مقاوم‌سازی پنهان‌نگاری در تصاویر سونارهای اسکن جانبی توسط روش رمزنگاری ترکیبی

سید محمدرضا موسوی[۱]، یوسف حاتم خانی[۲]، ابراهیم شفیعی[۳]، محمد خویشه[۴]

m_mosavi@iust.ac.ir

۱- استاد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

۲- دانشجوی کارشناسی ارشد دانشکده مهندسی برق، دانشگاه علوم دریایی امام خمینی (ره)، نوشهر

۳- دانشجوی کارشناسی ارشد دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

۴- دانشجوی دکتری دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

چکیده

در دنیای امروزی برای ارسال پیام‌های طبقه‌بندی شده معمولاً از پنهان‌نگاری پیام مورد نظر در قالب تصاویر، فیلم‌ها و صوت‌های عادی استفاده می‌شود. اهمیت بالای پنهان ماندن پیام‌های مهم باعث می‌شود، الگوریتم‌های جدیدی برای پنهان‌سازی اطلاعات در خروجی چندرسانه‌ای ارائه گردد. با توجه به اینکه الگوریتم‌های استخراج این نوع نهان‌نگاری‌ها نیز به موازات الگوریتم‌های نهان‌نگاری، در دسترس قرار می‌گیرند، در این مقاله از الگوریتم ترکیبی استاندارد رمزنگاری پیشرفته و تبدیل کسینوسی گسسته برای افزایش امنیت اطلاعات نهان‌نگاری شده در تصاویر سونارهای اسکن جانبی استفاده می‌شود، به‌طوری‌که الگوریتم ترکیبی پیشنهادی باعث بالا رفتن امنیت اطلاعات می‌گردد و از افشای آن جلوگیری می‌نماید. اهمیت فوق‌العاده ارتباطات کشتی‌ها و زیرسطحی‌ها و طبقه‌بندی فوق سری اطلاعات آن‌ها برای نیروی دریایی، موجب به وجود آمدن الگوریتم پیشنهادی شده است.

واژگان کلیدی: سونارهای اسکن جانبی، نهان‌نگاره، رمزنگار AES، تبدیل فوریه Walch.

تاریخ دریافت مقاله : ۹۶/۱۰/۱۷

تاریخ پذیرش مقاله : ۹۷/۰۲/۱۶

۱- مقدمه

گسترش سامانه‌های چندرسانه‌ای و استفاده از شبکه‌های کامپیوتری و اینترنت دسترسی به اطلاعات دیجیتال و کپی‌برداری از آن‌ها را به‌آسانی امکان‌پذیر نموده است که این، نیازی جهت حفاظت از حق مالکیت رسانه‌های دیجیتالی مختلف به وجود آورده است. بنابراین مسئله حفاظت از داده‌ها در مقابل کپی‌برداری و جعل از اهمیت بالایی برخوردار است. به این دلیل باید از روش‌هایی برای کنترل کپی کردن استفاده نمود. از روش‌های حل این مشکل می‌توان به استفاده از نهان‌نگاری[1] و روش‌های مختلف رمزنگاری اشاره نمود [۱].

نهان‌نگاری به فرآیندی اطلاق می‌گردد که در آن اطلاعات مخفی در رسانه‌ای مثل تصویر، با تغییراتی که در پیکسل‌های آن داده می‌شود، جاسازی می‌گردد. نهان‌نگاری به دو دسته مرئی و غیرمرئی تقسیم می‌شود. مفهوم نهان‌نگاری مرئی بسیار ساده است. این نوع نهان‌نگاری مانند مهری بر روی کاغذ می‌باشد و قابل رویت است [۲].

در سال‌های اخیر نهان‌نگاری دیجیتال برای کاربردهای مختلف مانند سندیت و حفاظت از حقوق مؤلفین مورد توجه قرار گرفته است. نهان‌نگاری دیجیتال تکنیکی برای جاسازی اطلاعات داخل تصویر است که می‌توان از آن برای اهداف متفاوت مثل سندیت، حفاظت حق مالکیت و غیره استفاده نمود. به دلیل پیشرفت‌های شبکه‌های ارتباطی و افزایش روزافزون تصاویر دیجیتالی، استفاده از نهان‌نگاری دیجیتال مورد اهمیت فراوانی قرار گرفته است. تصاویر دیجیتالی به‌راحتی می‌توانند در معرض تغییرات عمدی و غیرعمدی قرار بگیرند؛ بنابراین به‌طور معمول نمی‌توان از صحت تصاویر اطمینان حاصل نمود. برای مثال در کاربردهای قضایی و گزارش‌های خبری، ما باید اطمینان از چیزی که می‌بینیم، حاصل کنیم تا چه اندازه سندیت دارد. به‌عنوان مثالی دیگر می‌توان به تجارت الکترونیک اشاره کرد. زمانی که فروشندگان تصاویر دیجیتالی را برای خریداران ارسال می‌کنند. در این مورد شخص خریدار می‌خواهد، بداند که تصویر رسیده تا چه اندازه معتبر است. در این مورد هم تصویر و هم منبع باید مورد تصدیق قرار بگیرند [۳]. همچنین با افزایش کاربرد اینترنت، کپی‌های غیرقانونی و دیگر حملات، حفاظت از حق مالکیت به یک موضوع حیاتی مبدل گشته است؛ بنابراین نیاز به روش‌های کارآمد برای مقابله با این مشکلات بیش از پیش احساس می‌گردد که با استفاده از نهان‌نگاری می‌توان به این مهم دست‌یافت.

در طی دو دهه گذشته، روش‌های مختلفی برای نهان‌نگاری دیجیتالی ارائه شده است. این روش‌ها را از نقطه نظرات گوناگون می‌توان دسته‌بندی کرد. از نقطه نظر نوع سندی که نهان‌نگاری می‌شود، چهار نوع سیستم نهان‌نگاری متن [۴]، صوت [۵و۶]، تصویر [۷-۱۱] و ویدیو [۱۲-۱۵] وجود دارد.

