استگانوگرافی تصویر بر اساس پیام تکمیل شده و جایگزینی LSB بیت معکوس

خلاصه

استگانوگرافی هنر رمزگذاری/جاسازی اطلاعات محرمانه در رسانه های پوششی به گونه ای است که سوء ظن استراق سمع را برانگیزد. هدف اصلی این مقاله ارائه سه سطح امنیت است، اول با تکمیل پیام مخفی، دوم با پنهان کردن پیام مخفی تکمیل شده در پیکسل های تصویر جلد که به طور تصادفی با استفاده از مولد اعداد تصادفی شبه انتخاب می شوند، سوم با استفاده از بیت معکوس LSB ارائه می شود. روش ۲ به عنوان تکنیک استگنوگرافیک به جای LSB ساده، احتمال شناسایی پیام پنهان را کاهش می دهد. MSE (میانگین مربع خطا) و PSNR (نسبت پیک سیگنال به نویز) دو اندازه گیری کیفیت رایج هستند.

برای اندازه گیری تفاوت بین تصویر جلد و تصویر استگو. نتایج نشان داد که روش پیشنهادی نتایج بهتری نسبت به LSB ساده و LSB معکوس با PSNR بالاتر و MSE کمتر دارد.

۱. معرفی

با پیشرفت سریع فناوری‌های چندرسانه‌ای در سال‌های اخیر، ارتباطات و تبادل اطلاعات بسیار آسان‌تر و سریع‌تر شده است، اما در عین حال مسائل مربوط به امنیت و محرمانگی داده‌ها به یکی از دغدغه‌های اصلی عصر امروز تبدیل شده است. برای رفع این نیاز به امنیت اطلاعات، تعدادی از تکنیک های ارتباطی پنهان و مخفی توسعه داده شده است. استگانوگرافی به هنر ارتباطات پنهان اشاره دارد، کدگذاری/جاسازی اطلاعات محرمانه در رسانه های پوششی به گونه ای که برای یک فرد غیرمجاز کار دشواری است که ببیند چیزی در رسانه پوشش پنهان است. خروجی تصویری به نام stego-image است که شبیه به رسانه پوشش است. سپس این تصویر استگو به گیرنده ارسال می‌شود، جایی که گیرنده با اجرای فرآیند استگانوگرافی، پیام پنهان را بازیابی می‌کند. یک stego-key برای فرآیند تعبیه یا رمزگذاری برای محدود کردن رمزگشایی یا استخراج داده های تعبیه شده در رسانه پوشش استفاده می شود.

استگانوگرافی عصر مدرن معمولاً به صورت محاسباتی پیاده سازی می شود، جایی که فایل های چند رسانه ای به عنوان رسانه پوشش استفاده می شوند. یک روش Steganographic خوب دارای سه ویژگی است، ظرفیت پنهان خوب، نامحسوس بودن خوب و آخرین ویژگی استحکام است.

در این مقاله از سه سطح امنیتی برای ایمن سازی اطلاعات تعبیه شده و افزودن پیچیدگی بیشتر برای استگانالیز استفاده شده است. این یک فرآیند سه مرحله‌ای است، به‌جای جاسازی بیت‌های پیام به طور مستقیم در تصویر جلد، پیکسل‌ها به‌طور تصادفی از طریق مولد اعداد تصادفی شبه تولید می‌شوند و پس از آن داده‌های مخفی تکمیل‌شده با استفاده از روش LSB بیت معکوس در تصویر جلد جاسازی می‌شوند. در بخش ۲ بررسی ادبیات ارائه شده است. پس از یک بحث مختصر در مورد LSB و بیت معکوس LSB در بخش ۳، بخش ۴ روش پیشنهادی را شرح می دهد. بخش ۵ آزمایش ها و نتایج را نشان می دهد. بخش ۶ مقاله را به پایان می رساند.

۲. بررسی ادبیات

استگانوگرافی به دو حوزه فضایی و حوزه تبدیل طبقه بندی می شود. این مقاله با بررسی ادبیات خود بر فناوری‌های حوزه فضایی تأکید می‌کند که در آن دو روش مبتنی بر LSB و مبتنی بر EDGE مورد بحث قرار می‌گیرند.

