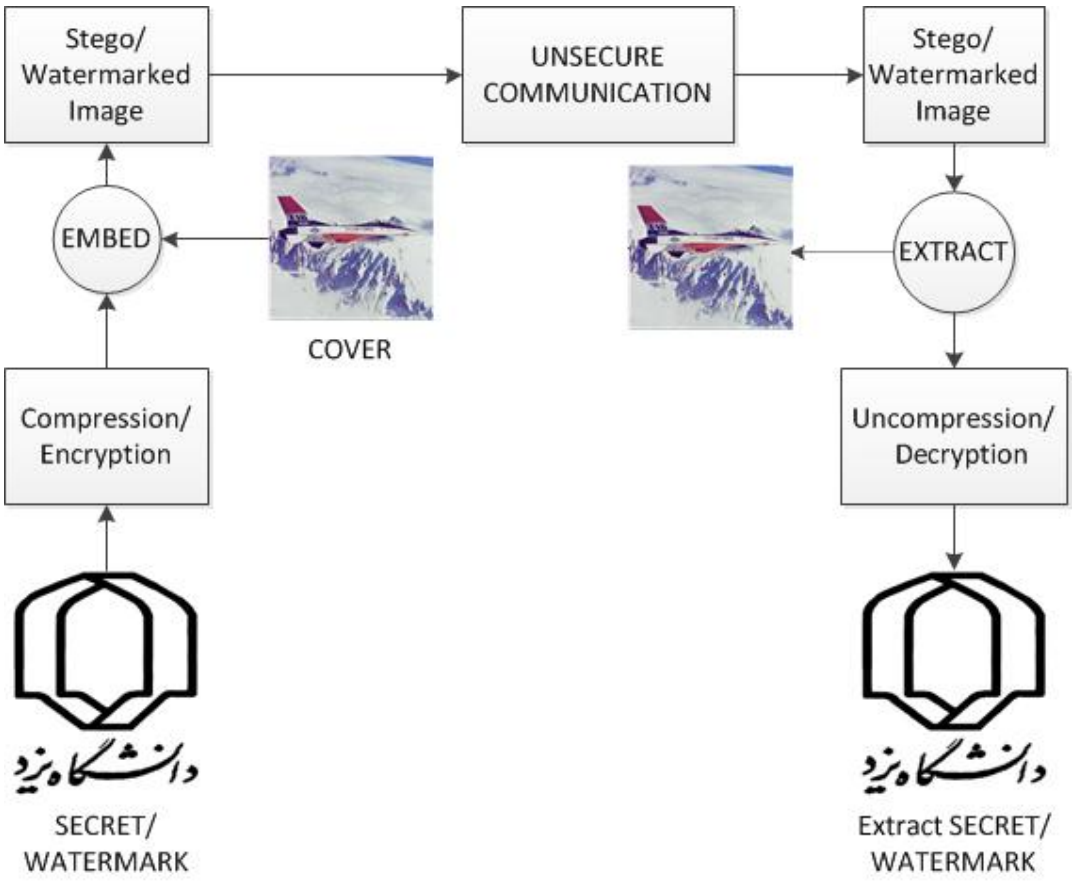
[۲۱] Watermarking

[۲۲] Transparency

[۲۳] Robustness

[۲۴] Peak Signal to Noise Ratio

امنیت بیش‌تر ابتدا تصویر واترمارک یا مخفی را رمزگذاری کرده و سپس در تصویر پوشش جاسازی می‌کنند. شکل ۱.۱ نشان دهنده‌ی روندنما روش‌های واترمارکینگ و مخفی‌نگاری است.



شکل ۱.۱: روندنمای روش‌های مخفی‌نگاری و واترمارکینگ

همان طور که مطرح شد، اغلب روش‌های رمزنگاری با استفاده از یک یا چند کلید و یک روش محاسباتی تصویر را رمزگشایی می‌کنند. رمزگشایی بدون این کلیدها غیرممکن است؛ ضمن این که تصویر رمزگذاری شده به صورت صحیح قابل بازیابی نیست. نقطه ضعف الگوریتم‌های مطرح شده نیاز آن‌ها به محاسبات در مرحله رمزگشایی است. رمزنگاری بصری به عنوان راه حلی برای این مشکل توسط محققین ارائه شده است. در بخش بعدی به بررسی این روش پرداخته خواهد شد.