روش‌های نهان‌نگاری نیز به دو دسته حوزه مکان و حوزه تبدیل تقسیم می‌گردند. نهان‌نگاری حوزه مکان ابزاری مناسبی برای سندیت است. روش‌های حوزه تبدیل در برابر حملات مقاومت بیشتری از خود نشان می‌دهند و باوجود اینکه از آن‌ها هم می‌توان برای سندیت بهره برد، ولی بیشتر برای حفاظت حق چاپ مورد استفاده قرار می‌گیرند که در این روش‌ها از تبدیل‌هایی مانند تبدیل موجک گسسته (DWT[2])، تبدیل کسینوسی گسسته (DCT[3]) و غیره استفاده می‌شود.

در [۱۶]، به یک طرح پنهان‌نگاری مبتنی بر DCT اشاره شده است که در آن تصویر در حوزه DCT به بلاک‌های ۸×۸ تقسیم می‌شود و پنهان‌نگاری در ضرایب فرکانس پایین تعبیه می‌گردد که در آن مؤلف از الگوریتم خارج قسمت-جاسازی بهره برده است. قبل از جاسازی اطلاعات هم یک سری اعداد شبه تصادفی برای تغییر نهان‌نگاری مورد استفاده قرارگرفته است.

در [۱۷]، یک الگوریتم نهان‌نگاری مقاوم را پیشنهاد شده است که در آن DCT و JND[4] به کار برده و از ضرایب DC برای جاسازی نهان‌نگاری استفاده شده است. سپس از مقادیر JND تصویر پوشش برای ایجاد مقاومت استفاده شد.

در [۱۸]، ابتدا ضرایب DCT تصویر محاسبه می‌گردد و سپس تصویر به چهار بلاک دیگر برحسب مقادیر ضرایب

[1] Watermarking

[2] Discrete Wavelet Transform
[3] Discrete Cosine Transform
[4] Just Noticeable Difference

فرکانس تقسیم می‌شود که این ضرایب در طیف‌های بالایی، میانی و پایینی قرار می‌گیرند؛ یعنی یک بلاک فقط شامل ضرایب فرکانس بالا، دو بلاک شامل ضرایب فرکانس میانی و ضرایب فرکانس پایین می‌گردد. سپس برای هر بلاک، SVD[1] آن محاسبه‌شده و مقادیر منفرد آن با ضریبی از مقادیر منفرد نهان‌نگاری جمع می‌گردد و به این صورت تصویر نهان‌نگاری شده حاصل می‌شود. مقاله [۱۹]، یک الگوریتم مبتنی بر SVD را معرفی می‌کند. در بیشتر مقالات از DCT استفاده شده است. الگوریتم مرسوم نهان‌نگاری پایه و اساس برخی از الگوریتم‌های مبتنی بر DCT و SVD است. به این صورت که برخی مقالات مانند [۱۸و۲۰] با تغییراتی که در آن ایجاد نموده‌اند، باعث ارتقاء آن شده‌اند.

سونار اسکن جانبی یک وسیله تصویربرداری رایج برای استفاده در زیردریا و یافتن آثار مخروبه کف دریا و موانع بستر دریا است که می‌توانند برای کشتیرانی و تأسیسات دریایی مربوط به صنعت نفت و گاز خطرناک باشند. به‌علاوه وضعیت خطوط لوله و کابل‌ها بر بستر دریا می تواند با استفاده از سونار اسکن جانبی بررسی شود. داده های سونار اسکن جانبی و داده‌های مربوط به کف دریا که یک نمایش اجمالی از ساختار ظاهری بستر دریا فراهم می کنند، در طول عملیات عمق‌یابی صوتی به دست می‌آیند. سونار اسکن جانبی از یک وسیله سونار که پالس‌هایی به پایین به‌سوی بستر دریا در گستره یک زاویه بزرگ منتشر می‌کند، استفاده می‌نماید. این وسیله قادر است اشیاء بزرگی را که بر روی بستر دریا افتاده‌اند و در آب تاریک دریا کاملاً ناپیدا هستند، نمایش دهد. فرکانس صوتی استفاده شده در سونار اسکن جانبی معمولاً دارای محدوده بین ۱۰۰ تا ۵۰۰ کیلوهرتز است [۲۱].

در سال‌های گذشته به علت نیازهای فراوانی که برای کاربردهای رمزنگارها وجود داشته است، بحث استانداردسازی الگوریتم‌های رمزنگاری مطرح شده است که نمونه‌های استاندارد شده آن در سال‌های گذشته DES[2] و در سال‌های اخیر AES[3] می‌باشد. در این مقاله، پیشنهاد پیاده‌سازی یک روش برای حفظ امنیت داده‌های مهم به دست آمده از سونار اسکن جانبی با استفاده از الگوریتم رمزنگاری قوی AES به‌عنوان رمزنگار اولیه قبل از طرح نهان‌نگاری مبتنی بر DCT مطرح شده است، به‌طوری‌که الگوریتم ترکیبی در نظر گرفته شده باعث بالا رفتن امنیت اطلاعات در زمان ارسال شده و از افشای آن جلوگیری می‌نماید [۲۲].

در ادامه و در بخش دوم ساختار الگوریتم AES تشریح خواهد شد. بخش سوم به معرفی رویکرد پیشنهادی می‌پردازد. در بخش چهارم نتایج شبیه‌سازی ارائه می‌شود. در نهایت، در بخش پنجم نتیجه‌گیری و پیشنهاد کارهای آینده ارائه خواهد گردید.

۲- ساختار الگوریتم AES

الگوریتم AES رمزنگاری کلید متقارن می‌باشد که در آن هر دو فرستنده و گیرنده از یک کلید واحد برای رمزنگاری استفاده می‌کنند. ساختار این الگوریتم بدین‌صورت است که یک جعبه شامل چندین ماژول وجود دارد. متن اصلی و کلید رمزنگاری با طول رشته‌های ثابت به‌صورت بلوک‌های پیاپی وارد این جعبه می‌شوند و پس از گذراندن یک رشته عملیات به‌صورت رمز شده از جعبه خارج می گردند. درنهایت تمام بلوک‌ها پس از خروج از جعبه کنار یکدیگر قرار داده شده و متن رمز شده تولید می‌شود. طول رشته برای متن اصلی ۱۲۸ بیت و برای کلید نیز ۱۲۸ بیت است. طول کلید ورودی این ساختار متفاوت است که این بستگی به حالت الگوریتم AES دارد. الگوریتم مذکور در سه ساختار تولید شده است و حداقل طول رشته برای کلید این الگوریتم ۱۲۸ بیت است.

