وزارت علوم تحقیقات و فن آوری

دانشکده فنی مهندسی

پنهان نگاری سیگنال های صوتی دیجیتال به روش طیف گسترده و بهبود آشکارسازی اطلاعات پنهان شده

پایان نامه برای دریافت درجه کارشناسی ارشد

در رشته مهندسی برق گرایش مخابرات_سیستم

حسین فمی تفرشی

استاد راهنما:

دکتر علی اصغر سلطانی فرانی

بهمن 1392

وزارت علوم تحقیقات و فن آوری

دانشکده فنی مهندسی

گروه برق

پنهان نگاری سیگنال های صوتی دیجیتال به روش طیف گسترده و بهبود آشکارسازی اطلاعات پنهان شده

پایان نامه برای دریافت درجه کارشناسی ارشد

در رشته مهندسی برق گرایش مخابرات_سیستم

حسین فمی تفرشی

استاد راهنما:

دکتر علی اصغر سلطانی فرانی

استاد مشاور:

دکتر عباس طاهرپور

بهمن 1392


بسم الله الرحمن الرحيم

تقدیم به پدر، مادر خانواده عزیزم که در تمام لحظات زندگی یار

و یاور من هستند.

تشکر و قدردانی از استاد عزیز جناب آقای دکتر سلطانی

فر و همچنین آقای دکتر عباس طاهر پیام دوستانی که مرا در انجام

این پروژه یاری نمودند.

چکیده

امروزه با گسترش وسیع شبکه ی جهانی اینترنت و همچنین به سبب بوجود آمدن رسانه های دیجیتال، امکان کپی کردن، نمونه برداری، اصلاح و در کل تغییر اطلاعات دیجیتال امری ساده به نظر می رسد. این اطلاعات دیجیتال عبارتند از: صوت، تصویر، ویدئو، متن و... . حفظ مالکیت و همچنین حفاظت از حق نشر یک اثر آن هم با فرمت دیجیتال، امروزه به یک چالش تبدیل شده است بطوریکه در بسیاری موارد بعد از کپی کردن غیرمجاز، فایل کپی شده از نمونه ی اصلی آن قابل تفکیک نیست.

از طرف دیگر روش های سنتی رمزنگاری که برای انتقال امن اطلاعات استفاده می شد، راه حل مناسبی برای حفظ حق مالکیت اثر و تعیین اصلی بودن آن نیست. پنهان نگاری یک روش مرسوم برای اضافه کردن اطلاعات به محتوای اصلی و ایجاد یک امضای دیجیتال، در آن است. به همین دلیل در بسیاری از سناریوها می توان با اضافه کردن اطلاعاتی به محتوای اصل (مانند یک تصویر یا یک فایل صوتی) امکان حفظ حق مالکیت اثر را فراهم ساخت. درحالت ایده آل می بایست از نظر ظاهر تفاوتی بین سیگنال اصلی و سیگنال پنهان نگاری شده مشاهده نشود.

در این رساله از روشی نوین بر پایه ی طیف گسترده برای پنهان نگاری استفاده شده است. در روش ارائه شده با استفاده از بلوک های پیش پردازش صوتی (کدینگ پیش بینی خطی و فیلتر بالا گذر) و استفاده از تابع کنترل گین به ترتیب در احتمال صحت بازیابی اطلاعات پنهان شده و همچنین شفافیت سیگنال پنهان نگاری شده، نسبت به روش مرسوم پنهان نگاری صوتی، بهبود حاصل شده است. همچنین افزایش ظرفیت پنهان نگاری (میزان اطلاعات پنهان شده در هر فریم) از دیگر دست آورد های روش پیشنهادی رساله می باشد.

