ارزیابی و سنجش متریکهای پنهان نگاری

عرفانه نوروزی[۱]
۱- دانشکده مهندسی کامپیوتر، واحد سپیدان، دانشگاه آزاد اسلامی، سپیدان، ایران

چکیده:

هدف پنهان نگاری ، پنهان کردن اطلاعات واضح درون اطلاعات دقیق دیگری است تا از نفوذ افراد بیگانه برای تشخیص پیغام محرمانه جلوگیری کند. پنهان نگاری یک هنر قدیمی است که در سالهای اخیر مجددا مورد توجه قرار گرفته است.خلاصه مقاله به شرح زیر است:

در ابتدا نگاهی کلی به پنهان نگاری و علاوه بر آن مشاهده آثار و نوشته هایی از پنهان نگاری در ویدئو بطور خلاصه گفته شده است و در کل متریکهای پنهان نگاری توضیح داده می شود.

کلمات کلیدی: پنهان نگاری در ویدئو، متریکهای پنهان نگاری

۱. مقدمه

همواره ، پیشرفت در بررسی جهان و صنایع در مسیر اجرای مخفی سازی اطلاعات بطور هم زمان در مقابل حوزه های رمز نویسی معمول وجود داشته است.کلمه پنهان نگاری مشتق شده از ریشه یونانی است که از نوشتن محافظت می کند و معمولا در جهت علامت گذاری اطلاعات مخفی در اطلاعات مرتبط دیگر است.تفسیر پنهان نگاری به دلیل هنر و دانش تطبیق به گونه ای است که محتوا را درون متن و زمینه پنهان نگاری مخفی نگه می دارد. تعداد اصطلاحات افزایشیافته و صفتها در اطلاعات تعریف و ثابت نگه داشته شده است. واژه پوشش (جلد) در جهت توضیح خلاقیت در پیام دقیق، اطلاعات شنیداری، دیداری و غیره استفاده شده است. به هنگام رجوع به علائم پنهان نگاری شنیداری، علائم پوششی اغلب علائم میزبان نامیده می شود. اطلاعات مخفی درون اطلاعات پوششی به عنوان داده های ثابت شناخته می شود. داده های stego شامل هر دو نوع اطلاعات پوششی و ثابت می باشد. بطور کلی شیوه قراردادن سد ثابت یا مخفی در پوشش اطلاعات به عنوان تثبیت کردن داده تعریف می شود. خصوصا هنگام رجوع به پنهان نگاری ویدئویی ، پوشش تصویری یک کانتینر نامیده می شود.