در LSB، LSBهای تصویر جلد تحت تأثیر قرار می گیرند. در تطبیق LSB، در صورتی که پیام مخفی مشابه نباشد، تغییرات کمتری برای پیکسل های تصویر پوششی با افزودن یا کم کردن یکی از پیکسل های پوششی انجام می شود، اما تعبیه LSB را می توان با حملات steganalysis تجزیه و تحلیل کرد. Jarno et. al. LSBMR را پیشنهاد می‌کند، از دو پیکسل برای جاسازی بیت‌های اطلاعات مخفی استفاده می‌کند، یک بیت در LSB اول و تابعی از دو پیکسل برای حمل بیت دیگری از اطلاعات استفاده می‌شود.

این تکنیک پیام را به طور یکنواخت پخش می کند و بنابراین سطح امنیتی خوبی را در مقایسه با LSBM ارائه می دهد.

روش های مبتنی بر EDGE از تفاوت پیکسل ها و پیکسل های نزدیک آنها استفاده می کنند. D. Wu et al.4، تکنیک آنها به ظرفیت زیادی برای جاسازی بیت های پیام کمک می کند، در حالی که تعداد آنها با تفاوت بین پیکسل و پیکسل نزدیک آن محاسبه می شود. این تکنیک در برابر تحلیل های آماری به خوبی عمل نمی کند. X. zhang و همکاران ۵ پیشنهاد می کنند که PVD به دلیل مراحل غیر معمول در هیستوگرام آن، در برابر استگانالیز آسیب پذیر هستند. یک تحلیلگر می تواند اندازه پیام تعبیه شده را تعیین کند.

بنابراین او یک طرح تغییر ارزش پیکسل را پیشنهاد می کند. لو و. al.6 بیان می کند که طرح های مبتنی بر لبه بهتر از رویکردهای مبتنی بر LSB نیستند.

۳. مقدمات

۳.۱. جایگزینی LSB بیت معکوس

ندیم اختر و. al. طرحی پیشنهاد شده است که در آن PSNR تصویر استگو افزایش یافته و همچنین امنیت با انتخاب تصادفی پیکسل ها حفظ می شود. در این تکنیک بیت های پیام به صورت تصادفی در پیکسل های تصویر جلد تعبیه می شوند و با توجه به ترکیب بیت ها در بیت های ۲ و ۳ شمارش می شود. پیکسل حفظ می شود. فرض کنید بیت دوم و سوم یک پیکسل ۰۱ باشد، بنابراین اگر LSB تصویر مطابقت داشته باشد، این شمارنده برای پیکسل تغییر نکرده، شمارنده افزایش می‌یابد، در غیر این صورت شمارنده برای بیت‌های تغییر یافته افزایش می‌یابد، برای همه ترکیب‌ها (۰۰، ۰۱، ۱۰، و ۱۱) به همین ترتیب انجام می‌شود. .

مثال: چهار بیت پیام ۱ ۰ ۰ ۰ باید در چهار پیکسل تصویر جلد پنهان شوند

10000100
00101101
11101101
11101111

پس از استگانوگرافی LSB ساده، پیکسل های تصویر استگو هستند

10000101
00101100
11101100
11101110

تعداد پیکسل های تغییر یافته چهار است. با توجه به الگوریتم، بیت دوم و سوم کمترین اهمیت تصویر استگو را بررسی کنید. برای مثال، اجازه دهید پیکسل دوم=۰ و پیکسل ۳=۱ باشد. حال اگر بیت دوم و سوم پیکسل با ترکیب مورد نیاز مطابقت داشته باشند، LSB را معکوس کنید، در غیر این صورت، این کار را انجام می دهد. به همین صورت باقی می‌ماند. بنابراین اگر این حالت را در مثال بالا اعمال کنیم، پیکسل‌های موجود در تصویر استگو به صورت زیر خواهند بود:

10000100
00101101
11101101
11101110

تعداد پیکسل های تغییر یافته یکی است، بنابراین با استفاده از این تکنیک، PSNR افزایش می یابد زیرا مزایای پیکسل وجود خواهد داشت. فرآیند مشابهی برای تمام ترکیبات بیت انجام خواهد شد. وارونگی بیت تنها در صورتی انجام می‌شود که تعداد بیت‌های تغییر یافته بیشتر از تعداد بیت‌های بدون تغییر باشد، بنابراین منجر به اعوجاج کمتر تصویر جلد و افزایش PSNR می‌شود.

