

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

سمینار

عنوان

**مطالعه روش های رمزنگاری تصویر**

نگارنده

## فهرست مطالب

صفحه	عنوان
۵	چکیده.....
۶	فصل اول: مقدمه
۷	۱-۱- مقدمه.....
۱۰	فصل دوم: مروری بر رمزنگاری تصویر
۱۱	۱-۲- مقدمه.....
۱۲	۲-۲- مفاهیم اساسی رمزنگاری.....
۱۴	۳-۲- سیستم‌های امنیتی.....
۱۵	۴-۲- رمزنگاری.....
۱۶	۲-۴-۱-۱- انواع رمز نگاری.....
۱۶	۲-۴-۱-۲- رمزنگاری فیزیکی.....
۱۶	۲-۴-۱-۳- رمزنگاری ریاضی.....
۱۶	۲-۴-۱-۴- رمزنگاری کوانتومی.....
۱۷	۲-۵- تفاوت پنهان‌نگاری و رمزنگاری.....
۱۹	۲-۶- مثالی برای پنهان-نگاری و رمزنگاری.....
۲۰	۲-۷- رمزنگاری تصویر.....
۲۲	۲-۸- رمزنگاری چندرسانه‌ای.....
۲۵	۲-۹- بیت- سطح‌ها در حوزه مکانی.....
۲۶	۲-۱۰- معیارهای بررسی یک الگوریتم رمزنگاری تصویر.....
۲۶	۲-۱۰-۱- امنیت.....
۲۷	۲-۱۰-۲- سرعت.....
۲۷	۲-۱۰-۳- قبول رشته بیت.....
۲۸	۲-۱۰-۴- پردازش رشته بیت.....
۲۸	۲-۱۰-۵- تاثیر بر میزان فشردگی.....
۲۸	۲-۱۰-۶- سایفرهای رمزنگاری تصویر.....

۱۱-۲ - جمع بندی ..... ۳۲

فصل سوم: مطالعه و بررسی روش های رمزنگاری تصویر ..... ۳۳

۱-۳ - مقدمه ..... ۳۴

۲-۳ - روش های ارائه برای رمزنگاری تصویر مبتنی بر الگوریتم DNA ..... ۳۶

۱-۲-۳ - رمزنگاری تصویر مبتنی بر توسعه کلید AES ..... ۳۶

۲-۲-۳ - الگوریتم رمزنگاری تصویر RGB براساس رمزگذاری DNA و نگاشت آشوب ..... ۳۷

۳-۲-۳ - یک بررسی: تکنیک های رمزنگاری مبتنی بر DNA ..... ۳۸

۴-۲-۳ - رمزنگاری مبتنی بر DNA با استفاده از جایگشت و روش تصادفی تولید کلید ..... ۳۹

۵-۲-۳ - آنالیز امنیت بر روی یک رمزنگاری تصویر رنگی مبتنی بر رمزگذاری DNA ..... ۴۰

۶-۲-۳ - الگوریتم رمزنگاری تصویر چندسطحی مبتنی بر آشوب و رمزگذاری DNA ..... ۴۰

۷-۲-۳ - پژوهش بر یک الگوریتم رمزنگاری تصویر ..... ۴۳

۸-۲-۳ - روش ترکیبی رمزنگاری تصویر با استفاده از رمزنگاری DNA ..... ۴۴

۳-۳ - بحث و بررسی ..... ۴۵

۴-۳ - جمع بندی ..... ۴۶

فصل چهارم: نتیجه گیری و پیشنهادات ..... ۴۷

۱-۴ - نتیجه گیری و پیشنهادات ..... ۴۸

مراجع ..... ۵۰

## فهرست اشکال

- شکل ۱-۲- امنیت در کانال ارتباطی با استفاده از رمزگذاری و رمزگشایی..... ۱۳
- شکل ۲-۲- نمای کلی از سیستم‌های امنیتی..... ۱۴
- شکل ۳-۲- مدل پایه ای رمزنگاری..... ۱۸
- شکل ۴-۲- مدل پایه‌ای پنهان نگاری..... ۱۸
- شکل ۵-۲- تصویر رمزنگاری شده توسط AES به طور مستقیم..... ۲۳
- شکل ۶-۲- معماری رمزنگاری و رمزگشایی چندرسانه‌ای..... ۲۴
- شکل ۷-۲- نتایج bit-plane رمزگذاری شده در دامنه جزئی..... ۲۵
- شکل ۸-۲- ارتباط بین کیفیت تصویر (PSNR) و توانایی رمزگذاری..... ۲۶
- شکل ۱-۳- حساسیت کلید الگوریتم پیشنهادی..... ۳۷
- شکل ۲-۳- فلوجارت الگوریتم رمزنگاری تصویر..... ۳۹
- شکل ۳-۳- فلوجارت الگوریتم پیشنهادی در..... ۴۰
- شکل ۴-۳- فلوجارت رمزنگاری در الگوریتم پیشنهادی..... ۴۲
- شکل ۵-۳- بلوک دیاگرام الگوریتم رمزنگاری پیشنهاد شده در..... ۴۴
- شکل ۶-۳- بلوک دیاگرام طرح پیشنهادی در..... ۴۵