کلید واژه: پنهان نگاری صوتی، روش طیف گسترده، بلوک کدینگ پیش بینی خطی

فهرست مطالب

عنوان **صفحه**

فهرست نمودارها شکل ها ..... و

فهرست جدول ها ..... ح

فهرست علائم و اختصارها ..... ط

فصل1.پیشگفتار 1

1-1. مقدمه 2

2-1. تاریخچه ی پنهان نگاری 2

3-1. نهان نگاری 3

4-1. پنهان نگاری (نقش آب زنی) 4

5-1. تفاوت نهان نگاری و پنهان نگاری 5

6-1. تفاوت پنهان نگاری و رمزنگاری 6

7-1. انواع مختلف پنهان نگاری از لحاظ مقاومت 6

8-1. انواع مختلف پنهان نگاری از لحاظ آشکارسازی الگو 7

9-1. پارامترهای ارزیابی روش های پنهان نگاری 7

1-9-1. شفافیت 8

2-9-1. ظرفیت 9

3-9-1. مقاومت 9

1-3-9-1. برخی از انواع حملات 10

4-9-1. امنیت 10

5-9-1. پیچیدگی محاسبات 10
10-1. کاربرد های پنهان نگاری 10
1-10-1. حفظ حق مالکیت 10
2-10-1. اعمال اثر انگشت 11
3-10-1. تعیین اعتبار 11
4-10-1. کنترل کپی و دست یابی 11
5-10-1. کنترل ترافیک هوایی 12
6-10-1. حمل اطلاعات بیشتر 12
11-1. سازماندهی پایان نامه 12
فصل2. معرفی و بررسی اجمالی برخی از روش های پنهان نگاری 14
2-1.مقدمه 15
2-2. کد کردن بیت کم ارزش 16
2-3. نهان کردن در پژواک 16
2-4. مدولاسیون اندیس کوانتیزاسیون 18
2-5. کدینگ فاز 19
2-5-1. کدینگ فاز تبدیل فوریه یا روش بِندِر[1][1] 20
2-5-2. تغییر فاز فرکانس های تصادفی[2] 21
2-6. طیف گسترده 22

[1] Bender

2-6-1. روش SSW 23
2-6-2. روش ISS 23
2-6-3. سایر تحقیقات و مطالعات صورت گرفته در سال های اخیر 24
فصل3. روش پیشنهادی شنهان نگاری مبتنی بر تکنیک طیف گسترده 26
3-1. مقدمه 27
3-2. پنهان نگاری به روش طیف گسترده (SSW) 27
3-2-1. روند پنهان کردن اطلاعات در سیگنال میزبان 27
3-2-2. بازیابی اطلاعات پنهان شده 28
3-2-3. تعیین پارامتر شفافیت (α) 29
3-2-4. ظرفیت پنهان نگاری 30
3-2-5. تعیین طول سیگنال میزبان و دنباله شبه نویز (N) 30
3-2-6. بررسی احتمال خطا 30
3-3. روش پیشنهادی 33
3-3-1. ارائه ی روش ساخت تعداد بیشتری دنباله ی شبه نویز 33
3-3-2. جاسازی اطلاعات سیگنال میزبان 34
3-3-3. تعیین پارامتر شفافیت 34
3-3-4. پارامتر شفافیت اشباع (α_{sat}) 36
3-3-5. بازیابی اطلاعات پنهان شده 38

6-3-3. استفاده از بلوک های پیش پردازش برای بازیابی اطلاعات 40

4-3. بررسی روابط احتمال در روش پیشنهادی ($M = 3$) 42

5-3. بررسی رابطه ی احتمال خطا در حالت کلی 47

6-3. ظرفیت پنهان نگاری روش پیشنهادی 49

فصل4. بررسی آزمایشات، مقایسه ها و شبیه سازی ها 50

1-4. مقدمه 51

2-4. مقایسه ی تئوری احتمال خطای روش SSW و روش پیشنهادی رساله (بدون بلوک های پیش پردازش) در ظرفیت برابر 52

3-4. بررسی روش پیشنهادی با/بدون α_{sat} و بلوک های پیش پردازش 54

4-4. مقایسه ی روش SSW و روش پیشنهادی رساله بدون در نظر گرفتن حملات و دست کاریها 57