۲. پنهان نگاری در ویدئو

تکنیک مخفی کردن داده ای که از ویدیو ناشی شده است به روشهای مختلفی مورد استفاده قرار می گیرد. در این روش بطور تصادفی رشته کاغذی که تفاوت عمده ای را شامل می شود، تهیه می کنند.توالی پنهان نگاری بطور دقیق در مقدار منسجمی به همراه کدهایی واضح ایجاد شده و ترجمه انتقالی به منظور ایجاد یک فرایند ترکیبی صورت می پذیرد. بطور کلی جایگاه پنهان نگاری بالاتر از هدایت و کنترل زمینه و متن ویدئو می باشد. در کنار رمز گشایی ، پنهان نگاری مشابه بوجود آمده است و ذرات ثابت با استفاده از شیوه ارتباطی ، رمزگشایی می شود.بر اساس سازمان مخفی اطلاعات ویدئویی، اندازه گیری بر پایه این شیوه، این توانایی را بوجود می آورد که در مقابل طیف گسترده ای که رو به جلو در حرکت است قرار گیرد. شماری از تکنیکهای قابل دسترس که در ارتباط با ویدئو است بر اساس اطلاعات مخفی، درون شاخص تعدیل مقدار قرار می گیرد.(QIM) متداولترین شیوه در اینگونه تکنیکها استفاده از شاخص تعدیل مقدار باشد که ضرایبشان متغیر است. فایده استفاده از سیستمهای طیف گسترده آن است که در برابر حملات تصاعدی مستحکمتر است. ولی اندازه گیری بر اساس تکنیکها معمولا ظرفیت و قدرت تخریبی بیشتری دارد. در رابطه با حوزه میزبان، اطلاعات مخفی شده توالی درون دو نقطه از پایگاه اطلاعاتی کامل می شود. تحت فشار، زوائی اضافی در سطح جریان شکسته می گردد. اغلب رمز گشاها تغییر متناوبی برای مدت زمان رمز گذاری دارند و این آزادی انتخاب در جهت تغییر هدف مخفی کردن اطلاعات مناسب است. از سوی دیگر این تکنیکها وابسته به جریان ذره است. بنابراین اینگونه روش مخفی کردن معمولا برای شکست آسان تر ، اختیاری است. در مقابل این شیوه ها، سطح داده در برابر حملات به شدت مقاوم هستند.بنابراین آنها برای دامنه وسیعی از کار مناسب می باشند. از این رو ، کاربردهای مخفی کردن اطلاعات از جریان ذره بر پایه این تکنیکها استفاده می شود. قابل توجه است که بیشتر روشهای مخفی کردن اطلاعات در ویدئوی دیجیتالی، بکارگیری داده های ویدئویی غیرفشرده است. sarkar madhow موج برانگیخته ای را برنامه ریزی کرد که قلمرو و حوزه اطلاعات مخفی شده در ویدئو ها را ایجاد می کرد.این محقق از شاخص تغییر مقدار در جهت انتقال جریانی ناپیوسته استفاده کرد.(DCT) ضرایب و متغییر های اندازه گیری از پارامترهای MPEG2 مشتق می شود. به علاوه محققین تثبیت خاصی را بسته به نوع ظرف بکار می برند. برطبق ثبات و گستردگی، شیوه جایگزینی در سطح رمزگشا و پایه نامتقارن تغییر می کند. محققین از جمع آوری کدهای تکراری استفاده می کنند تا در برابر جریان مقاومت نمایند. جمع آوی کدهای تکراری در مخفی نمودن اطلاعات ویدئویی بکار می رود. در یک توالی متناسب، تنوع در نامتقارن بودن قرار می گیرد و محقق از جمع آوری کدهای تکراری استفاده می کند تا گستردگی را کنترل کند. خروج و یا تثبیت میتواند در امتداد کدهای پیچیده کنترل شود. محققین کدهای پیچیده را در بخش ثابت استفاده می کنند و لی وابستگی بر روی رمز گشا قرار می گیرد. بیشتر رمزگشاهای موازی در جهت اصلاح معایب نامتقارن استفاده می شوند. در سال 2005 از حوزه انتقال موج ناپیوسته سه بعدی استفاده شد تا اطلاعات را مخفی کند.این محقق از هیچ انتخاب متناوبی استفاده نکرد. در نتیجه از کدهای صحیح- غلط در جهت استحکام گزینه استفاده نکرد. بطور غیرمعمول از کد (BCH) در جهت افزایش ظرفیت تغییر خطا استفاده نمود. محققین خروج سه بعدی را در جهت حذف گسستگی خطاها انجام دادند. بعلاوه انتخاب این محقق، یک روش متقارن موقتی به منظور کنترل حملات موقتی بود. تصویر ثابت و داده های ویدئویی مخفی، نقاط بیشماری را تقسیم کردند. از طرفی دیگر داده های مخفی ویدئویی طرح های چند منظوره بیشتری را لازم داشت. بنابراین اطلاعات ویدئویی با مخفی شدن به تراکم و موضوع فعال تحقیق ادامه دادند.در یک رومان کوتاه، بحث ثبات تغییر در جهت مخفی کردن اطلاعاتی استفاده می شود که از منطقه ممنوعه استفاده می کند و جمع آوری کدهای تکراری با مکانیسم توالی متقارن مکمل در تطابق است. اطلاعات مخفی منطقه ممنوعه برای فرایندی مفید است که بالاترین شاخص تغییر تعدیل استفاده شود. جمع آوری کدهای تکراری پیش از این در پنهان نگاری ویدئو از زمان مقاومتشان در مقابل محو شدگی برای اطلاعات مخفی استفاده می شده است. استحکام و مقاومت ، کنترل روند نامتقارن بین رمز گشا ورمز را که به عنوان محصول تفاوت در ضرایب انتخابی ست، آسان تر می کند. محقق از یک جمع سیستماتیک کدهای تکراری استفاده می کند تا ذرات و چارچوب پیغام را ثابت نگه دارد. هر ذره به تنهایی با کل مجموعه مرتبط است.