در مرحله اول یک عملیات XOR وجود دارد. کلید در همان آغاز وارد چرخه شده و برای تک‌تک مراحل موجود توسط ماژول تولید Sub Key اقدام به تولید کلیدهای جدید می‌کند. پس از اولین مرحله عملیات XOR متن وارد ۱۰ مرحله عملیات به شرح زیر می‌گردد. در هر مرحله ۴ عملیات انجام می‌شود. مرحله اول جایگزینی، در مرحله دوم عملیات جابجایی انجام می‌شود. در مرحله سوم باز عملیات جایگزینی و درنهایت عملیات XOR روی ۱۲۸ بیت رشته انجام می‌پذیرد. مشخص است که Sub Key

[1] Singular Value Decomposition
[2] Data Encryption Standard
[3] Advanced Encryption Standard

تولید شده برای هر مرحله در مرحله چهارم وارد چرخه می‌شود [۲۲و۲۳].

مراحل این الگوریتم به‌صورت ذیل تشریح می‌شوند:

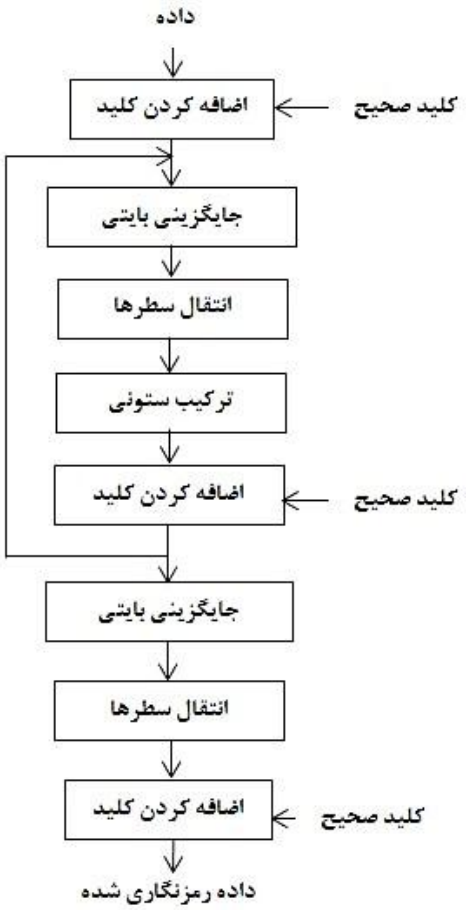
۱. ۱۲۸ بیت به ترکیبی ۸ تایی از دو بایت تبدیل می‌شود؛ یعنی ۸ رشته ۱۶ بیتی و هر بایت با یک بایت متفاوت دیگر جایگزین می‌گردد و این اطلاعات درون یک جدول ثبت می‌شود. احتمال جایگزینی در این حالت ۲ به توان ۸ است؛ یعنی ۲۵۶ حالت ممکن برای این جایگزینی ها وجود دارد. به عبارت دیگر، ترکیبات متفاوتی از ۰ و ۱ ها برای این ساختار حاصل می‌شود.

۲. جابجایی بیت‌ها، بر اساس یک ساختار مشخص بیت‌ها با یکدیگر جابجا می‌گردند.

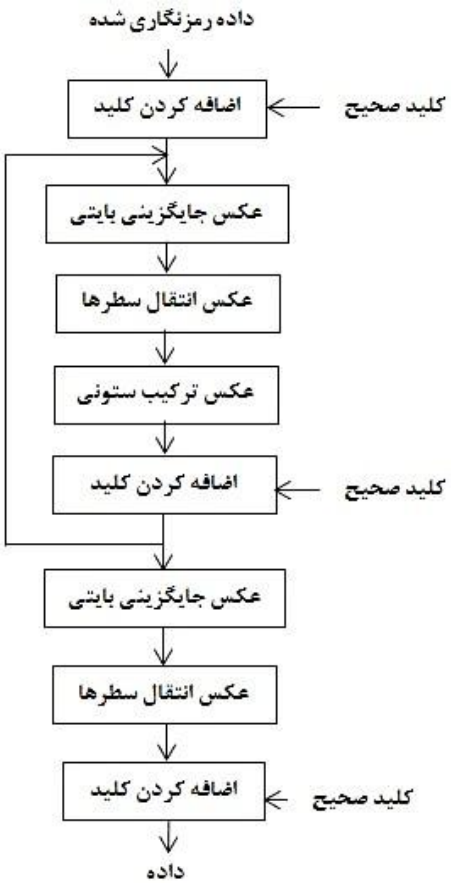
۳. در این مرحله از جایگزینی، عملیات به‌صورت ۴ بایت ۴ بایت انجام می‌پذیرد. درنتیجه 2^{32} حالت ممکن به وجود می‌آید. چون تهیه یک جدول برای این تعداد حالت مشکل است، به همین دلیل یک رابطه جایگزین جدول در این مرحله می‌گردد.

۴. در این مرحله عملیات XOR با یک کلید جهت اعمال روی بیت‌ها وارد ساختار می‌شود [۲۲و۲۳].

نمودار فرآیند رمزنگاری و رمزگشایی AES در شکل‌های (۱) و (۲) نشان داده شده است [۲۴].



شکل (۱) رمزنگاری با AES.



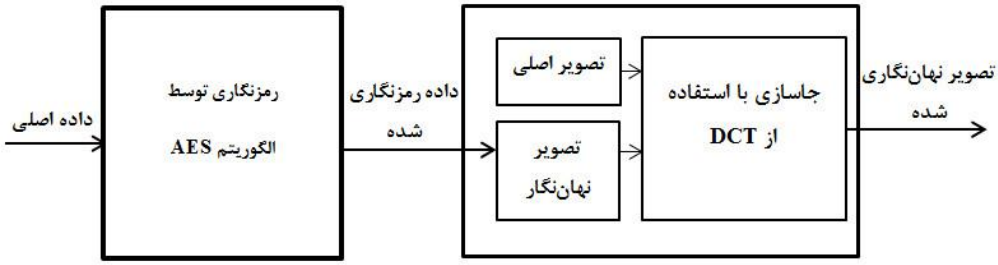
شکل (۲) رمزگشایی با AES.