۳.۱ معرفی رمزنگاری بصری

اغلب روش‌های رمزنگاری برای رمزگشایی تصویر محرمانه نیاز به محاسبات دارند؛ اما در رمزنگاری بصری فرایند رمزگشایی به طور مستقیم توسط چشم انسان صورت می‌گیرد. در رمزنگاری بصری یک تصویر محرمانه به چند تصویر (سهم[۲۵]) درهم‌ریخته‌ی تصادفی تبدیل می‌شود. با چاپ این تصاویر روی کاغذ شفاف، صاحب رمز به هر شریک[۲۶] یک سهم رمز شده از تصویر را می‌دهد. هر شریک با استفاده از سهم خودش نمی‌تواند اطلاعاتی از رمز پنهان شده به دست بیاورد؛ اما هنگامی که تعداد کافی از شرکاء سهم خود را روی یکدیگر قرار دهند، می‌توانند رمز پنهان شده را ببینند. بدیهی است در این مورد برای رمزگشایی به ابزار محاسبات و دانش رمزنگاری نیازی نیست. با چنین خاصیت جالبی که فرایند رمزگشایی (به جای دستگاه‌های محاسباتی) با سیستم بینایی بشر صورت می‌گیرد، رمزنگاری بصری محققان بسیاری را به خود جلب کرده است.

برای رمزگشایی به کمک بینایی، در هر سهم به ازای هر پیکسل از تصویر محرمانه، یک بلوک پیکسلی[۲۷] شامل چند پیکسل قرار می‌گیرد. بلوک‌ها به گونه‌ای طراحی و انتخاب می‌شوند که سهم‌ها به طور جداگانه اطلاعاتی را درباره‌ی تصویر اصلی به کاربر ندهند؛ ولی با چاپ بر روی کاغذ شفاف و برهم گذاری دقیق رمز را نمایان کنند. در بخش ۱.۲ این روش به تفصیل مورد بررسی قرار خواهد گرفت.

۴.۱ روش‌های هوشمند رمزنگاری

در نوشتارهای اخیر، استفاده از روش‌های هوشمند در انواع الگوریتم‌های رمزنگاری تصاویر به چشم می‌خورد. به عنوان مثال از شبکه عصبی برای فشرده سازی تصویر [۱۳]، از الگوریتم ژنتیک برای بخش بندی و تعیین کلید مولد شبه تصادفی [۱۴] و از اتوماتای سلولی برای تولید اعداد تصادفی [۱۵] استفاده شده است. البته، استفاده از الگوریتم‌های هوشمند سبب تغییر ماهیت این روش‌ها نشده بلکه فقط قسمتی از کار رمزنگاری را دست‌خوش تغییر کرده است.

---

[۲۵] Share

[۲۶] Participant

[۲۷] Pixel Block

با وجود ارائه الگوریتم‌های هوشمند مختلف در روش‌های رمزنگاری تصویر، جای خالی استفاده از این الگوریتم‌ها در روش‌های رمزنگاری بصری در نوشتارها حس می‌شود. روش‌های هوشمند در صورت استفاده صحیح، امکان مدل‌سازی متفاوت مسئله را فراهم می‌سازند. هم‌چنین به سبب تعمیم مسئله، توسعه‌ی روش‌های جدید و گسترش آن را ممکن می‌سازند.

۵.۱ ساختار پایان‌نامه

در این پایان‌نامه روشی نوین برای رمزنگاری بصری تصاویر سطوح خاکستری و رنگی با استفاده از الگوریتم ژنتیک ارائه می‌شود. پس از تشریح روش رمزنگاری بصری و کارهای مرتبط در فصل ۲ در فصل ۳ روش پیشنهادی مطرح می‌شود.

در بخش ۱.۳ روشی برای توسعه کارایی رمزنگاری بصری دودویی به تصاویر سطوح خاکستری ارائه می‌شود. این روش با استفاده از یک جدول جستجو[۲۸] تصویر محرمانه سطوح خاکستری را به دو سهم سطوح خاکستری تبدیل می‌کند. سهم‌ها در صورت چاپ بر روی کاغذ شفاف، تصویر محرمانه را نمایان می‌کنند.پس از آن، مدل توسعه یافته‌ی روش ارائه شده برای تصاویر سطوح خاکستری، در بخش ۲.۱.۳ به منظور استفاده در تصاویر رنگی ارائه می‌شود. در بخش ۲.۲.۳ نحوه‌ی فرموله‌سازی رمزنگاری بصری تصاویر سطوح خاکستری برای استفاده از الگوریتم ژنتیک تشریح و توسعه‌ی این روش به تصاویر رنگی در بخش ۳.۲.۳ مورد بررسی قرار می‌گیرد و نتایج پیاده‌سازی روش‌های ارائه شده نمایش داده می‌شوند. تصاویر انتخاب شده از نظر سطح جزئیات متفاوت بوده و مقبولیت روش را ارزیابی می‌کنند. در نهایت در فصل ۴ جمع بندی کلی از مسائل مطرح شده و نتیجه‌گیری ارائه خواهد شد.

[۲۸] Lookup Table