۴. روش پیشنهادی

در این تکنیک از یک دانه تصادفی برای انتخاب تصادفی پیکسل ها استفاده می شود و بیت های پیام در کمترین بیت مهم این پیکسل انتخاب شده به طور تصادفی جاسازی می شود. در طرح داده شده همراه با پیام، بیت‌های p نیز تعبیه شده‌اند که معکوس بودن یا نبودن بیت‌ها را تعیین می‌کنند، در اینجا برای تعیین به ۴ بیت نیاز داریم. بیت های اول نشان دهنده ترکیب "۰۰" در صورت وارونه شدن نسبت به یکی دیگر هستند، بیت دوم نشان دهنده ترکیب "۰۱"، بیت سوم نشان دهنده ترکیب "۱۰" و بیت آخر نشان دهنده ترکیب "۱۱" است.

۴.۱ الگوریتم جاسازی داده ها

ورودی: تصویر جلد C با اندازه I x I، داده مخفی، M با اندازه J x J، p=4 بیت (در ابتدا همه صفر هستند).

خروجی: تصویر استگو، کلید

مرحله ۱: M را در صفحات LSB C قرار دهید تا تصویر استگو S را بدست آورید. روش جاسازی به صورت زیر ارائه شده است.

۱. بیت های پیام را تکمیل کنید.

۲. مجموعه ای از پیکسل های تصادفی را با استفاده از کلید مخفی ایجاد کنید

۳. برای i = 1 تا J

۴. برای j = 1 تا J

۵. k1=بیت دوم C(i,j) را دریافت کنید

۶. k2= بیت سوم C(i,j) را دریافت کنید

۷. m1=بیت اول C(i,j) را دریافت کنید

۸. بررسی k1 و k2 متعلق به کدام ترکیب است (۰۰,۰۱,۱۰,۱۱)

۹. اگر m1==M(i,j) سپس شمارنده مربوطه را برای LSB بدون تغییر افزایش دهید

۱۰. دیگری

۱۱. LSB تصویر جلد را به صورت m1 تنظیم کنید

۱۲. شمارنده مربوطه را برای LSB تغییر یافته افزایش دهید

۱۳. پایان؛ پایان؛ پایان

۱۴. اگر countCt00>countNc00 باشد، LSB تمام پیکسل های دارای بیت دوم و سوم را ۰۰ معکوس کنید.

۱۵. در غیر این صورت، اگر countCt10>countN10 داشته باشید، LSB همه پیکسل های دارای بیت دوم و سوم را به صورت ۰۱ معکوس کنید.

۱۶. در غیر این صورت، اگر countCt01>countNc01 باشد، LSB تمام پیکسل‌های دارای بیت دوم و سوم را برابر با ۱۰ معکوس کنید.

۱۷. در غیر این صورت اگر countCt11>countNc11 باشد، LSB تمام پیکسل های دارای بیت ۲ و ۳ را به صورت ۱۱ معکوس کنید.

۱۸. با توجه به مقادیر شمارنده تغییراتی را در بیت های p ایجاد کنید و در تصویر جاسازی کنید.

جایی که C (i j) ،S (i ،j)،M (i ،j)، به معنای مقدار پیکسل در موقعیت (j،i) در تصویر جلد، تصویر استگو و بیت‌های پیام است.

۴.۲ الگوریتم استخراج داده

استخراج پیام از تصویر استگو شامل مقایسه معکوس با آن چیزی است که در جاسازی استفاده می شود.

ورودی: Stego-Image، Key Matrix.