۳- معرفی رویکرد پیشنهادی

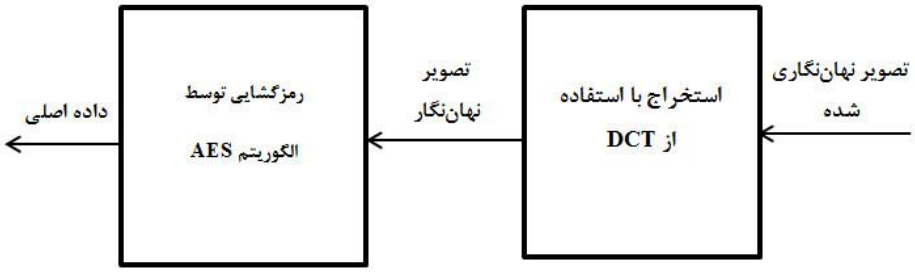
در این مقاله سعی شده است که با استفاده از الگوریتم رمزنگاری قوی AES به‌عنوان رمزنگار اولیه قبل از طرح نهان‌نگاری مبتنی بر تبدیل کسینوسی گسسته (DCT)، یک سیستم نهان‌نگار مقاومی طراحی شود. به این منظور، یک روش نهان‌نگاری کور در دامنه فرکانسی ارائه شده که یک تصویر خاکستری را نهان‌نگاری می‌کند. الگوریتم مورد نظر یک تصویر باینری را درون یک تصویر خاکستری مخفی می‌نماید. بدین منظور ابتدا داده‌ها به داده‌های دستگاه اعداد پایه ۱۶ تبدیل شده و توسط الگوریتم رمزنگاری قوی AES رمزنگاری شده و تصویر باینری به

دست می‌آید. سپس تصویر باینری که همان نهان‌نگاری است، توسط کلیدی رمزگذاری مد زنجیره‌ای (CBC) می‌شود. این عمل سبب مقاوم‌تر شدن نهان‌نگاری در برابر شناسایی و حذف می‌شود. سپس تصویر اصلی به بخش‌های جداگانه‌ای بر اساس الگوریتم تقسیم شده و هر بخش، جداگانه تحت تبدیل DCT قرار می‌گیرد. نهان‌نگاری رمز شده نیز به‌طور جداگانه توسط الگوریتم جاسازی، در هر یک از این قسمت‌ها، مخفی می‌شود.

در الگوریتم جاسازی از روابط بین ضرایب همسایه استفاده می‌شود و نهان‌نگاری در بین ضرایب میانی مخفی می‌گردد. پس از عملیات جاسازی عکس عملیات تبدیل انجام می‌شود و دوباره بخش‌های مختلف تصویر کنار یکدیگر قرار می‌گیرند و تصویر نهان‌نگاری شده را به وجود می‌آورند. سپس توسط الگوریتم رمزنگاری قوی AES داده را از تصویر نهان‌نگاری شده به دست می‌آورد. تغییراتی که سیستم نهان‌نگاری موجود روی تصویر به وجود می‌آورد و غیرقابل رؤیت است، در صورت استخراج نهان‌نگاره به هر طریقی بدون داشتن کلید و بردار ابتدایی غیرقابل تحلیل است. شکل‌های (۳) و (۴)، بلوک دیاگرام کلی این سیستم نهان‌نگاری را نشان می‌دهد که شکل (۳) بخش رمزنگاری و جاسازی و شکل (۴) بخش استخراج و رمزگشایی است.



شکل (۳) بلوک دیاگرام کلی سیستم رمزنگاری و نهان‌نگاری.



شکل (۴) بلوک دیاگرام کلی سیستم استخراج تصویر نهان‌نگاری و رمزگشایی.

مزایای مهم این روش، استخراج کور نهان‌نگاری از تصویر نهان‌نگاری شده است. به این ترتیب برای استخراج نهان‌نگاری در طول فرآیند استخراج، نیازی به تصویر اصلی و مقایسه آن با تصویر نهان‌نگاری شده نیست. این مزیت باعث کمتر شدن بار محاسباتی سیستم نهان‌نگاری می شود. مزیت بعدی این روش استفاده از دو مرحله رمزنگاری است که این عمل باعث بالا رفتن امنیت اطلاعات می‌گردد. در فرآیند استخراج، همانند فرآیند جاسازی، تصویر دریافتی به چندین بخش تقسیم شده و از هر بخش به‌طور جداگانه تبدیل DCT گرفته می‌شود. آنگاه طبق روابط موجود بین ضرایب میانی با ضرایب همسایه، اطلاعات مخفی شده استخراج می‌شود. ضرایب میانی که مورد بررسی قرار می‌گیرند، می‌توانند ضرایب ثابتی باشند یا اینکه توسط اعداد تصادفی انتخاب گردند.