۳. متریکهای پنهان نگاری

در این قسمت بر روی امنیت سازمان پنهان نگاری تمرکز می کنیم و اینکه چطور محققین ارزش پوشش چند منظوره را پس از تثبیت پیغام امن، اندازه گیری می کنند.در این مقاله چندین محقق وجود دارد که هدف همگی تمرکز بر روی پنهان نگاری یعنی جلوگیری از شک در مورد وجود داده های مخفی است.این محققین از مقداری پنهان نگاری تصویری که موضوع آزمایش توسط SNR و بسیاری دیگر است ، استفاده می کنند. قبل از نمایش تحقیق بر روی متریکهای پنهان نگاری، محقق بایستی نشان دهد که چگونه اندازه شی پنهان نگاری شده، اندازه گیری می شود. بیشترین اندازه گیری های استفاده شده امواج سیگنال- صدا(SNR)، اوج امواج سیکنال-صدا (PSNR)، خطاهای مرکزی و خطاهای ریشه (RMSE) می باشد. این نمودار قادر است بگوید که آیا تصویر ظاهر شده است یا نه؟ آیا نور مستقیم بوده یا خیر؟ چه تطابقی بهتر عمل میکند؟ آیا هیچ تغییری در رنگها وجود دارد یا خیر؟این نمودار از طریق آزمایش تکرار هر رنگ در تصویر ایجاد شده، جائیکه هر پیکسل در تصویر دارای یک رنگ است که از طریق ترکیب رنگهای اصلی قرمز، سبز و آبی تولید شده است.هر یک ازاین رنگها می تواند درجه روشنایی خاص خود را از ۰ تا ۲۵۵ را داشته باشد. برای یک تصویر دیجیتالی با عمق ۸ ذره، امواج سیگنال-صدا به منظور اندازه گیری مقدار سیگنال پیچیده شده در یک صدا استفاده می شود و بر روی وزن در مقابل سطح سیگنال کار می کند. بالاترین موج SNR ، کمترین زمینه صدا را نشان می دهد. پس از دریافت سطح صدا در هر تصویر، SNR برخلاف سطح صدا در هر دو تصویر موجود است و تفاوت بین دو تصویر را نشان میدهد تا کیفیت تصویر به عنوان نتیجه اطلاعات تثبیت شده شناسایی شود.

$$SNR= 10* Log10\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(Aij)}{\sum_{i=1}^{n}\sum_{j=1}^{m}(Aij-Bij)}$$

مکان Aij یک پیکسل را درون تصویر اصلی (قبل از تثبیت داده مخفی)نشان می دهد و مکان Bij یک پیکسل را درون تصویر (بعد از ثبات داده مخفی) نشان میدهد.نتیجه نهایی بوسیله مقداری ثابت و واحد اندازه گیری دسی بل نشان داده خواهد شد. محدوده خطا ، افزایش میدان خطا را بین تصویر اصلی و تصویر فرعی نشان می دهد. پایین ترین مقدار خطا به معنای کمترین خطا بین دو تصویر است. اندازه گیری برای اهداف پنهان نگاری بدین طریق نشان داده می شود.

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}(Aij - Bij^2)\,(Aij^2)$$

مکان Aij یک پیکسل را درون تصویر اصلی (قبل از تثبیت داده مخفی)نشان می دهد و مکان Bij یک پیکسل را درون تصویر (بعد از ثبات داده مخفی) نشان میدهد و (m*n) ارتفاع و عرض تصویر را نشان می دهد. نتیجه نهایی بوسیله مقداری ثابت و با واحد اندازه گیری دسی بل نشان داده خواهد شد. اوج مقدار سیگنال- صدا (PSNR) متریکی است که از محاسبه اوج امواج سیگنال-صدا بین دو تصویر در مقیاس دسی بل حاصل می شود. این امواج اغلب به منظور واحد اندازه گیری بین تصویر فرعی و تصویر اصلی مورد استفاده قرار می گیرد. هرچه PSNR بالاتر باشد اندازه گیری درون تصویر فرعی پس از انکه داده های مخفی تثبیت شد، بهتر خواهد بود.