خروجی: داده های مخفی

مراحل مرحله استخراج به شرح زیر است:

۱. پیکسل تصادفی را با استفاده از کلید ایجاد کنید.

۲. بیت های p را استخراج کنید

۳. اگر بیت اول p 1 باشد، LSB تمام پیکسل های دارای بیت دوم و سوم را ۰۰ معکوس کنید.

۴. در غیر این صورت اگر بیت دوم p 1 باشد، LSB تمام پیکسل های دارای بیت ۲ و ۳ را ۰۱ معکوس کنید.

۵. در غیر این صورت اگر بیت سوم p 1 باشد، LSB تمام پیکسل های دارای بیت دوم و سوم را ۱۰ معکوس کنید.

۶. در غیر این صورت اگر بیت چهارم p برابر با ۱ باشد، LSB تمام پیکسل های دارای بیت دوم و سوم را به صورت ۱۱ معکوس کنید.

۷. برای i = 1 تا N

۸. برای j = 1 تا N

۹. اگر s(i,j)==حتی آنگاه M(i,j)=1

۱۰. در غیر این صورت M(i,j)=0

۱۱. پایان;پایان;پایان;

که در آن S(i,j)، به معنای مقدار پیکسل در موقعیت (i,j) در تصویر استگو و M (i,j) به معنای مقدار بیت های پیام در موقعیت (i,j) است.

۵. نتیجه و تجزیه و تحلیل

در این بخش، آزمایش‌هایی برای اثبات کارایی روش پیشنهادی انجام می‌شود که شبیه‌سازی بر روی Matlab 14 انجام می‌شود. مجموعه‌ای از تصویر ۸ بیتی در مقیاس خاکستری به اندازه ۵۱۲ × ۵۱۲ به عنوان تصویر جلد برای پنهان کردن تصویر باینری و خاکستری استفاده می‌شود. در اندازه ۱۲۸ × ۱۲۸ برای تشکیل تصویر استگو. با مطالعه تجربی، ما متوجه شدیم که تفاوت‌های بصری بین تصاویر جلد اصلی و تصاویر استگو با پیام تکمیل‌شده و تکنیک LSB معکوس به سختی با چشم غیر مسلح تشخیص داده می‌شود.

۵.۱ تجزیه و تحلیل PSNR

MSE (میانگین مربع خطا) و PSNR (نسبت پیک سیگنال به نویز) دو اندازه گیری کیفیت رایج برای اندازه گیری تفاوت بین تصویر پوششی و تصویر استگو هستند.
MSE میانگین اختلاف پیکسل به پیکسل مربع بین تصویر پوششی و تصویر استگو است.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [C(i,j) - S(i,j)]^2 \qquad (1)$$

که در آن، M و N به ترتیب ردیف‌ها و ستون‌های تصویر جلد هستند و C(i, j) و S(i, j) به معنای مقدار پیکسل در موقعیت (i, j) در تصویر جلد و استگو مربوطه است. -تصویر، به ترتیب.