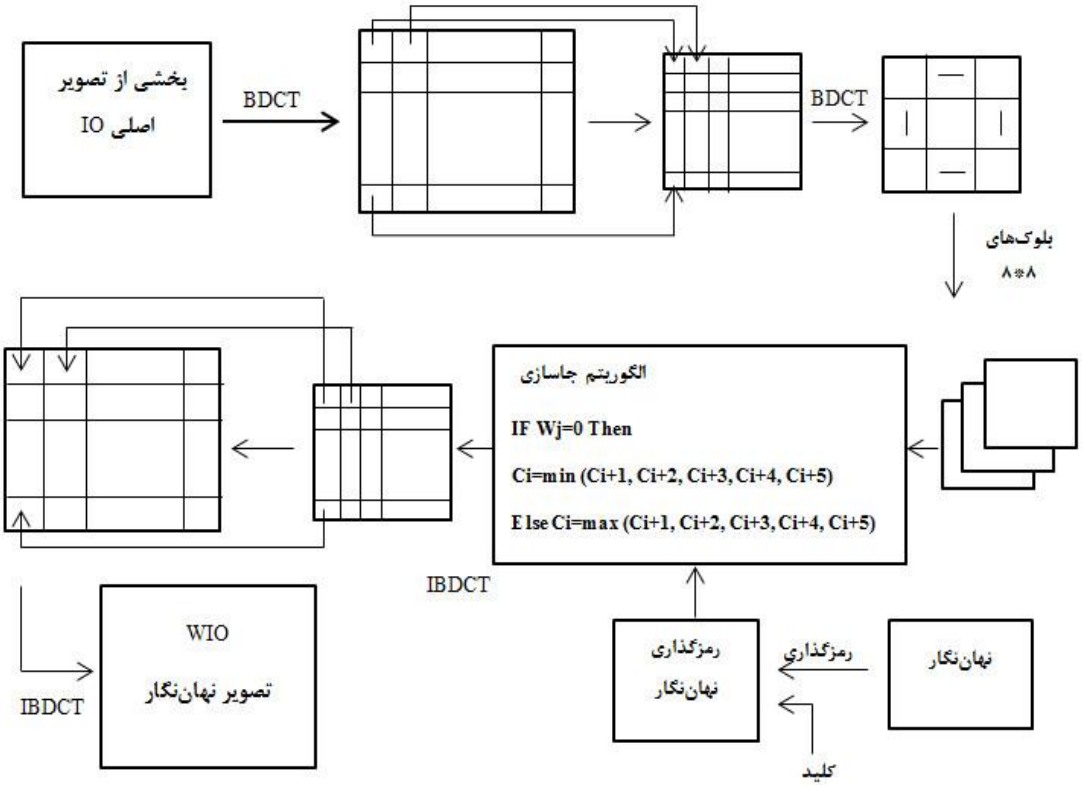
۳-۱- الگوریتم جاسازی در دامنه فرکانسی با استفاده از تبدیل DCT

بخشی از تصویر به‌عنوان سندی که باید نهان‌نگاری شود (W) و بخشی از نهان‌نگاری (IO) به‌عنوان نهان‌نگار وارد می‌شوند. صرفاً برای نام‌گذاری از حروف به‌صورت اختصار استفاده می‌شود و معنای دیگری ندارند. IO تحت تبدیل BDCT قرار می‌گیرد (تبدیل کسینوسی گسسته تحت بلاک‌های ۸×۸). سپس با استفاده از اعداد شبه تصادفی، یکی از ضرایب میانی بلاک‌های ۸×۸، از ماتریس ضرایب حاصل (DIO) انتخاب می‌شوند. با استفاده از این ضرایب انتخاب شده، یک ماتریس کوچک‌تر که ابعادش نسبت به

DIO، ۱/۸ برابر است، تشکیل می‌شود که هر درآیه آن یکی از ضرایب انتخابی از بلاک‌های DIO است و در جایگاه متناسب با بلاک متناظرش در DIO قرار دارد. از این ماتریس (RDIO) که خود ضرایب DCT یک ماتریس بزرگ‌تر است، تبدیل کسینوسی گسسته تحت بلاک‌های ۸×۸ گرفته می‌شود و ماتریس DRDIO به وجود می‌آید. اکنون در هر بلاک ۴ ضریب بر اساس مراجع [۱و۲۵] انتخاب و با استفاده از همسایگی آن با ضرایب اطرافش عملیات جاسازی طبق شبه کد زیر انجام می‌شود:

```
IF Wj=0 Then
Cki=MIN(Ci+1,Ci+2,Ci+3,Ci+4,Ci+5)
ELSE
    Cki=MAX(Ci+1,Ci+2,Ci+3,Ci+4,Ci+5)
```

که در آن، Wj مبین jامین بیت نهان‌نگار مورد نظر و Cki نشان دهنده یکی از چهار ضریب انتخابی از بلاک‌های ۸×۸ می‌باشد. پس از عمل جاسازی، ماتریس ضرایب DRDIO تبدیل به WDRDIO خواهد شد. از WDRDIO تبدیل کسینوسی گسسته معکوس تحت بلاک‌های ۸×۸ می‌گیریم. سپس هر عنصر از این ماتریس را که یکی از ضرایب میانی بلاک متناظرش در DIO است را به جایگاه خود باز می‌گردانیم تا بدین ترتیب ماتریس WDIO به دست آید. اکنون از ماتریس حاصل تبدیل کسینوسی گسسته معکوس می‌گیریم تا WIO حاصل شود. WIO یک تصویر نهان‌نگاری شده می‌باشد. شکل (۵) بلاک دیاگرام جاسازی را نمایش می‌دهد.



شکل (۵) بلوک دیاگرام جاسازی در دامنه فرکانسی با استفاده از تبدیل DCT .

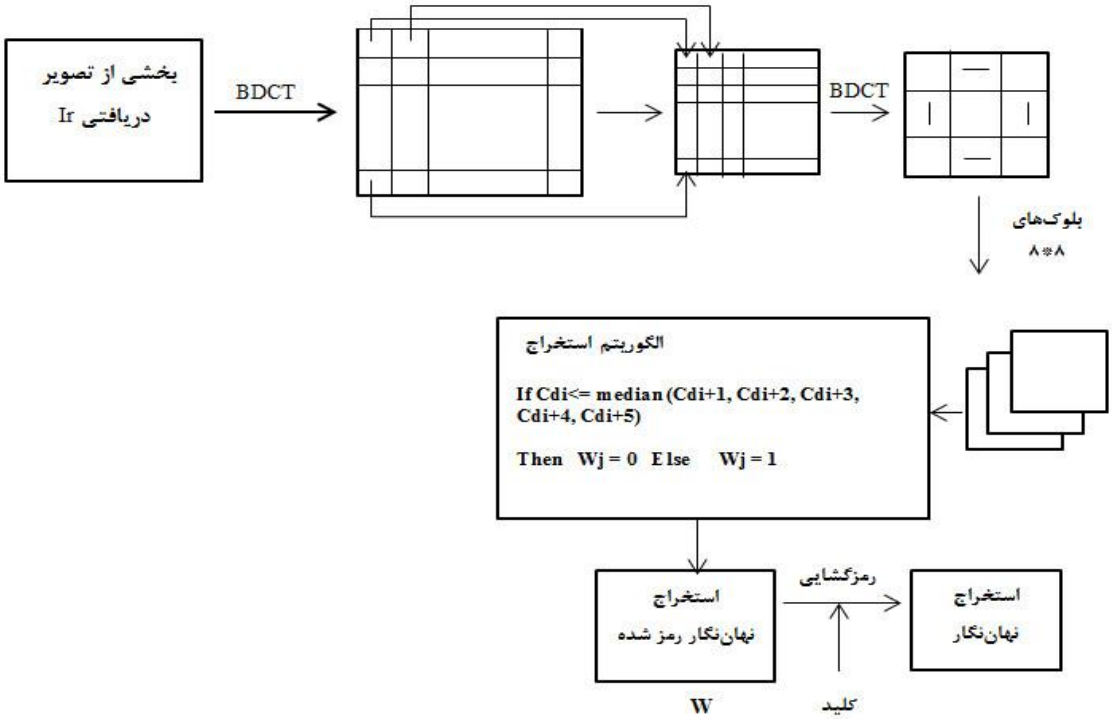
۳-۲- الگوریتم استخراج در دامنه فرکانسی با استفاده از تبدیل DCT

