

ترکیب الگوریتم رمزنگاری تصویر
و شبکه‌های اتصالی درونی

فریبا دهقانی، ف. و. آ. دی
دکتر علی محمد لطیف
فاطمه دهقانی فیروزآبادی

سرشناسه: دهقانی فیروزآبادی، فریبا، ۱۳۶۹ -
عنوان و نام پدیدآور: ترکیب الگوریتم رمزنگاری تصویر و شبکه‌های اتصالی درونی /
فریبا دهقانی فیروزآبادی، علی محمد لطیف، فاطمه دهقانی فیروزآبادی.

مشخصات نشر: تهران: سیمیا هنر، ۱۳۹۵.
مشخصات ظاهری: ۶۴ ص. مصور، جدول، نمودار.
شابک: ۹۷۸-۶۰۰-۷۶۱۳-۱۰-۸ ۵۰۰۰۰ ریال

وضعیت فهرست نویسی: فیبا

یادداشت: واژه‌نامه.

یادداشت: کتابنامه. ص. ۶۰-۶۲.

موضوع رمزنگاری

موضوع Cryptography

موضوع الگوریتم‌های موازی

موضوع Parallel algorithms

نمونه افزوده: لطیف، علی محمد، ۱۳۵۰ -

شناسه: خروده دهقانی فیروزآبادی، فاطمه، ۱۳۶۷ -

رده بندی: ۱۳۶۴/۱۹۶۴/۱۰۳ Z

رده بندی دیویی: ۶۵۲

شماره کتابشناسی: ۴۳۱ ۱۶۰



نام کتاب: ترکیب الگوریتم رمزنگاری تصویر

و شبکه‌های اتصالی درونی

مؤلفان: فریبا دهقانی فیروزآبادی،

دکتر علی محمد لطیف، فریبا دهقانی فیروزآبادی

ناشر: نشر سیمیا هنر

طرح جلد: فریبا دهقانی فیروزآبادی

نوبت چاپ: اول / ۱۳۹۵

تیراژ: ۱۰۰۰ جلد

شابک: ۹۷۸-۶۰۰-۷۶۱۳-۱۰-۸

قیمت: ۵۰۰۰ تومان

فهرست مطالب

صفحه	عنوان
۱۳	پیشگفتار
۱۵	فصل ۱- مقدمه
۱۵	۱-۱- تاریخچه
۱۶	۲- معرفی رمزنگاری
۱۸	۳- حذف رمزنگاری چندرسانه‌ای
۱۸	۴- شیوه‌های رمزنگاری
۱۸	۵-۱- الگوریتم‌های رمزنگاری تصویر
۱۸	۱-۵-۱- الگوریتم به هم‌ریزی تصویر بر اساس تبدیل آرنولد
۱۹	۲-۵-۱- الگوریتم به هم‌ریزی تصویر بر اساس کد گری
۲۱	۳-۵-۱- الگوریتم به هم‌ریزی تصویر بر اساس تبدیل فیوناچی
۲۱	۴-۵-۱- الگوریتم به هم‌ریزی تصویر بر اساس نظریه بی‌نظمی و تبدیل مرتب
۲۴	۶-۱- مقایسه‌ی الگوریتم‌های رمزنگاری
۲۴	۱-۶-۱- آزمون بصری و تحلیل هیستوگرام
۲۵	۲-۶-۱- تحلیل ضرایب همبستگی
۲۹	۷-۱- ساختار کتاب
۳۰	۸-۱- جمع‌بندی
۳۲	فصل ۲- الگوریتم‌های موازی و شبکه‌های اتصالاتی درونی
۳۲	۱-۲- محاسبه موازی
۳۳	۲-۲- سیستم‌های محاسبه موازی
۳۳	۲-۲-۱- تک دستورالعمل و تک داده
۳۴	۲-۲-۲- تک دستورالعمل و چند داده
۳۴	۳-۲-۲- چند دستور و تک داده
۳۴	۴-۲-۲- چند دستورالعمل و چند داده
۳۵	۳-۲- شبکه اتصالاتی درونی بین پردازنده و حافظه
۳۷	۴-۲- جمع‌بندی