PSNR در دسی بل بیان می شود و می توان آن را با استفاده از MSE محاسبه کرد

$$PSNR = 10\times\log\left(\frac{P^2}{MSE}\right) \quad (2)$$

که در آن، P مقدار سیگنال اوج تصویر پوشش و

$$P=\max\left(C(i,j),S(i,j)\right) \quad (3)$$

جدول ۲ (شکل ۲)، جدول ۳ (شکل ۳)، جدول ۴ (شکل ۴) و جدول ۵ (شکل ۵) مقادیر اندازه گیری شده MSE و PSNR انواع مختلف تصاویر پوششی با اندازه ۵۱۲×۵۱۲ را به ترتیب برای LSB ساده نشان می دهد. LSB تصادفی، LSB معکوس، LSB معکوس تکمیل شده. مشاهده می‌شود که وقتی بار محموله افزایش می‌یابد، MSE افزایش می‌یابد و این بر PSNR به طور معکوس تأثیر می‌گذارد و برای همه تصاویر پوششی PSNR بیشتر از ۵۰ است، این نشان‌دهنده عملکرد خوب سیستم پیشنهادی است. همانطور که در شکل ۲ مشاهده می شود، کاهش PSNR در مقایسه با افزایش اندازه پیام تعبیه شده بسیار ناچیز است و این نشان می دهد که کیفیت تصویر با افزایش اندازه پیام تقریبا ثابت می ماند. این بدان معنی است که تصاویر استگو ایجاد شده با سیستم پیشنهادی می توانند از حمله متداول پوشش پوششی جان سالم به در ببرند. جدول ۱ (شکل ۱) مقادیر اندازه گیری شده MSE و PSNR تصاویر جلد با اندازه ۵۱۲×۵۱۲ و اندازه پیام پنهان ۱۲۸×۱۲۸ را نشان می دهد. به ترتیب ۱۲۸. مشاهده می شود که مقدار PSNR روش پیشنهادی بهتر از سایر تکنیک ها است.

Cover Image	Message Image	Simple LSB		Random LSB		Invert LSB		Complemented Random Invert LSB	
Lena	Cameraman	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
512x512	4225 bits	59.6578	0.0649	59.6958	0.0644	59.7138	0.2494	59.7275	0.0645
512x512	16384 bits	53.7982	0.2499	53.8054	0.3806	53.8149	0.2486	53.8174	0.2492
512x512	24964 bits	51.9777	0.3807	51.9788	0.3806	51.9841	0.3801	51.9979	0.3809

Table 2 Image Steganography through Simple LSB

Simple LSB						
Cover Image	Msg1(4225bits)		Msg2(16384 bits)		Msg3(24964 bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.0700	0.0650	53.2174	0.2500	51.3902	0.3808
Lena	59.6578	0.0649	53.7982	0.2503	51.9777	0.3807
Baboon	59.1370	0.0645	53.2761	0.2488	51.4320	0.3804

Table 3 Image Steganography through Random LSB

Random LSB						
Cover Image	Msg1(4225 bits)		Msg2(16384 bits)		Msg3(24964 bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.0840	0.0648	53.2117	0.2503	51.3672	0.3828
Lena	59.6958	0.0644	53.8054	0.2499	51.9788	0.3806
Baboon	59.0912	0.0646	53.2297	0.2493	51.3986	0.3800

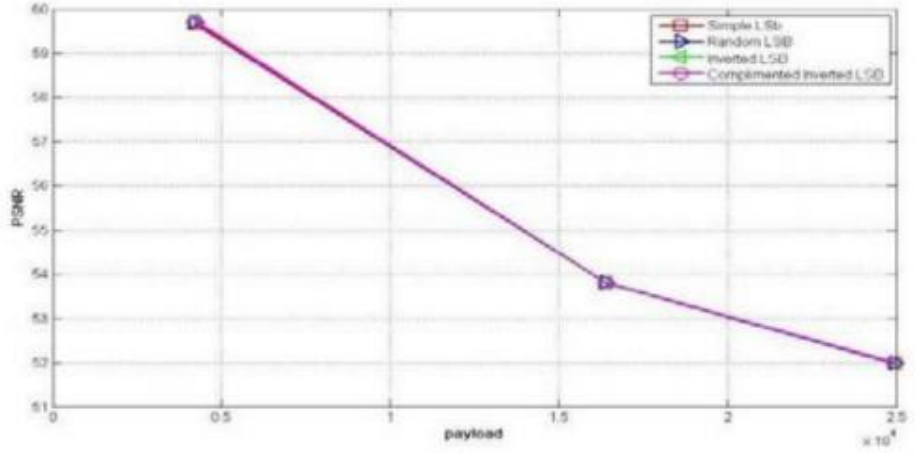
Table 4 Image Steganography through Inverted LSB

Invert LSB						
Cover Image	Msg1(4225Bits)		Msg2(16384Bits)		Msg3(24964Bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.1391	0.0639	53.227	0.2497	51.3583	0.3836
Lena	59.7138	0.0641	53.8149	0.2486	51.9841	0.3801
Baboon	59.1025	0.0650	53.2495	0.2503	51.4332	0.3803

