وابستگی کلیدی تصاویر نهان‌نگاری با استفاده از لبه یابی

شهزاد عالم، وپین کومار، واسیم ا صدیقی و مشیر احمد
دپارتمان مهندسی کامپیوتر، دانشکده فنی و مهندسی،
Jamia Millia Islamia, New Delhi-110025, INDIA
{shahzad5alam, vipin.kumar, was.jmi}@gmail.com

مترجم حسین اصحابی
passhabi@outlook.com

چکیده-نهان‌نگاری علم ارتباط داشتن بصورت نامریی است. هدف آن مخفی کردن اطلاعات حساس در در داخل رسانه دیجیتال به نحوی که مخفی باشد. دراین مقاله به دنبال پیشنهاد یک طرح بهبود یافته از نهان‌نگاری ایمن در تصویر هستیم که به تازگی توسط Chen et al. مطرح شده است. طرح بهبود یافته secret key (کلید رمز گذاری) براساس random LSB substitution (جایگذاری در LBS بصورت تصادفی) است. همچنین از امتیازات لبه یابی براساس وابستگی پیکسل هم بهره می‌برد تا به سطح بالایی از ظرفیت برای جاسازی در تصویر، برسد؛ و نتایج آزمایشات انجام شده گویای گفته فوق است. امتیاز بالای PSNR از اینکه تفاوت چندانی میان cover Image(تصویر پوششی) و stego-image (تصویر-نهان‌نگاری) نیست، پرده برمیدارد. علاوه بر این، طرح بهبود یافته قابل اطمینان است و میتواند بطور موثر از پیام جاساز شده در برابر steganalysis (آنالیز نهان‌نگاری) محافظت کند؛ به لطف تصادفی بودن پیکسلهای وابسته و وابستگی کلید.

کلمات کلیدی— نهان‌نگاری، لبه یابی، امنیت، سیستم‌های آشوب، عدم نفوذ.

I. مقدمه

تکنولوژی‌های نهان‌نگاری برای انتقال اطلاعات حساس که پنهان شده است بسیار مهم هستند در فضای شبکه‌های مستعد حمله. علم نهان‌نگاری دیجیتال در اصل از فقدان قدرت سیستم‌های رمزنگاری ناشی شده است تا بتوان در یک محیط باز سیستمی، محرمانگی خواستار شده را داشت. تقریبا تمام داده‌های دیجیتال ساده، خواه تصویر باشد یا متن یا هر رسانه دیگری، می‌تواند در رسانه پوششی مخفی شود. براساس رشدی خوبی که در استفاده از تصاویر گرافیکی، در ارتباطات داشته‌ایم، پژوهش فوق با نهان‌نگاری تصویر آغاز میشود؛ این شاخه با سرعتی بسیار سریع ادامه یافته. وقتی در نهان نگاری با تصاویر دیجیتال سر و کار داریم [۴]، معمولا از سطح خاکستری و رنگ پیکسل فایلهای تصویری استفاده می‌شود. تکنیکهای نهان‌نگاری تصویر نیازمند دو فایل هستند: تصویر پوششی و داده (پیام) که میخواهیم مخفی شود. یکی از برتریهای تصاویر دیجیتال نسبت به ویدیوها، اندازه آنهاست، که باعث میشود در شبکه‌های با پهنای باند کم، بیشتر از تصاویر دیجیتال استفاده بشود تا ویدیوهای دیجیتال که اندازه بزرگ و زائدی دارند [۹].