۳۸	فصل ۳- روش درهم‌ریزی پیشنهادی
۳۸	۳-۱- مقدمه
۳۹	۳-۲- مرحله اول الگوریتم پیشنهادی
۴۰	۳-۳- مرحله دوم الگوریتم پیشنهادی
۴۵	۳-۴- رمزگشایی "گوریتم" پیشنهادی
۴۵	۳-۵- جمع‌بندی
۴۶	فصل ۴- نتایج آزمایش‌ها
۴۶	۴-۱- تحلیل الگوریتم پیشنهادی با آزمون بصری و تحلیل هیستوگرام
۵۰	۴-۲- تحلیل الگوریتم پیشنهادی با آزمون تحلیل همبستگی و معیارهای اندازه‌گیری
۵۶	۴-۳- جمع‌بندی
۵۸	فصل ۵- نتیجه‌گیری و پیشنهادها
۵۸	۵-۱- نتیجه‌گیری
۵۹	۵-۲- پیشنهادها
۶۰	فهرست مراجع
۶۳	واژه‌نامه فارسی به انگلیسی
۶۴	واژه‌نامه انگلیسی به فارسی

پیشگفتار

امنیت اطلاعات همواره یک امر مهم و حیاتی برای حرم اطلاعات افراد و سازمان‌ها است. یکی از ابزارهای پر قدرت برای ارضای این نیاز رمزنگاری است. رمزنگاری یکی از روش‌های تأمین امنیت است که با استفاده از یک رابطه ریاضی برگشت‌پذیر انجام می‌گیرد. تصویر به عنوان یکی از پر استفاده‌ترین محصول دیجیتال به دلیل ماهیت خاص خود، دارای الگوریتم‌های رمزنگاری ویژه است. اما مشکل اینجا است که وابستگی زیاد سطوح خاکستری پیکسل‌های مجاور باعث شده است تا الگوریتم‌های سنتی رمزنگاری بر روی تصاویر دیجیتال قابل استفاده نباشند. الگوریتم‌های رمزنگاری زیادی برای رمزنگاری تصاویر دیجیتال ارائه شده است به طور نمونه به الگوریتم‌های فیناچی، تبدیل آرنولد، تبدیل مرتب و کد گری می‌توان اشاره کرد؛ اما طبق بررسی‌های انجام شده که در پایان‌نامه آمده است الگوریتم‌های فیناچی و تبدیل آرنولد در اولین اجرا به خوبی نمی‌توانند تصویر را بهم بریزند. الگوریتم کد گری به تنهایی نمی‌تواند بر روی تصویر اجرا شود. در برخی از قسمت‌های تصویر رمز شده توسط الگوریتم تبدیل مرتب همبستگی بین پیکسل‌ها همچنان وجود دارد. در این پایان‌نامه یک الگوریتم رمزنگاری جدید برای تصاویر دیجیتال با استفاده از شبکه‌های اتصالی درونی پیشنهاد شده است. در این الگوریتم ابتدا تصویر بلوک‌بندی می‌شود و سپس با استفاده از شیوه جابه‌جایی و یک شبکه پروانه‌ای پیکسل‌های هر بلوک درهم‌ریخته می‌شود. در مرحله‌ی بعد تصویر به دست آمده با استفاده از شیوه جایگزینی و یک شبکه‌ی آمیخته بهم‌ریخته می‌شود. این طرح با استفاده از آزمون‌های بصری، تحلیل همبستگی، معیارهای اندازه‌گیری و تحلیل هیستوگرام سنجیده شد. پس از یک بار اجرای الگوریتم پیشنهادی بر روی تصویر استاندارد مرد عکاس و میکی موس تصاویر به خوبی بهم‌ریخته می‌شوند همچنین این الگوریتم همبستگی بین پیکسل‌های مجاور را به شدت کاهش داده است و معیارهای اندازه‌گیری را بهبود بخشیده است. به طور کلی با توجه به نتایج، الگوریتم از کارایی مناسبی برخوردار است.

کلیدواژه: درهم‌ریزی، تصویر، شبکه‌های اتصالی درونی، شبکه امگا، شبکه پروانه‌ای.