$$PSNR= 10* Log10\frac{(max^2)}{\frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}(Aij-Bij^2)(Aij^2)}$$

مکان Aij یک پیکسل را درون تصویر اصلی (قبل از تثبیت داده مخفی)نشان می دهد و مکان Bij یک پیکسل را درون تصویر (بعد از ثبات داده مخفی) نشان میدهد و (m*n) ارتفاع و عرض تصویر را نشان می دهد و Max حداکثر مقدار رنگ را نشان میدهد.(۲۵۵)و یا در روشی دیگر نمایش PSNR بدین طرق است:

$$PSNR= 10*\log10\frac{(max^2)}{MSE}$$

MSE خطای مربع را نشان میدهد و Max حداکثر مقدار رنگ را که ۲۵۵ است نمایان می سازد. اثرPSNR در امتداد محتوا با واحد اندازه گیری دسی بل نشان داده می شود. بازگشایی خطای مربع و اوج امواج سیگنال – صدا هم اکنون برای ویدئو و تصویر جامعه بخاطر این متریک قابل اطمینان، مورد استفاده قرار می گیرد. (PSNR نمایش لوگاریتمی MSE است هنگامیکه RMSE ریشه مربع را نشان می دهد).

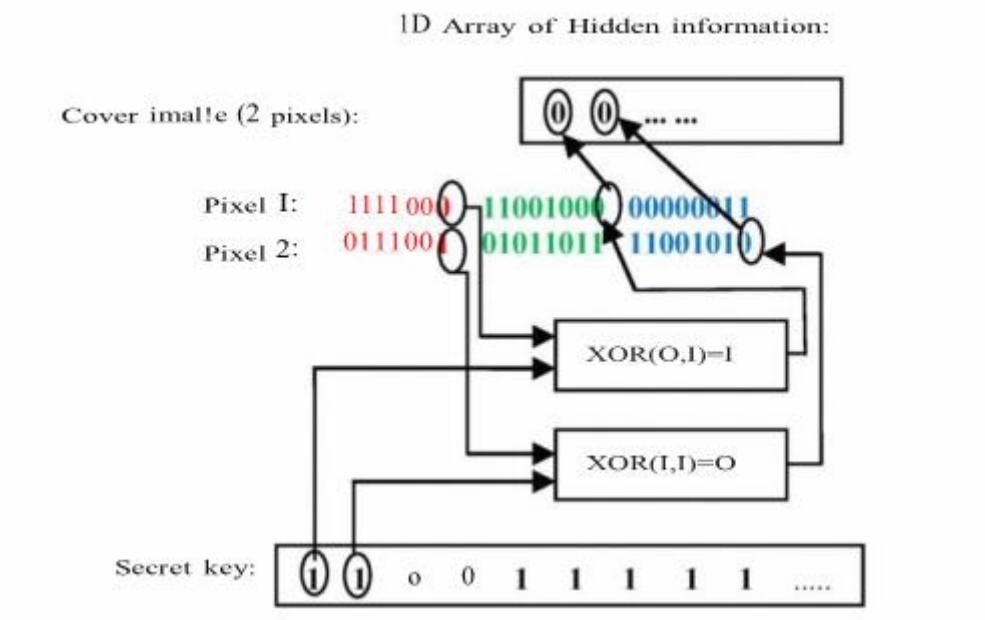
محاسبه این متریکها در مقایسه با درک و اجرای دیگر متریکها ، آسان و سریع می باشد. اینها دلایلی است که باعث شده این متریکها عمومیت یابند. در محدوده روند تصویری، خطای اصلی مرکز ریشه(RMSE)از میانگین مربع در ریشه مربع که در هر پیکسل درون تصویر پیچیده شده و شباهت عنصری در تصویر دیجیتال قابل تشخیص است.

$$PSNR = \frac{1}{m*n}\sum_{i=1}^{n}\sum_{j=1}^{m}(Aij - Bij^2)10*\log10\frac{(max^2)}{}$$