در این قسمت نیز تا حدودی اعمال انجام شده در فرآیند جاسازی انجام می‌شود. پس از دریافت بخش مورد نظر بنام Ir، از آن تحت بلاک‌های ۸×۸ تبدیل DCT گرفته می‌شود و بدین ترتیب BDIr حاصل می‌گردد. از هر بلاک ۸×۸ یک یا چند ضریب، بر طبق همان روندی که در مرحله جاسازی انتخاب شده بود، انتخاب می‌شود. سپس از کنار هم قرار دادن ضرایب متناظر از بلاک‌های ۸×۸ ماتریس کوچک‌تری تولید می‌گردد، به‌طوری که هر عنصر از این ماتریس، عضوی از یک بلاک ۸×۸ است و متناظر با جایگاه بلاک خودش قرار گرفته است. ابعاد ماتریس حاصل برابر ۱/۸ ماتریس BDIr است که می‌توان نام آن را RBDIr گذاشت. از RBDIr تحت بلاک‌های ۸×۸ تبدیل DCT گرفته می‌شود. اکنون ضرایب حاصله از هر بلاک طبق مراجع [۱و۲۵] انتخاب و بر اساس رابطه آن با

ضرایب هم‌جوارش، نهان‌نگار رمز شده بر اساس شبه کد آورده شده، استخراج می‌شود:

If Cdi<= median (Cdi+1, Cdi+2, Cdi+3, Cdi+4, Cdi+5)
Then
Wj = 0
Else
Wj = 1

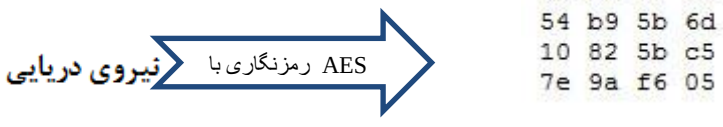
که در آن، Wj مبین j امین بیت استخراج شده و Cdi نشان‌دهنده d امین ضریب انتخاب شده است. پس از استخراج کامل، W با استفاده از کلید مخصوص رمزنگاری، رمزگشایی شده و به این ترتیب، بخش دیگری از نهان‌نگار در دسترس است. بلوک دیاگرام شکل (۶) روند استخراج در دامنه فرکانسی با استفاده از تبدیل کسینوسی گسسته را نمایش می‌دهد.



شکل (۶) بلوک دیاگرام روند استخراج در دامنه فرکانسی با استفاده از تبدیل DCT.

۴- نتایج شبیه‌سازی

برای شبیه‌سازی این روش، داده با عنوان «نیروی دریایی» در نظر گرفته می‌شود و به داده دستگاه اعداد پایه ۱۶ تبدیل می‌گردد. برای شبیه‌سازی از نرم‌افزار MATLAB ۲۰۱۴ استفاده شد. با استفاده از الگوریتم رمزنگاری AES داده، دستگاه اعداد پایه ۱۶ مطابق شکل (۷) رمزنگاری می‌شود.

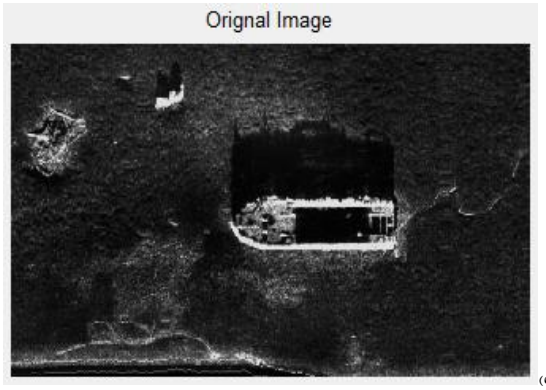


(الف) (ب)

شکل (۷) (الف) داده اصلی و (ب) داده رمزنگاری شده توسط AES.

داده توسط الگوریتم AES رمزنگاری می‌شود و سپس جهت انجام نهان نگاری، یک تصویر کف دریا که توسط سونار اسکن جانبی گرفته شده، به عنوان تصویر اصلی در نظر گرفته می‌شود و تصاویر داده رمزنگاری شده توسط AES به‌عنوان تصاویر نهان‌نگار استفاده می‌شود، به طوری که شکل (۸-الف) شامل تصویر اصلی و (۸-ب) تصاویر نهان‌نگار درآیه اول تا درآیه ۱۶ از شکل (۷-ب) می باشد. شکل (۹-الف) تصویر نهان نگار شده اصلی و (۹-

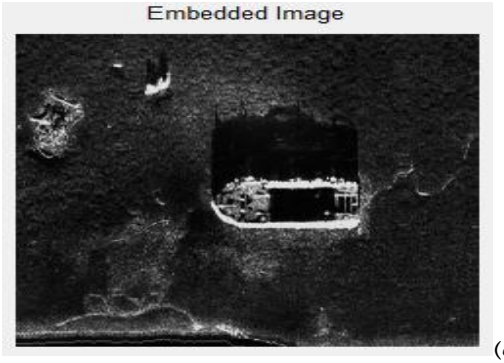
ب) تصاویر نهان‌نگاری استخراج شده درآیه اول تا درآیه ۱۶ است.