مفهوم و اصل "آنچه که می‌بینی آن چیزی است که بدست می آوری"، که در هنگام چاپ تصاویر و دیگر اقلام گاهی با آن مواجه می‌شویم، دیگر دقیق نیست و یک نهان‌نگار را همیشه گول نمی‌زند. تصاویر می‌توانند بیشتر از چیزی که ما انسان‌ها با سیستم بینایی مان (HVS) میبینیم، باشد. نهان‌نگاری بر پایه امنیت اطلاعات برای انتقال داده محرمانه ضروریست. سه نیاز پایه در فیلد نهان‌نگاری دیجیتال وجود دارد. نیاز اول ظرفیت است. یعنی تعداد بیتهای رمزی که در هر پیکسل کار پوششی قرار است جاساز شود. ظرفیت بالاتر یعنی داده بیشتری در رسانه پوششی ذخیره میشود. نیاز دوم Robustness (تنومندی) است که از اطلاعات حساس در مقابل حملات جلوگیری می‌کند. نیاز سوم Imperceptibility (عدم نفوذ)، هم معمولا توسط نرخ سیگنال به نویز محاسبه میشود. از اینرو رسانه-نهان‌نگاری وقتی که عدم نفوذ بالاست، مفید شناخته میشود. زمانی که نهان‌نگاری به عنوان روشی برای مخفی کردن اطلاعات محرمانه برای انتقال و ارتباط گمارده میشود، عدم نفوذ به نیاز خیلی مهم در کنار تنومندی تبدیل می‌شود[۷] و احتمالا ظرفیت قربانی میشود [۳]. یک طرح قوی و کارا، بطور محتاطانه ایی به تاثیر هر سه نیاز توجه دارد.

نهان‌نگاری جایگزینی LSB یکی از معمولترین روش‌ها هست که بطور گسترده استفاده میشود؛ که در آن کمترین مقدار ارزشی هر بیت (LSB) با بیت پیام محرمانه جایگزین میشود تا جایی که پیام به اتمام برسد. گرچه، تکنیک ساده‌ایی است اما احتمال شناسایی داده مخفی بالاست که تهدیدی برای امنیت حساب میشود. در رویارویی با این مشکل، یک روش ساده و موثر مفهوم تکنیک لبه یابی هیبرید را برای جایگزینی LSB به کار گرفته است که توسط Chen et al. [۱] مطرح شده است. طرح آنها مستقل از کلید است و تعداد بیتها برای جاسازی، به پیکسل‌های لبه تصویر پوششی وابسته است. در این کار یک طرح نهان‌نگاری تصویر بر پایه یک کلید وابسته به جایگذاری تصادفی در LSB به همراه تکنیک تشخیص لبه مطرح شده است. جایگذاری تصادفی در LSB براساس کلید مخفی است و همچنین مقدار پیکسل تا بتواند تنومندی را افزایش دهد. این نتایج تجربی نشان می‌دهد که طرح بهبود یافته خوبی‌های طرح Chen et al. را به ارث برده است. همینطور طرح بهبود یافته بر پایه لبه یابی، علاوه بر کارآمد بودن، در برابر تحلیل‌های نهان‌نگاری غیرمجاز قابل اطمینان است.

II. متن اصلی

برای ایجاد یک برنامه وابستگی کلید نهان‌نگار LSB با استفاده از تکنیک لبه یابی که بتواند در مقابل تحلیل‌های نهان‌نگاری پایدار باشد، طرح Chen et al. را تغییر می‌دهیم. تغییرات شامل آغاز وابستگی کلیدی و تصادفی بودن است. در هر پیکسل تصویر پوششی، مکانیزم تغییر یافته اجازه انتخاب اعدادی تصادفی از LSB را روی یک کلید مخفی میدهد که برای جایگزینی پیام مخفی استفاده می شود. برای اینکه بیتها جاساز شوند، ابتدا آنها با تعدادی مساوی از پر ارزش ترین بیتها (MSBs) از همان پیکسل رمزگذاری میشود.

این تغییر نه تنها به عدم نفوذ کمک می‌کند بلکه روی تصادفی بودن، وابستگی پیکسل‌ها و وابستگی کلید هم تمرکز دارد تا درکنار جاسازی بارگذاری (payload) بالا

978-1-4799-4910-6/14 $31.00 © 2014 IEEE
DOI 10.1109/ACCT.2014.72

به تنومندی برسد. chaotic logistic map (نقشه منطق آشوب) برای تولید زنجیره تصادفی به کار گرفته شده است و لابه یابی canny هم برای استخراج لبه از تصویر پوششی که توضیح هر دو در ادامه آورده شده است.