مکان Aij یک پیکسل را درون تصویر اصلی و مکان Bij یک پیکسل را درون تصویر فرعی نشان میدهد و (m*n) ارتفاع و عرض تصویر را نشان می دهد. نتیجه نهایی PMSEبا واحد دسی بل اندازه گیری می شود. در سال 2008 محققین از مقدار ۵۱۲۱۹ بایت از تصویر را جهت مخفی نمودن اطلاعات استفاده کردند . مقدار PSNR برای این تحقیق ۴۱,۱ دسی بل است. از سوی دیگر در سال ۲۰۰۲ چانگ، مقدار ۵۳۲۴۸ بایت از تصویر را جهت مخفی نمودن اطلاعات استفاده نمود. مقدار PSNR در این روش ۳۴,۸۴ دسی بل است. بعد از آن چانگ و تسینگ این مقدار را تا ۳۸۹۰۰۴ بایت افزایش داده ومقدار PSNR تنها ۴۱,۲۲ دسی بل بود. RMSE قبلا به عنوان متریکی برای اندازه گیری مقدار شکستگی تصویر پیرو تثبیت و حفاظت متن مورد استفاده قرار می گرفته است. مقدار RMSE به منظور اندازه گیری میزان بهره وری روشهای پیشنهادی مورد استفاده قرار گرفته شده و مشخص گردیده که با مخفی نمودن مقدار ۵۰۹۶۰ بایت، مقدار RMSE ۲,۰۷ دسی بل خواهد بود. محققین از SNR به منظور سنجش مقالاتشان استفاده کردند انجا که SNR رشد پیشنهادی را در سندشان محاسبه کرد و مقدار ۱۸,۱۴۷۶ دسی بل را برای پنهان نگاری تصویر پس از تثبیت اطلاعات حاصل گردید. در سال ۲۰۰۷ محقق وانگ، از یک تصویر به اندازه ۵۱۲*۵۱۲ و ۲۵۶ سطح خاکستری برای مخفی کردن اطلاعات بوسیله تغییر روش افزایش معمول LSB استفاده کرد و اندازه گیری های سطح تحریف شده را با استفاده از متریک MSE برای همان تصویر محاسبه نمود. محققین ادعا کردند که LSBبدست آمده، مقدار ۲۱۶۸,۶ دسی بل MSE دارد در حالیکه در روش افزایش معمول LSB این مقدار ۵۲۱۹,۴ دسی بل می باشد.در متریکهای بالا، سطح تحریف شده برای تصویر کلی قابل قبول است اما بدون اندازه دقیق از پیکسلهای تصویر که بر دیگر پیکسلها اثر می گذارد. در جدول پایین خلاصه ای از شمار مقالات آورده شده است.

جدول ۱- نتایج تجربی برای روشهای ارائه شده

Author	Image	PSNR	SNR	RMSE
C.M. Wang, et al., (2008)	51,219bytes	4l.ldB	.....	.....
C. C. Chang, S.Chen, & Chung, (2002)	53,248bits	34.84dB	.....	.....
C.-C. Chang & Tseng, (2004)	389,004 bits	4l.22dB	.....	.....
Wu & Tsai, (2003)	50,960 bits	.....	.....	2.07 dB
Satish, Jayakar, Tobin, Madhavi, & Murali, (2004)	64 KB	.....	18.1476 dB	.....



شکل ۱ – تبدیل اطلاعات پنهان در هر پیکسل

آرایه IO از جریان کمی کلید های مخفی و ماتریس رنگ قرمز تنها برای تصمیم گیری به جای اطلاعات پنهان که هم از ماتریس سبز یا ماتریس آبی استفاده می شود. هر بیت از کلید های مخفی XOR با هر LSB ماتریس قرمز است.

همین روند ادامه می یابد تا زمانی که این اطلاعات پنهان را به پایان رساند. نمودار جریان برای مخفی کردن اطلاعات پنهان به تصویر پوشش در شکل ۴ نشان داده شده است.