5-4. مقایسه ی روش SSW و روش پیشنهادی رساله در حضور حملات و دست کاری ها 59

1-5-4. نویز گوسی جمه شونده 59

2-5-4. فیلتر میان گذر 59

3-5-4. فیلتر تمام گذر 59

4-5-4. اضافه شدن اکو 59

فصل5. جمع بندی و راهکارهای آتی 63

1-5. نتیجه گیری 64

2-5. پیشنهادات 66

فهرست مراجع..... 67

پیوست 1. تولید شبه نویزهای متعامه به کمک ماتریس هادامرد.....70

پیوست 2. بلوک کدینگ پیش بینی خطی.....73

فهرست نمودارها و شکل ها

عنوان **صفحه**

شکل (1-1) نمایش کلی بلوک جاسازی اطلاعات..... 5

شکل (1-2) نمایش کلی بلوک بازیابی اطلات 5

شکل (2-1) طریقه درج یک بیت اطلاعات 0 یا 1 به روش مدولاسیون اندیس کوانتیزاسیون 18

شکل (1-3) منحنی تغییرات پارامتر شفافیت α بر حسب تغییرات توان هر فریم از سیگنال صوتی.. 27

شکل (2-3) مقادیر مختلف C_j به ازای تغییرات j، محل مازیمم همان اندیس s است 29

شکل (3-3) آشکارساز بدون استفاده از بلوک های پیش پردازش 40

شکل (4-3) بخش بازیابی اطلاعات به همراه بلوک های پیش پردازش 42

شکل (5-3) منحنی تغییرات احتمال خطا بر حسب انرژی دنباله های شبه نویز (α^2)..... 47

شکل (1-4) الف: سیگنال صدای زنگوله. ب: قطعه ای از کنسرت موسیقی بتهوون. ج: سیگنال صدای کلیک موس. د: سیگنال صوتی نمونه مورد آزمایش نرم افزار متلب (handle) 51

شکل (2-4). احتمال خطای پنهان نگاری (Pe) برای سه حالت روش پیشنهادی و همچنین روش SSW به ازای تغییرات HWR 54

شکل (3-4) نمودار میله ای احتمال خطای بازیابی اطلاعات (در مرتبه 10^{-2}) برای سیگنال های صوتی مختلف 58

شکل (4-4) نمودار میله ای ظرفیت پنهان نگاری اطلاعات بر حسب $[\frac{bit}{sample}]$ برای سیگنال های صوتی مختلف 58

شکل (5-4) احتمال خطای بازیابی اطلاعات با اعمال انواع حملات برای سیگنال صدای زنگ 60

شکل (6-4) نمودار احتمال خطای بازیابی اطلاعات با اعمال انواع حملات برای سیگنال قطعه موسیقی بتهوون 61

شکل (4-7) نمودار احتمال خطای بازیابی اطلاعات با اعمال انواع حملات برای سیگنال صدای کلیک موس 61

شکل (4-8) نمودار احتمال خطای بازیابی اطلاعات با اعمال انواع حملات برای سیگنال صوتی handle 61

فهرست جداول

عنوان **صفحه**

جدول (1-1) میزان اختلال و کیفیت سیگنال بر حسب امتیاز 8

جدول (4-1) مشخصات فایل های صوتی مورد آزمایش 52

جدول (4-2) حالات مختلف برای بررسی احتمال خطای روش پیشنهادی رساله نسبت به روش SSW در ظرفیت برابر 52

جدول (4-3) تعداد دفعات مورد نیاز برای ارسال در هر یک از حالات 53

جدول (4-4) احتمال خطای بازیابی اطلاعات روش پیشنهادی رساله برای سیگنال صدای زنگ 55

جدول (4-5) احتمال خطای بازیابی اطلاعات روش پیشنهادی رساله برای سیگنال قطعه ی موسیقی بتهون 55

جدول (4-6) احتمال خطای بازیابی اطلاعات روش پیشنهادی رساله برای سیگنال صدای کلیک موس 55