A. *Chaotic 1D Logistic Map*

نقشه منطقی یک-بعدی توسط R. M.May [۱۰] مطرح شده است که یکی از ساده‌ترین سیستم‌های گسسته آشوب غیرخطیست که رفتار آشوبگری را نمایش می‌دهد؛ توسط رابطه زیر کنترل می‌شود.

$$w(n+1) = \lambda w(n)(1- w(n)) \qquad (۱)$$

w(0) شرط اولیه است، λ پارامتر سیستم است و n تعداد تکرار است. پژوهش فوق نشان می‌دهد که نقشه برای ۳٫۵۷ < λ < ۴ و $w(n+1) \in (0,1)$ برای تمام nها دارای هرج و مرج یا آشوب است.

B. *Canny Edge Detection*

یک لبه براساس تغییرات قابل توجه در سطوح خاکستری توصیف می‌شود تا مرز بین دو ناحیه در تصویر را نشان دهد. لبه یابی یکی از اصلی‌ترین ابزارها در پردازش تصویر، بینایی ماشین و بینایی کامپیوتر خصوصا در حوزه تشخیص ویژگی ها و استخراج ویژگی‌ها است. لبه یاب *Canny* سختگیر و به عنوان اپراتوری که از آن بیشتر استفاده را میشود، شناخته شده است. لبه یاب *Canny* ۳ مشخصه دارد [۲]. (۱) هیچ لبه غیر مهمی هم نباید از قلم بی‌افتد، و هیچ لبه‌ایی تشخیص اشتباه داده نشود. (۲) تفاوت میان مکان تعیین شده و واقعی لبه باید در کمترین حد (۳) باشد و فقط یک پاسخ به یک لبه واحد وجود دارد.

III. متد مطرح شده

طرح بیان شده یک بهبود روی طرح پیشنهادی Chen et al. [۱] است. طرح ما نه‌تنها ویژگی ظرفیت بالا جاسازی داده و عدم نفوذ خوب روی تصاویر stego بهره مند است بلکه روی تنومندی در برابر آنالیزهای نهان‌نگاری که توسط آنالیزهای آماری انجام میشود و در طرح Chen et al. [۱] در نظر گرفته نشده است تمرکز دارد. طرح از تولید کلید مخفی تصادفی (عدد) استفاده میکند که با استفاده از نقشه منطقی آشوب برای جایگزینی LSB تصادفی بر اساس لبه های تصویر پوششی انجام میشود. مقدار اولیه *w(0)* از فرمول آشوب، به عنوان کلید مخفی برای انتخاب تصادفی مقدار بیتهایی از پیام عمل میکند که باید در یک پیکسل جاسازی شود. تنومندی به سبب رمزگذاری بیت‌های پیام با پرارزشترین مقدار بیتی پیکسل، حاصل میشود.

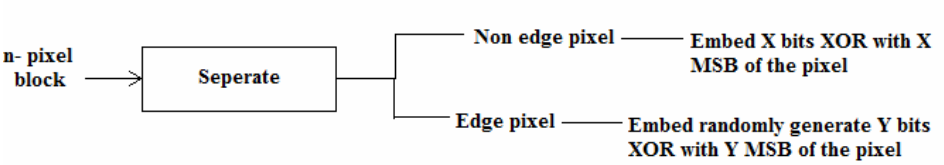
مراحل روش پیشنهادی به شرح زیر است:

گام ۱: لبه یابی اعمال می‌شود تا لبه تصویر B از سطح خاکستری تصویر G بدست آید.

گام ۲: تصویر سطح خاکستری به مجموعه ایی از بلوکها تقسیم میشود، هر بلوک شامل n پیکسل است. در اینجا ما از پیکسل P1 برای ذخیره سازی وضعیت پیکسل دیگر استفاده می‌کنیم. وضعیت هر پیکسل Pi، اگر پیکسل لبه باشد '1' تعریف شده است. در غیر این صورت پیکسل غیر لبه '0' است. توسط عمل جانشینی LSBs وضعیت پیکسل‌ها از P2 تا Pn در داخل P1 ذخیره شده است. برای حفظ کیفیت پیکسل P1 و همچنین برای افزایش ظرفیت بارگذاری در تعبیه کردن، براساس نتایج آزمایش شده، پیشنهاد می‌کنیم که به مقدار n, عدد ۳ و ۴ اختصاص داده شود.