(a)Lena

(b) Baboon

(c) Peppers

۰ ۰ ۱۹۳ ۲۴۸ ۲۴۸ ۲۵۲

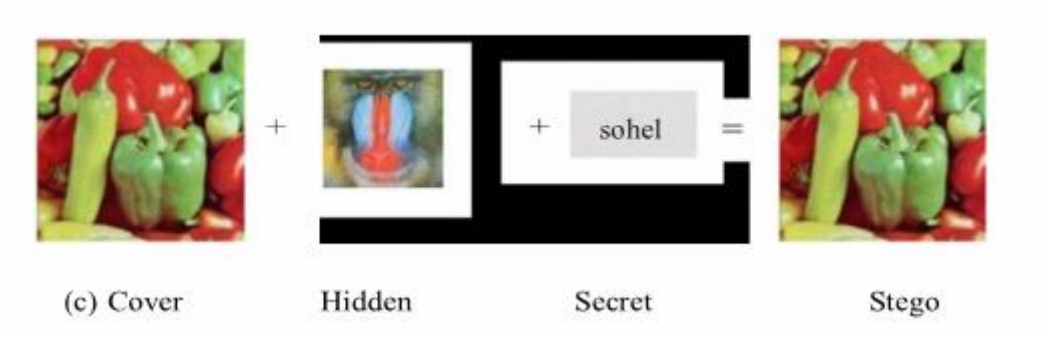
۲۴۸ ۲۴۸ ۲۴۶ ۱۱۳

(a) Cover Hidden Secret Stego

۲۵۱ ۲۵۰ ۱۱۳ ۱۸۶

(b) Cover Hidden Secret Stego

۱۲۴ ۱۸۸ ۲۴۸ ۲۴۶



۰ ۰ ۰ ۰ ۰ ۰ ۱۴۶ ۲۵۵ ۲۴۸ ۱۲۰

شکل ۲ – RGB نمایش از یک تصویرهای پوشش استاندارد

جریان کمی ID از اطلاعات مخفی که ۳ ID نمایندگی آرایه ای از پنهان شمارنده = ۰و R = دریافت LSB قرمز (تصویر پوشش)و KCV = K بیت مخفی. در شکل ۲، LSB ماتریس قرمز رنگ پیکسل است و اولین بیت از کلید های مخفی ارزش XOR از O است، اگر ارزش XOR و سپس LSB ماتریس سبز جایگزین توسط اولین بیت از اطلاعات پنهان است. اگر مقدار XOR O است و سپس LSB ماتریس قرمز است اولین بیت از اطلاعات مخفی جایگزین شده است که آرایه IO از کلید های مخفی دایره ای است. این فرایند تعویض بسته خواهد شد به طول اطلاعات مخفی که ۱۰ آرایه دارد.

Pixell: 1111100
پیکسل ۲: ۰۰۱۱۱۰۰
کلید های مخفی: ۰ ۰

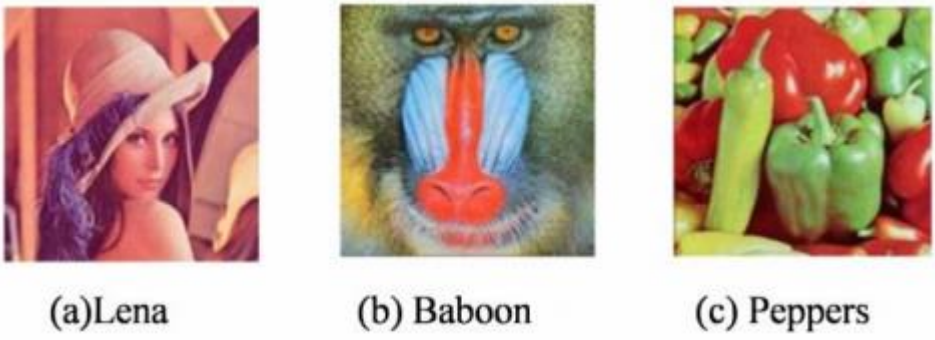
به بازیابی اطلاعات پنهان، از یک تصویر stego. این تصویر stego به سه ماتریس (قرمز، سبز و آبی) همانطور که در شکل نشان داده شده است تقسیم شده است. سپس ما باید بدانیم که کلید های مخفی به IO جریان کمی آرایه تبدیل شده است. هر بیت از کلید های مخفی XOR با هر LSB قرمز ماتریس تصویر stego است.