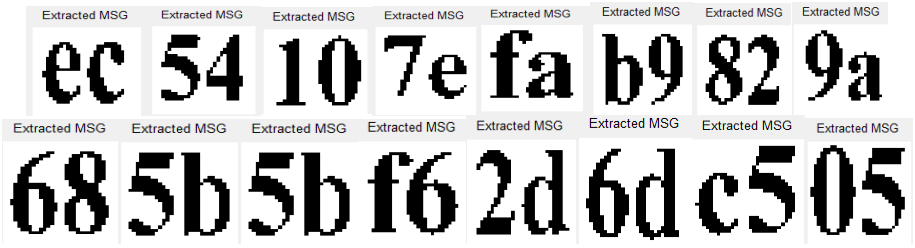
(الف)

(ب)

شکل (۸): (الف) تصویر اصلی و (ب) تصاویر نهان‌نگار.

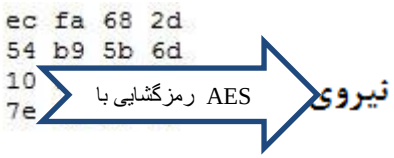


(الف)



(ب)

شکل (۹) (الف) تصویر نهان‌نگاری شده و (ب) نهان‌نگار استخراج شده.



(ب) (الف)

شکل (۱۰) (الف) داده رمزگشایی شده توسط AES و (ب) داده اصلی.

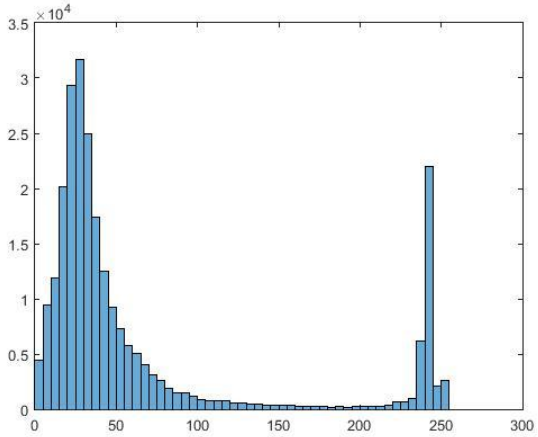
حالا با توجه به تصاویر نهان‌نگاری استخراج شده و با استفاده از الگوریتم AES آن‌ها را رمزگشایی کرده و داده اصلی را به‌صورت شکل (۱۰) به دست می‌آوریم.

همان‌طور که مشاهده می‌شود، روش فوق در عین ساده بودن تبدیل DCT، به علت کاربرد الگوریتم AES دارای امنیت بسیار بالایی می‌باشد و نیز بین تصویر اصلی و تصویر نهان‌نگاری شده از نظر ظاهری، تفاوت زیادی وجود ندارد. نسبت سیگنال به نویز PSNR[1] بین تصویر اصلی و تصاویر نهان‌نگاری شده برابر ۴۰/۹۵۳ اندازه‌گیری شده است. برای تخمین شباهت نهان‌نگار استخراج شده و نهان‌نگار اصلی از رابطه همبستگی متقابل نرمالیزه (NCC[2]) استفاده شده است. به این ترتیب شباهت بین نهان‌نگاری اصلی و نهان‌نگاری استخراج شده برابر ۱ اندازه‌گیری شد. بعد از این مرحله، اثرات حملات برش، تغییر اندازه و اضافه کردن نویز روی تصویر نهان‌نگاری شده به‌صورت جدول (۱) بررسی شد. ملاحظه می‌شود NCC مقادیر قابل قبولی را برای آشکارسازی نهان‌نگار فراهم نموده است.

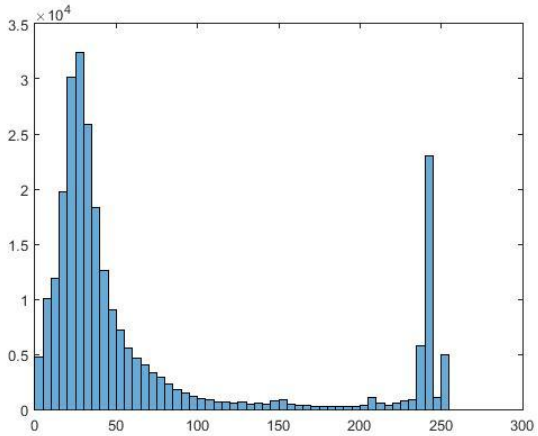
جدول (۱) مقاومت در مقابل حملات مختلف.

نوع حمله	PSNR	NCC
برش	۱۰/۷۳	۰/۵۶
نویز گوسی	۲۰/۰۵	۰/۴۱
فیلتر میانه	۲۶/۶۲	۰/۶۵
فیلتر پایین‌گذر	۲۵/۷۶	۰/۶۴
فشرده‌سازی ٪۸۰	۲۵/۵۹	۰/۹۲
فشرده‌سازی ٪۵۰	۲۵/۴۳	۰/۸۴
فشرده‌سازی ٪۲۰	۲۵/۱۰	۰/۶۴

با بررسی هیستوگرام تصویر نهان‌نگاری شده و تصویر اصلی مشاهده می‌شود هیستوگرام دو تصویر نزدیک به هم می‌باشد. محورها عمودی و افقی به ترتیب تعداد پیکسل‌ها و شدت روشنایی را نشان می‌دهد.



(الف)



(ب)

شکل (۱۱) (الف) هیستوگرام تصویر اصلی و (ب) هیستوگرام تصویر نهان‌نگاری شده.