گام ۳: توسط جایگزینی LSB، در یک بلوک برای پیکسل های غیر لبه، 'x' بیت از پیام XOR شده با 'x' پیکسل از MSBs را جاساز می‌کنیم. برای تثبیت کیفیت تصویر stego مقدار x عدد ۱ و یا ۲ است.

گام ۴: برای یک پیکسل لبه در یک بلوک، 'y' بیت از پیام XOR شده با 'y' بیت از پیکسل MSB را توسط جایگزینی LSB، جاساز می‌کنیم. مقدار 'y' بصورت تصادفی برای هر پیکسل توسط نقشه آشوب تولید می‌شود. برای حفظ کیفیت تصویر نهان‌نگاری (stego) عددی بین ۱ تا ۴ برای مقدار y تولید میشود.



شکل۱. دسته بندی و جایگذاری پیکسل‌ها

برای مثال، بیایید فرض کنیم که یک تصویر داریم که ۴ پیکسل به که راست به چپ به ترتیب به صورت {[0 1 0 1 0 1 0 1]، [0 0 0 0 0 0 0 1]، [0 0 1 1 1 1 1 1]، [1 1 1 1 0 0 0 0]} است. متناظر با P1، P2، P3 و P4 با پیام مخفی M = '0 1 0 1 0 1 0'. تصویر A یک بلوک ۴ پیکسلی در نظر گرفته شده است. بیایید در نظر بگیریم که براساس لبه یاب Canny؛ P2 و P4 پیکسل های لبه هستند. واضح است که وضعیت پیکسل P2، P3 و P4 بصورت '101' است. جایگذاری ۳ LSBs در پیکسل P1 با '101'. از اینرو، پیکسل P1 مقدار جدید [1 0 1 0 1 1 0 1] را دریافت می کند و میشود پیکسل P1.

در ادامه فرض میکنم که مقدار پارامتر 'x' عدد ۱ است و مقدار تصادفی 'y' که توسط نقشه آشوب برای پیکسل P2 تولید شده است هم ۴ است. حال 'y' بیت از پیام را با 'y' بیت از پیکسل۲ MSBs، XOR می‌کنیم. یعنی 'Z' = b8b7b6b5 با m1m2m3m4، XOR میشود، بصورت نمایش داده شده در شکل ۱. در اینجا ما 'y' LSBs را در پیکسل P2 با 'z' بیت مخفی جایگزین می کنیم. همچنین، یک LSB در پیکسل۳ را با 'z' = b8XORm1 جایگزین می‌کنیم. بطور مشابه، عدد تصادفی جدید 'y' LSBs را در پیکسل P4 با 'z' بیت مخفی جایگزین می‌کنیم، که 'z' در تعریف عمومی بیانگر 'y' MSBs از یک پیکسل XOR میشود با y بیت از پیام'.

978-1-4799-4910-6/14 $31.00 © 2014 IEEE
DOI 10.1109/ACCT.2014.72

برای پیکسل P4 بگذارید مقدار 'y' را ۳ در نظر بگیریم. مقادیر جدید از پیکسل های P2، P3، P4 هست {[0 1 1 1 0 0 0 1], [0 0 1 1 1 1 1 1], [0 1 0 1 0 0]}.

کلید مخفی در فرآیند استخراج کردن، *w(0)* از نقشه آشوب، هر دو یکی نقش کلیدی را بازی می‌کنند. اگر کلید استفاده شده در طی جاسازی و خارج کردن یکی باشد، تنها می‌توانیم مقدار یکسان از بیت های تعبیه شده در هر پیکسل لبه را بدست آوریم. در غیر اینصورت پیام بصورت صحیح قابل استخراج نیست. این جایست که تنومندی الگوریتم ما وارد میدان میشود. گام های فرآیند استخراج به شرح زیر است.

گام ۱: مشابه عمل تقسیم کردن که در روش قبلی دیدیم. تصویر نهان‌نگاری به n بلوک پیکسلی تقسیم میشود.