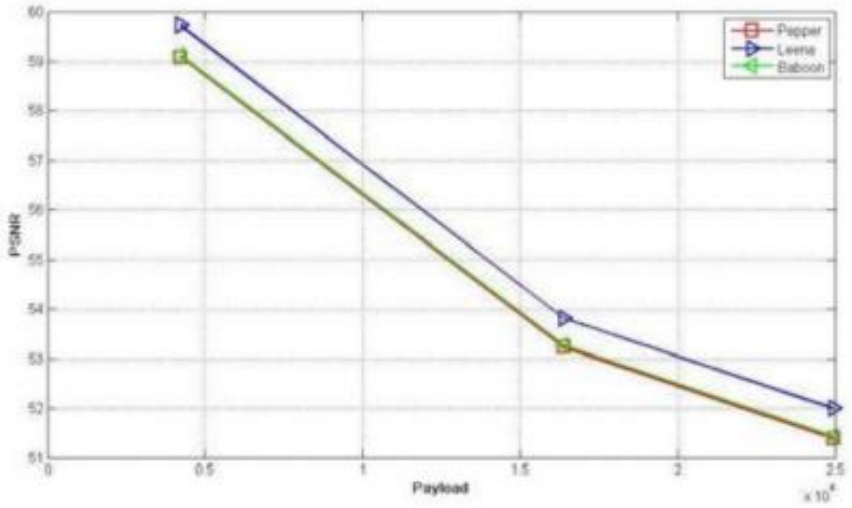
Table 5 Image Steganography through Complemented Inverted LSB

Invert LSB						
Cover Image	Msg1(4225Bits)		Msg2(16384Bits)		Msg3(24964Bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.0945	0.0647	53.2341	0.2490	51.3912	0.3807
Lena	59.7275	0.0645	53.8174	0.3810	51.9979	0.3789
Baboon	59.1234	0.0647	53.2779	0.2487	51.4310	0.3805

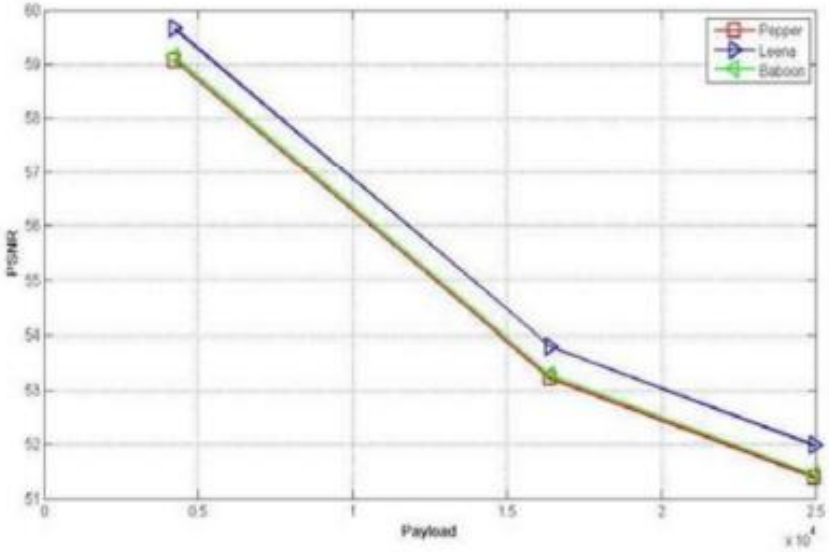
شکل 1مقایسه طرح پیشنهادی با LSBساده، تصادفی و معکوس