جدول (4-7) احتمال خطای بازیابی اطلاعات روش پیشنهادی رساله برای سیگنال handle 56

جدول (4-8) نتایج آزمایشات پنهان نگاری روش پیشنهادی رساله برای چهار سیگنال صوتی مورد آزمایش (ظرفیت بر حسب $[\frac{bits}{sample}]$ است.)..... 56

جدول (4-9) نتایج آزمایشات پنهان نگاری روش SSW برای چهار سیگنال صوتی مورد آزمایش .. 57

جدول (4-10) احتمال خطای بازیابی اطلاعات روش پیشنهادی رساله در مرتبه 10^{-2} 60

جدول (4-11) احتمال خطای بازیابی اطلاعات روش SSW در مرتبه 10^{-2} 60

فهرست علائم و اختصارها

عنوان	صفحه
نرخ خطای بیت	BER
پنهان نگاری به روش طیف گسترده	SSW
پنهان نگاری توسعه یافته به روش طیف گسترده	ISS
نویز سفید گوسی جمع شونده	AWGN
نسبت انرژی سیگنال میزبان به انرژی سیگنال واترمارک	HWR
ظرفیت پنهان نگاری در روش طیف گسترده	C_{TSS}
تابع احتمال خطا	$erfc$
تابع احتمال خطا	Q(.)
سیگنال پنهان نگاری شده	W
سیگنال میزبان	X
دنباله ی شبه نویز	U
طول فریم	N
تعداد دنباله های شبه نویز	M
یک بیت اطلاعات	b
پارامتر شفافیت پنهان نگاری	α
نویز	$\bar{n}$

احتمال خطای بازیابی اطلاعات	P_e
وزن پنهان نگاری	c
پارامتر فریم های سکوت	ε
دسی بل	dB

فصل 1

پیشگفتار

فصل 1. پیشگفتار

1-1. مقدمه

پنهان نگاری اطلاعات در در داخل یک شئ پوشش یکی از موضوعات علم پردازش سیگنال های دیجیتال است. در طول تاریخ نیز از این تکنیک با توجه به تکنولوژی موجود در آن عصر و دوره، استفاده می شده است. در پنهان نگاری اطلاعات در سیگنال های دیجیتال، درحالت ایده آل می بایست از نظر ظاهر تفاوتی بین سیگنال اصلی[1] و سیگنال پنهان نگاری شده[2] مشاهده نشود[۲].

در این فصل به بررسی تاریخچه ی پنهان نگاری، ارائه ی تعریف پنهان نگاری، تفاوت پنهان نگاری با نهان نگاری و رمز نگاری، انواع مختلف پنهان نگاری، معیار های الگوریتم های پنهان نگار و در نهایت کاربردهای این حوزه، می پردازیم.

1-2. تاریخچه ی پنهان نگاری اطلاعات

در کتاب هیستوریس[3] نوشته ی تاریخ نگار معروف یونانی هرودوت[4] که متعلق به سال 440 قبل از میلاد مسیح (ع) است، اولین مستندات و یادداشت های مربوط به پهان نگاری اطلاعات آمده است. در یکی از یادداشت ها آمده است که داریوش پادشاه قدرتمند ایران زمین، دستور داده بود که موی سر یکی از زندانیان تراشیده شود و پیام محرمانه ای روی پوست سر او حک شود و بعد از اینکه موی سر زندانی بلند شد وی را به سمت میلدوس[5](یکی از شهرهای یونان قدیم) روانه سازند. همچنین خبر حمله ی خشایار شاه پادشاه ایران، به یونان نیز بصورت مخفی و پنهان شده توسط یک یونانی به نام دمراتوس[6] به سمت اسپارتا[7] فرستاده شد. وی پیام مربوط را بر روی یک تخته نوشته بود و سپس آنرا با لایه ای از موم پوشانده بود[3].