گام ۲: براساس $(n-1)$ LSB در پیکسل P1، وضعیت دیگر پیکسل ها از P2 تا Pn را بدست می‌آوریم. از این مقدار وضعیتی، می توانیم دو دسته بندی متناظر، یعنی پیکسل های لبه و پیکسل های غیر-لبه را میتوانیم شناسایی کنیم.

گام ۳: از پیکسل های غیر-لبه، براساس مقدار 'x' که در فرآیند تعبیه سازی استفاده شده، 'x' تعداد از LSB که XOR شده با 'x' پیکسل از MSB را خارج می‌کنیم تا به بیت های پیام منبع دست بیابیم.

گام ۴: از پیکسل لبه، براساس مقدار تصادفی تولید شده 'y' ، 'y' پیکسل از LSB را که با 'y' پیکسل از XOR MSB شده را خارج می‌کنیم تا به قسمتی از پیام برسیم. مقدار 'y' تولید شده برای یک پیکسل در تعبیه سازی و استخراج کردن یکسان خواهد بود اگر کلید مخفی وجود داشته باشد. یعنی مقدار اولیه *w(0)* از نقشه آشوب در سمت گیرنده و فرستنده یکسان خواهد بود.

برای مثال، تصویر نهان‌نگاری A را در نظر بگیرید که چهار پیکسل آن به این شرح است: {[1 0 1 0 1 1 0 1], [1 0 0 0 1 1 1 0], [1 1 1 1 1 1 0 0], [0 0 0 0 1 0 1 0]} متناظر با چهار پیکسل P1، P2، P3 و P4. با توجه به مقدار حاصله 3 = (n -1) تعداد LSB در پیکسل اول، ۳ بیت '1 0 1' را میگیریم.

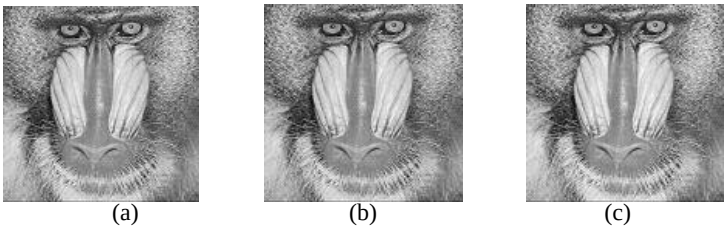
از اینرو پیکسل های دوم و چهارم لبه هستند و پیکسل سوم، پیکسل غیر-لبه است. براساس روش تعبیه سازی، چهار LSB و MSB را از پیکسل P2 استخراج میکنیم و آنها را XOR می‌کنیم. در ادامه سه LSB از P4 را انتخاب و سه MSB از P4 و آنها را با هم XOR می‌کنیم. سپس یک LSB از P3 و اولین MBS از پیکسل P3 را استخراج می‌کنیم و در نهایت آنها را XOR می‌کنیم. بیتهای استخراج شده از پیکسل P2 بصورت '0 1 1 0' هستند. بیت استخراج شده از پیکسل P3 هست '1'. بیت های استخراج شده از پیکسل P4 هست '0 1 0'. با استفاده از این بیتهای استخراج شده، پیام مخفی را بصورت M = '0 1 1 0 1 0 1 0' به دست می آوریم.

IV. نتایج تجربی

طرح مطرح شده به ظرفیت بالایی از تعبیه سازی و کیفیت خوبی در تصویر نهان‌نگاری دست می‌یابد اما در ازای هزینه تنومندی. طرح ما نه تنها بر روی ظرفیت بالا و عدم نفوذ بالا تمرکز کرده بلکه تنومندی را هم در نظر گرفته است. تنومندی در طرح ما به دو شیوه فراهم شده است، (الف) استفاده از جایگزاری LSB تصادفی براساس کلید مخفی، (ب) رمز گذاری n بیت از پیام با n پیکسل از MSB. نقطه قوت طرح ما بر روی کلید مخفی تکیه دارد چراکه باعث میشود که قابل اطمینان در مقابله با آنالیز های نهان‌نگاری وجود داشته باشد. برای انجام آزمایش ما از تصاویر سطح خاکستری ۱۲۸×۱۲۸ استفاده کرده ایم. نتایج آزمایش نمایانگر کارایی طرح ما در شکل ۳-۲ نمایش داده شده است و همینطور جدول I برای تصاویر لِنا و میمون. کیفیت تصویر نهان‌نگاری در منظر PSNR در نظر گرفته شده است. همچنین ما کیفیت تصویر نهان‌نگاری که در تصویر پوششی کار گذاشته شده است را توسط سیستم بینایی انسان مقایسه کردیم. معیار PSNR بیشتر از 40dB است که عملکرد رضایت طرح بهبود یافته روی لبه وابسته به کلید براساس الگوریتم تصویر نهان‌نگاری را نشان می‌دهد.