در نتیجه ارزش XOR تصمیم می گیرد که از اطلاعات مخفی بیتی است در هر دو LSB ماتریس سبز یا ماتریس آبی از تصویر stego ذخیره می شود. طول این اطلاعات پنهان است در سطر اول از تصویر stego در طول فرایند مخفی ذخیره می شود. روند بهبودی بسته خواهد شد به طول پنهان جریان کمی اطلاعات، نمودار جریان برای بازیابی اطلاعات پنهان از stego تصویر نشان داده شده است.

در شکل ۲، LSB ماتریس پیکسل قرمز است و اولین بیت از کلید های مخفی I. ارزش XOR از O است در روش پیشنهادی ما، ارزش XOR پس از آن می توان در یافت LSB ماتریس سبزپنهان نمود اگر مقدار XOR O است و سپس پنهان را می توان در LSB ماتریس آبی یافت. این بیت را برداشت ومقدارذخیره شده را به یک آرایه ID نسبت داد. در نهایت آرایه IO به ۲۰ آرایه را تغییر به شکل اطلاعات واقعی قابل پنهان است. این فرایند برای بازیابی اطلاعات پنهان از stego تصویر است

سه RGB (رنگ واقعی) تصاویر استاندارد، به نام لنا، بابون و فلفل به عنوان عکس روی جلد استفاده می شود. این تصاویر در شکل ۲ نشان داده شده که اطلاعات پنهان استفاده شده برای مخفی کردن در داده وارد شده. اطلاعات مخفی به تصویر پوشش با کلید های مخفی وارد می شود. تصویر حاصل است تصویر stego نامیده می شود. روش به دست آوردن تصویر stego از تصویر پوشش در شکل ۲ نشان داده شده است. این تصاویر stego، به نام لنا، بابون و فلفل در شکل ۳ نشان داده شده است. تحریف را در تصاویر stego به دلیل تعبیه مقدار زیادی از پیام های مخفی با استفاده از روش پیشنهادی ما نامعلوم به چشم انسان می باشد. عکس روی جلد مورد استفاده در روش پیشنهادی ما در شکل ۳ نشان داده شده است.

تصاویر stego حاصل از روش پیشنهادی ما در شکل زیر نشان داده شده است.



شکل ۳ – RGB نمایش از تصویرهای پوشش لنا بابون فلفل

با استفاده از معادله و ارزش (PSNR)، محاسبه stego تصویر. این مقادیر PSNR در جدول ۲ نمایش داده شده است.

جدول ۲- نتایج و مقادیر PSNR برای عکس های استاندارد

Images	PSNR (in dB)
Lena	53.7618
Baboon	53.7558
Peppers	53.7869

۴. نتیجـــه

در این مقاله، امکان تشخیص متریک های پنهان نگاری برای طراحی نموداری از این متریکها، مورد بررسی قرار گرفت. این بررسی بر متریکهای اصلی تمرکز کرده درحالیکه متریکهای بیشمار دیگری نیز وجود دارند، اما برای آزمایش بطور قابل استفاده گسترده نیستند. این مجموعه، در طول سالها دانش صنعتی در مورد PSNR دارد که به آنها این اجازه را میدهد تا اصول مورد نیاز را تحلیل و بررسی کند. اما استفاده از این متریکها هنوز بهترین نوع اندازه گیری برای اصطلاحات پنهان نگاری نمی باشد. متریکهای پنهان نگاری در مقالات بیشماری به منظور اندازه گیری مقدار پنهان نگاری تصویر مورد استفاده قرار گرفته است. محققین از این متریکها استفاده کردند تا مطمین شوند که روشهای پیشنهادی، هدف پنهان نگاری را از طریق جلوگیری از دستیابی به پیام های مخفی، حاصل نموده است. همانطور که قبلا گفته شد که چطور متریکهای پنهان نگاری کار می کنند، محققین شیوه های پیشنهادی شان را بوسیله مقایسه پیکسل های تصویر پنهان نگاری شده با پیکسل های تصویر اصلی اندازه گیری میکنند. این امر از طریق مقایسه پیکسل های تصویر اصلی و سپس بکار گیری عملی معادله متریکها، انجام پذیر است.