[1] Host signal
[2] Watermarked signal
[3] Histories
[4] Herodotus
[5] Miletus
[6] Demeratus
[7] Sparta

طی جنگ های جهانی اول و دوم نیز به دلیل ماهیت جنگ و فشارهای ناشی از آن، پنهان نگاری و روش های مربوطه دستخوش پیشرفت های قابل ملاحظه ای شد. بطور مثال استفاده از جوهر های نامرئی برای نوشتن پیام های مخفی و دارای اهمیت، تکنیکی بود که در جنگ جهانی اول مورد استفاده قرار می گرفت. اجزای سازنده ی این جوهر ها مواد ساه ای مانند عصاره ی میوه بودا، شیر و سرکه بود که با گرم کردن کاغذ حاوی اطلاعات، رنگ جوهر مرئی و قابل خواندن می شد. در جنگ جهانی دوم نازی ها روش های پیشرفته تری را توسعه دادند و از آنها برای ارسال اطلاعات بصورت پنهان توسط جاسوسان خود استفاده می کردند[4].

3-1. نهان نگاری[1]

واژه ی استگانوگرافی یا نهان نگاری کلمه ای است که از یک تکنیک قدیمی بنام رمز نگاری[2] گرفته شده است. در رمز نگاری محتوای پیام حفظ می شود [5]. در واقع نهان نگاری تکنیکی است که در آن اطلاعات در داخل یک پوشش، بطور غیرقابل مشاهده، جاگذاری می شوند. به همین دلیل کلمه استگانوگرافی ترکیبی از دو واژه ی پوشش[3] و نوشتن[4] است [6]. پنهان نگاری ایده آل زمانی است که اطلاعات بصورت کاملا غیرمحسوس (غیر قابل مشاهده برای فایل های تصویری یا غیر قابل شنود برای فایل های صوتی) در داخل یک پوشش جاسازی شوند.

همانطور که گفته شد در پنهان نگاری به یک شی پوشش[5] نیاز داریم تا اطلاعات درون آن جاسازی شود. همچنین به منظور افزایش امنیت می توان برای جاسازی اطلاعات از کلید یا کلید های مخفی[6] نیز استفاده کرد که در این حالت می بایست هم فرستنده و هم گیرنده از این کلید یا کلید ها اطلاع داشته باشند و در اختیار آن ها قرار گرفته باشد [7].

[1] Steganography
[2] Cryptography
[3] Stego = Covered
[4] Graphy = Writing
[5] Cover Object
[6] Secret Key

4-1. پنهان نگاری [1](نقش آب زنی)

نقش آب زنی یا پنهان نگاری نیز روشی مشابه نهان نگاری است که از آن برای درج اطلاعات بصورت مخفی داخل یک شئ پوشش، استفاده می شود (تفاوت این دو روش در ادامه ذکر می گردد). از این پس در این رساله برای تکنیک مذکور فقط از کلمه ی پنهان نگاری استفاده می شود و دیگر کلمه ی نقش آب زنی بعنوان ترجمه ی واژه ی انگلیسی آن مورد استفاده قرار نخواهد گرفت. در پنهان نگاری نیز مجددا از یک یا چندین کلید مخفی استفاده می شود. استفاده از کلید مخفی بدین دلیل است که کاربرهای غیرمجاز قادر به استخراج اطلاعات پنهان شده نباشند و بدین ترتیب امنیت روش پنهان نگاری افزایش می یابد. در پنهان نگاری به اطلاعات پنهان شده اطلاعات الگو یا پیام[2] ، به شئ پوشش، سیگنال میزبان[3] یا سیگنال اصلی[4] و در نهایت به سیگنالی که در آن اطلاعات جاگذاری شده است سیگنال جاسازی شده[5]، یا سیگنال پنهان نگاری شده[6] می گویند [6]. روش های مختلف پنهان نگاری از دو بخش اصلی تشکیل می شوند:

1. بلوک جاسازی اطلاعات[7]
2. بلوک بازیابی اطلاعات[8]

در شکل (1-1) و (1-2) بلوک های جاسازی اطلاعات و بازیابی اطلاعات بطور جداگانه نشان داده شده اند.

[1] Watermarking
[2] Watermark
[3] Host signal
[4] Original Signal
[5] Embedded signal
[6] Watermarked signal
[7] Embedding Block
[8] Reconstruction block