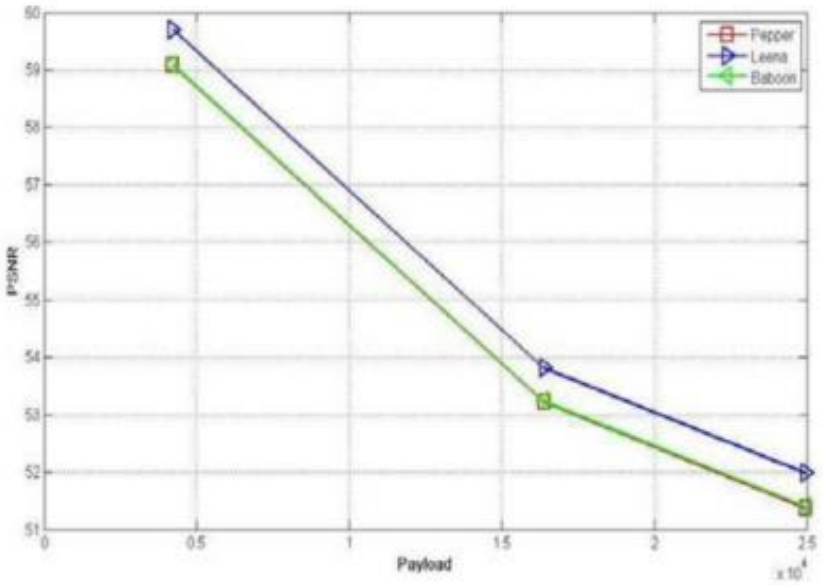
شکل 2مقایسه LSB PSNRمعکوس تکمیل شده



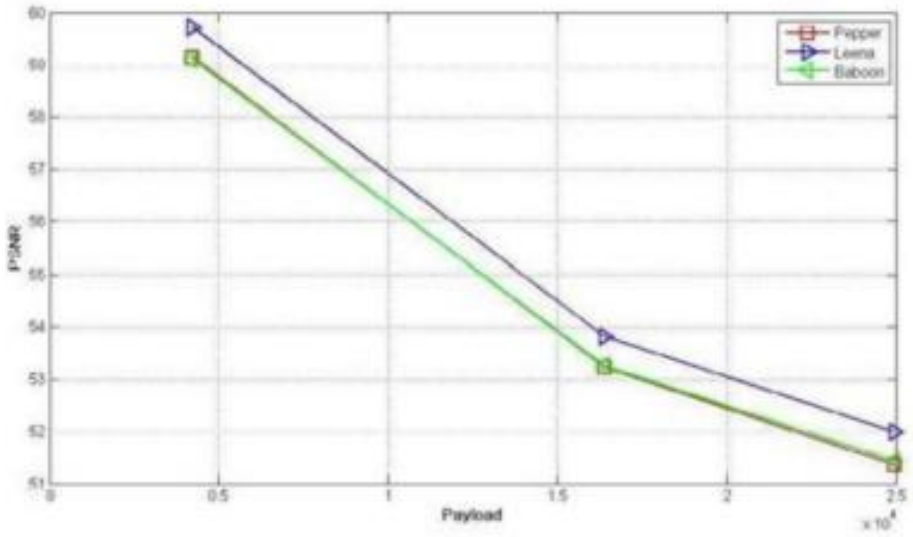
شکل 3مقایسه ساده LSB PSNR



شکل :4مقایسه تصادفی LSB PSNR



شکل 5مقایسه LSB PSNRمعکوس



۶. نتیجه گیری

هدف اصلی این مقاله ارائه سه سطح امنیت است، به جای پنهان کردن بیت‌های پیام به طور مستقیم در تصویر جلد، پیکسل‌ها به‌طور تصادفی از طریق مولد اعداد تصادفی شبه تولید می‌شوند پس از آن که داده‌های مخفی در پشت تصویر جلد با استفاده از روش LSB معکوس پنهان می‌شوند.

مطالعه تجربی نشان می‌دهد که سیستم پیشنهادی از نظر کیفیت بصری بالاتر از روش LSB اولیه بهتر است همانطور که با مقادیر بالای PSNR پنهان کردن بیت‌های پیام ترشحی در تصویر نشان داده می‌شود، بنابراین شانس شناسایی پیام محرمانه را کاهش می‌دهد و ارتباط مخفی را امکان‌پذیر می‌سازد. برای کارهای آینده، ما از طریق اتوماتای سلولی به عنوان سیستم ایمن بیشتر، اعداد تصادفی تولید می کنیم و از انواع دیگری از شی پوشش برای مخفی کردن داده ها استفاده می کنیم.