مراجع

[1] Bai, L., Zhang, Y., & Yang, G. (2012, April). SM2 cryptographic algorithm based on discrete logarithm problem and prospect. In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on (pp. 1294-1297). IEEE.

[2] Bellare, K., Druck, G., & McCallum, A. (2009, June). Alternating projections for learning with expectation constraints. In Proceedings of the Twenty-Fifth Conference on Uncertainty in Artificial Intelligence (pp. 43-50). AUAI Press.

[3] Camenisch, J., & Groß, T. (2012). Efficient Attributes for Anonymous Credentials. ACM Transactions on Information and System Security (TISSEC), 15(1), 4.

[4] Cao, F., & Cao, Z. (2009). A secure identity-based proxy multi-signature scheme. Information Sciences, 179(3), 292-302.

[5] Chang, C. C., & Lin, C. J. (2011). LIBSVM: a library for support vector machines. ACM Transactions on Intelligent Systems and Technology (TIST), 2(3), 27.

[6] Desmedt, Y., Pieprzyk, J., Steinfeld, R., Sun, X., Tartary, C., Wang, H., & Yao, A. C. C. (2012). Graph coloring applied to secure computation in non-Abelian groups| Macquarie University ResearchOnline.

[7] Ding, J., Yang, B. Y., Chen, C. H., Chen, M. S., & Cheng, C. M. (2008). New differential-algebraic attacks and reparametrization of rainbow. In Applied Cryptography and Network Security (pp. 242-257). Springer Berlin/Heidelberg.

[8] Duffy, D. G., Goodwin, C. C., Johnes, A. W., & Binks, D. F. J. (2010). U.S. Patent Application 12/896,101.

[9] Elkamchouchi, H., Elshenawy, K., & Shaban, H. (2002, November). Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In Communication Systems, 2002. ICCS 2002. The 8th International Conference on (Vol. 1, pp. 91-95). IEEE.

[10] Goljan, M., Fridrich, J., & Filler, T. (2009). Large scale test of sensor fingerprint camera identification. Proc. SPIE, Electronic Imaging, Security and Forensics of Multimedia Contents XI, San Jose, CA.

[11] Huang, C. C., & Lo, C. C. (2010, January). Threshold based group-oriented nominative proxy signature scheme for digital rights management. In Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE (pp. 1-5). IEEE.

[12] Jansirani, A., Rajesh, R., Balasubramanian, R., & Eswaran, P. (2011). Hi-tech authentication for palette images using digital signature and data hiding. The International Arab Journal of Information Technology, 8(2), 117-123.

[13] Keromytis, A. (2010). X. 509 Key and Signature Encoding for the KeyNote Trust Management System.

[14] Kirsch, S. T. (2012), U.S. Patent No. 20,120,323,717. Washington, DC: U.S. Patent and Trademark Office.

[15] Naji, A. W., Hameed, S. A., Zaidan, B. B., Al-Khateeb, W. F., Khalifa, O. O., Zaidan, A. A., & Gunawan, T. S. (2009). Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advanced Encryption Standard and Distortion Techniques. arXiv preprint arXiv:0908.0216.

[16] R. Rivest, A. Shamir, L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21, no. 2, pp. 120-126, May 1978.

[17] Reddy, M. I., Bhat, P. J., Chetwavani, R., & Reddy, M. P. (2011). Establishment of Public Key Infrastructure for Digital Signatures. Computer Engineering and Intelligent Systems, 2(6), 33-43.

[18] Schuldt, J. C., & Matsuura, K. (2011). Efficient convertible undeniable signatures with delegatable verification. IEICE transactions on fundamentals of electronics, communications and computer sciences, 94(1), 71-83.

[19] Serret-Avila, X., & Boccon-Gibod, G. (2012). U.S. Patent No. 8,099,601. Washington, DC: U.S. Patent and Trademark Office.

[20] Shah, V., Rao, N. N., Agrawal, A., Sarkar, S., Subramanian, K., & Shukla, H. (2010). U.S. Patent No. 7,694,009. Washington, DC: U.S. Patent and Trademark Office.