۵- نتیجه‌گیری

در این مقاله، روش نهان‌نگاری دیجیتالی با استفاده از الگوریتم AES در تصاویر مورد مطالعه و بررسی قرار گرفت. با توجه به اینکه در نهان‌نگاری دیجیتالی، حجم اطلاعات جاسازی شده نسبت به پارامترهای دیگری مثل مقاومت، نامرئی بودن، نوع استخراج و غیره اهمیت بالایی ندارد و از طرفی فضای فرکانسی تصویر نیز می‌تواند در برآورده کردن نیازهای اصلی، مؤثرتر باشد، روش ارائه‌شده از فضای فرکانسی استفاده می‌کند و یک روش نهان‌نگاری در تصاویر JPEG، ارائه می‌دهد. طبق این روش، یک تصویر به قسمت‌هایی تقسیم می‌شود و هر قسمت توسط تبدیل DCT به فضای فرکانسی برده شده و الگوریتم

[1] Peak Signal to Noise Ratio
[2] Normalized Cross Correlation

جاسازی روی آن انجام می‌شود. سپس عکس تبدیل‌های مذکور صورت گرفته و قسمت‌های مختلف تصویر به فضای پیکسلی برگردانده و در کنار یکدیگر قرار می‌گیرند. در این روش، استخراج بدون نیاز به تصویر اصلی صورت می‌گیرد. همچنین با توجه ساختار ساده تبدیل DCT و استفاده از رمزگذاری در طول عملیات، بخصوص استفاده از الگوریتم رمزنگار AES، امنیت روش پیشنهادی را در عین سادگی بالا برده است، به‌طوری که امکان کشف و استخراج داده اصلی را از نهان‌نگار به کمترین حالت ممکن می‌رساند و در مقابل حملات مختلف نیز مقادیر NCC قابل قبولی برای آشکارسازی ارائه می‌دهد.

منابع

[1] R. Tomar, J. C. Patni, A. Dumka and A. Anand, "Blind Watermarking Technique for Grey Scale Image using Block Level Discrete Cosine Transform (DCT)", Emerging ICT for Bridging the Future, Vol.2, pp.81-89, 2015.

[2] W. C. Chu, "DCT-Based Image Watermarking using Sub sampling," IEEE Transactions on Multimedia, Vol.5, No.1, pp.1640-1647, 2003.

[3] P. W. Wong and N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification", IEEE Transactions on Image Processing, Vol.10, No.10, pp.1593-1601, 2001.

[4] Y. Kim, K. Moon and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-Word Space Statistics", 7th International Conference on Document Analysis and Recognition, pp.775-779, 2003.

[5] D. Kirovski, H. Malvar, "Robust Spread Spectrum Audio Watermarking", IEEE Conference on Acoustics, Speech, and Signal Processing, Vol.3, pp.1345-1348, 2001.

[6] S. Foo, T. Yeo and D. Huang, "An Adaptive Audio Watermarking System", IEEE Conference on Electrical and Electronic Technology, Vol.2, pp.509-513, 2001.

[7] H. Inoue, A. Miyazaki and T. Katsura, "An Image Watermarking Method based on the Wavelet Transform", International Conference on Image Processing, Vol.1, pp.296-300, 1999.

[8] C. Lu, H. Yuan and M. Liao, "Multipurpose Watermarking for Image Authentication and Protection", IEEE Transactions on Image Processing, Vol.10, No.10, pp.1579-1592, 2001.

[9] A. Herrigel, J. Ruanaidh, H. Petersen, S. Pereira and T. Pun, "Secure Copyright Protection Techniques for Digital Images", International Workshop on Information Hiding, Vol.1525, pp.169-1190, 1998.

[10] M. Buckley, M. Ramos, S. Hemami and S. Wicker, "Perceptually-based Robust Image Transmission Over Wireless Channels", International Conference on Image Processing, Vol.2, pp.128-131, 2000.

[11] R. Wolfgang and E. Delp, "A Watermark for Digital Images", International Conference on Images Processing, pp.219- 222, 1996.

[12] N. Checcacci, M. Barni, F. Bartolini and S. Basagni, "Robust Video Watermarking for Wireless Multimedia Communications", IEEE Wireless Communications and Networking Conference, Vol.3, pp.1530-1535, 2000.

[13] F. Hartung and B. Girod, "Watermarking of Uncompressed and Compressed Video", IEEE Transactions on Signal Processing, Vol.66, No.3, pp.283-301, 1998.

[14] C. Lu and M. Liao, "Video Object-based Watermarking: A Rotation and Flipping Resilient Scheme", International Conference on Image Processing, Vol.2, pp.483-486, 2001.

[15] R. Wolfgang, C. Podilchuk and E. Delp, "Perceptual Watermarks for Digital Images and Video", International Conference on Security and Watermarking of Multimedia Contents, Vol.3657, pp.40-51, 1999.

[16] C. Y. Yang, W. Hu and J. Lai, "DCT-based Watermarking by Quotient-Embedding Algorithm", 3rd International Conference Innovative Computing Information and Control, 2008.

[17] H. U. Seo, J. S. Sohn, B. I. Kim, T. G. Lee, S. I. Lee and D. G. Kim, "Robust Image Watermarking Method using Discrete Cosine Composition and Just Noticeable Distortion", The 23th International Technical Conference on Circuits/Systems, Computers and Comunicatuions, pp.765-768, 2008.

[18] P. Kumar and S. K. S. Gupta, "Improved RST-Attacks Resilient Image Watermarking based on Joint SVDDCT", International Conference on Computer and Communication Technology, pp.46-51, 2010.

[19] L. R. Zhen and T. T. Niu, "SVD based Digital Watermarking Method", Chinese

Journal of Electronics, Vol.29, No.2, pp.168-171, 2001.

[20] C. C. Lai and C. C. Tsai, “Digital Image Watermarking using Discrete Wavelet Transform and Singular Value Decomposition”, IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 11, pp.3060- 3063, 2010.

[21] سید محمدرضا موسوی، محمد خویشه و مجید آقابابایی، "مدل‌سازی و حذف کلاتر سونار فعال"، دانشگاه علوم دریایی امام خمینی (ره)، ۱۳۹۴.

[22] J. Daemen and V. Rijmen, “The Design of Rijndael: AES-The Advanced Encryption Standard”, Springer, Verlag, Berlin, Science & Business Media, 2002.

[23] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, “Strong Authentication for RFID Systems using the AES Algorithm”, Cryptographic Hardware and Embedded Systems, Vol.3156, pp.357-370, 2004.

[24] M. Dhankar and J. Soni, “DWT-SVD based Highly Secure Image Data Hiding System with AES Encryption”, International Journal of Engineering Research and General Science, Vol.3, No.5, pp.266-273, 2015.

[25] F. Duan, I. King, L. Xu and L. Chan, “Intrablock maxmin Algorithm for Embedding Robust Digital Watermark into Images,” International Workshop on Multimedia Information Analysis and Retrieval, Vol.1464, pp.255-264, 1998.