## چکیده

امروزه دردنیای دیجیتال حفاظت از اطلاعات رکن اساسی و مهمی در تبادل پیام‌ها و مبادلات تجاری ایفا می‌کند. برای تامین نیازهای امنیتی تراکنش، از رمزنگاری استفاده می‌شود با توجه به اهمیت این موضوع و گذر از مرحله سنتی به مرحله دیجیتال استفاده از روش‌های رمزنگاری ضروری به نظر می‌رسد که می‌توان رمزنگاری تصویر را مهم‌ترین رکن آن دانست. در سال‌های اخیر الگوریتم‌ها و روش‌های رمزنگاری متعددی برای رمزنگاری تصویر معرفی شده‌اند که بیشتر آنها نیز از توابع آشوب و الگوریتم ژنتیک برای رمزنگاری داده‌ها استفاده کرده‌اند. در این سمینار ابتدا رمزنگاری تصویر بررسی شده و سپس الگوریتم‌های رمزنگاری تصویر که روش‌های مختلف بهره برده‌اند مورد مطالعه و ارزیابی قرار داده‌ایم.

**کلمات کلیدی:** رمزنگاری تصویر، آشوب، حملات، پیام.

# فصل اول

## مقدمه

با استفاده گسترده‌ی کامپیوترها و فراگیر شدن اینترنت، انتقال داده‌های تصویری روز به روز در حال افزایش است. داده‌های تصویری یکی از اساسی‌ترین و مهمترین ابزارهای بیان اطلاعات برای انسان هستند. در نتیجه نیاز است تا داده‌ها و اطلاعات تصویری از قبیل تصاویری که با ماهواره‌ها نظامی فرستاده می‌شوند و عکسبرداری‌هایی که توسط سیستم‌های تسلیحاتی جدید و یا نمودارها و نقشه‌های سازمان‌ها و موسسات مهم و حساس و ..، توسط فرستنده و گیرنده رمز شوند مطابق با قوانین ارتباطی حاکم، این اطلاعات باید با حفظ محرمانگی کامل انتقال یابند. بنابراین؛ امنیت اطلاعات تصویری بسیار اهمیت می‌یابد. اما در شبکه‌های رایج امروزی چگونگی تضمین و افزایش امنیت داده‌های تصویری مسئله‌ای است که بخش اعظمی از تحقیقات حوزه‌ی امنیت اطلاعات را به خود اختصاص داده است.

دو تکنیک نهان‌نگاری و رمزنگاری، اساسی‌ترین روش‌های محافظت از داده‌های تصویری هستند. نهان‌نگاری پنهان‌سازی داده درون یک تصویر میزبان است به طوری‌که‌ای داده‌ها غیرقابل رویت باشند و همچنین امکان حذف آنها توسط کاربران غیرمجاز وجود نداشته باشد. هدف اصلی نهان‌نگاری کنترل حق تکثیر و احراز هویت می‌باشد. با این وجود استفاده از نهان‌نگاری در ارتباطات خاص و مهم از قبیل ارسال شرح حال و نقشه‌های نظامی در میدان جنگی چندان مناسب به نظر نمی‌آید چرا که امنیت آنها را تضمین نمی‌نماید. تاکنون، الگوریتم‌های بسیار زیادی برای رمزنگاری تصاویر پیشنهاد شده‌اند که عاری از عیب و نقص نبوده‌اند. بعضی از این الگوریتم‌ها کارایی کمتری دارند یا به عبارت دیگر برای رسیدن به سطح رمزنگاری بالاتر، یا برای رسیدن به امنیت مناسب، زمان بیشتری را برای رمز نمودن صرف می‌کنند بنابراین کارایی و کیفیت آنها پایین می‌آید. دسته‌ی دیگر از الگوریتم‌هایی که برای دسته‌ی دیگر از الگوریتم‌هایی که برای رمزنگاری تصاویر مورد استفاده قرار می‌گیرد از لحاظ امنیت دچار کمبودهایی هستند چرا که تصویر