(a) (b) (c)

شکل۲. تصویر لنا (الف) تصویر اصلی، (ب) تصویر نهان‌نگاری شده با جاسازی ۲۰۳۷بیت، (د) تصویر نهان‌نگاری شده با جاسازی ۱۱۰۷۴ بیت



(a) (b) (c)

شکل۳. تصویر میمون (الف) تصویر اصلی، (ب) تصویر نهان‌نگاری شده با جاسازی ۴۸۸۶، (د) تصویر نهان‌نگاری شده با جاسازی ۱۱۰۷۴ بیت

978-1-4799-4910-6/14 $31.00 © 2014 IEEE
DOI 10.1109/ACCT.2014.72

TABLE I. PSNR OF STEGO-IMAGES WITH DIFFERENT EMBEDDING CAPACITY

Bits embedded in *Lena* image	2037	4302	4998	7167	8365	9912	11074	12929
PSNR (in dB)	41.000	40.939	40.931	40.910	40.879	40.835	40.822	40.795
Bits embedded in *Baboon* image	1400	2912	4886	6944	8022	9772	11074	12012
PSNR (in dB)	40.915	40.867	40.754	40.728	40.662	40.611	40.571	40.522

V. نتیجه گیری

در این مقاله، طرح وابستگی کلید تصویر نهان‌نگاری را بهبود بخشیدیم که بر اساس مکانیزم نهان‌نگاری تصادفی LSB و به کار گرفتن لبه یابی با نام Canny است. لبه یاب Canny برای تولید کیفیت بهتر تصویر نهان‌نگاری همیاری می‌کند. نتایج تجربی تایید می‌کند که طرح فوق در رسیدن به بارگذاری بالا و همچنین کیفیت خوب تصویر نهان‌نگاری موفق بوده است. محتوای پیام به در فرآیند استخراج به درستی برگردانده شده است. بعلاوه، به لطف نهان‌نگاری LSB تصادفی و رمزگذاری شده، این طرح در مقابل حملات قابل اطمینان است و پیام بدون دانستن کلید قابل بازگشایی نیست.

VI. منابع

[1] W. J. Chen, C. C. Chang, and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, vol. 37, no. 4, pp 3292-3301, 2010.

[2] Z. Nanning, "Computer visualization and pattern recognition", National Defense Industry Press, vol. 2, pp. 1069–1074, 1998.

[3] K. Wang, Z. M. Lu, and Y. J. Hu, "A high capacity lossless data hiding scheme for JPEG images", The Journal of Systems and Software, vol. 86, no. 7, pp. 1965-1975, 2013.

[4] Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

[5] L. Hostalot, and D. Megıas, "LSB matching steganalysis based on patterns of pixel differences and random embedding", Computers & Security, vol. 32, pp. 192-206, 2013.

[6] Kanso, and H. S. Own, "Steganographic algorithm based on chaotic map", Communication in Nonlinear Science and Numerical Simulations, vol. 17, no. 8, pp. 3287-3302, 2012.

[7] N. H. A. Mahdi, A. Yahya R. B. Ahmad, and O. M. Al-Qershib, "Secured and robust information hiding scheme", Procedia Engineering, vol. 53, pp. 463-471, 2013.

[8] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure and high capacity image steganography technique", Signal and Image Processing: An International Journal, vol. 4, no.1, 2013.

[9] Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 2073-4212, 2011.

[10] R. M. May, "Simple mathematical model with very complicated dynamics", Nature, vol. 261, pp. 459–467, 1967.

978-1-4799-4910-6/14 $31.00 © 2014 IEEE
DOI 10.1109/ACCT.2014.72