رمز شده‌ی حاصل از این الگوریتم‌ها کاملاً تصادفی به نظر نمی‌رسد و بنابراین تصاویر رمز شده توسط این روش‌ها می‌توانند بوسیله مهاجمان شناسایی و آشکارسازی شوند. بعضی از الگوریتم‌های رمزنگاری نیز در برابر حملات دیفرانسیلی یا حملات متن اصلی معلوم، مقاوم نیستند و تصاویر رمز شده حاصل از این الگوریتم‌ها، می‌توانند توسط کامپیوترهایی با سرعت و قدرت محاسباتی بالا، به طور کامل رمزگشایی شوند [1]. تصاویر دیجیتال و رمزنگاری آنها بعنوان یکی از انواع داده‌های چند رسانه‌ای توجه بسیاری از محققان را به خود جلب کرده‌اند. اگر به داده‌های تصویری تنها به عنوان رشته‌ای از بیت‌ها توجه شود در این صورت هیچ اختلافی اساسی میان رمزنگاری تصویر و سایر الگوریتم‌های رمزنگاری داده وجود ندارد. بنابراین داده‌های تصویری می‌توانند همانند رشته‌ای از بیت‌ها به عنوان ورودی به سیستم‌های رمزنگاری سنتی وارد شوند. به این نوع از الگوریتم‌های رمزنگاری داده الگوریتم‌های ساده می‌گویند. با توجه به اندازه‌ی تصاویر ثابت و مقایسه‌ی آن با اندازه‌ی داده‌های متنی الگوریتم‌های ساده نمی‌توانند سرعت مورد نیاز برای انتقال و یا دیگر کاربردهای فرایندهای بلادرنگ تصاویر ثابت فراهم نمایند. دو سطح امنیتی متفاوت برای الگوریتم‌های رمزنگاری تصویر در نظر گرفته شده است: رمزنگاری امنیتی کم و رمزنگاری امنیتی بالا. در رمزنگاری امنیتی پایین کیفیت ظاهری تصاویر رمز شده در مقایسه با تصویر اصلی کاهش می‌یابد. اما محتوای تصویر همچنان تا حدودی واضح باقی مانده و برای بیننده نیز امکان تشخیص تصویر اصلی از روی تصویر رمز شده وجود دارد. در مورد امنیت سطح بالا، تصویر اصلی کاملاً بهم ریخته و تصویر رمز شده مانند یک نویز تصادفی به نظر می‌رسد. در این مورد بیننده قادر به آشکارسازی تصویر ابتدایی از تصویر رمز شده نمی‌باشد. در طراحی یک سیستم رمزنگاری تصاویر ثابت، لازم است تا از رمزنگاری بیت به بیت و با این حال از امنیت سیستم رمزنگاری نیز اطمینان حاصل شود. یک سیستم رمزنگاری تصویر باید همواره خصوصیات زیر را داشته باشد.

الگوریتم‌های رمزنگاری/رمزگشایی باید به اندازه‌ی کافی سریع باشند تا بتوانند نیازهای کاربردهای بلادرنگ را برآورد سازند.

فرآیند رمزنگاری نباید نرخ فشردگی را کاهش دهد یا اندازه‌ی تصویر را افزایش دهد.

الگوریتم رمزنگاری باید در برابر فرآیندهای تصاویر دیجیتال مقاوم باشند.

فرآیندها رمزنگاری و رمزگشایی نباید کیفیت تصویر اصلی را کاهش دهند.

بر مبنای این اقدامات، الگوریتم‌های بسیاری برای رمزنگاری تصاویر ثابت پیشنهاد شده‌اند [2]. تکنیک‌های

رمزنگاری تصاویر ثابت که اخیراً پیشنهاد شده‌اند شامل الگوریتم‌های مبتنی بر تبدیلات مستوی و

سیستم‌های آشوبگون و تبدیلات فوریه و روش‌های مبتنی بر پویس و روش‌های مبتنی بر چهار درختی

می‌باشد [3]. در این سمینار به بررسی جامع و کامل در ارتباط با رمزنگاری تصویر را مورد مطالعه و ارزیابی

قرار می‌دهیم.