روشهای رمزکردن آنالوگ سیگنال گفتار

یوسف پورابراهیم
دانشکده برق
دانشکده فنی دانشگاه امام حسین(ع)
yousef.pourebrahim@gmail.com

بابک پناهنده ینگجه
دانشکده برق
دانشکده فنی دانشگاه آزاد واحد اردبیل
panahandeh@gmail.com

چکیده : صحبت وگفتارمهمترین ودرعین حال آسانترین روش برقراری ارتباط در جامعه است و از آنجا که اکثر دستگاههای برقرار کننده ارتباط دو طرفه وسایل همگانی‌اند(مانند رادیو، تلفن و...) انجام دادن موفقیت‌آمیز حمله‌های فعال ونافعال به این سیستم ارتباطی امری ساده است. مثلا درمورد کانال تلفنی دشمن می‌تواند با یک دستگاه تلفن ازخط مورد نظرش استراق سمع کند؛ یا باتغییرلهجه خود را به جای فرد معتبری جا زده وگیرنده را به واکنش دلخواه خود وادارد.[1].لذا در این مقاله سعی شده‌است که انواع اسکرامبلرهای گفتار بررسی شده و نکات قوت و ضعف هریک بیان گردد ودر نهایت بهترین روش جهت رمز کردن سیگنال گفتار را معرفی نماید.

کلمات کلیدی: *اسکرامبلر، استراق سمع، سیگنال صحبت*

۱- مقدمه

سیستمهای رمزنگاری صحبت(اسکرامبلرها) ازلحاظ چگونگی ارسال سیگنال رمزشده به دودسته کلی تقسیم می شوند:

الف- سیستمهای رمز آنالوگ ب- سیستمهای رمزدیجیتالی

درروش آنالوگ، شکل موج ارسالی برای گیرنده، یک سیگنال آنالوگ است که بطورپیوسته نسبت به زمان تغییر می کند. در صورتیکه در روشهای دیجیتالی، سیگنال ارسالی در هرلحظه تنها یک مقدار از چند مقدار اصلی قابل قبول راخواهد داشت. البته درسیستمهای آنالوگ نیز علاوه بر پردازش آنالوگ می توان از پردازش دیجینالی نیز استفاده کرد. ولی در هرصورت سیگنال ارسالی آنالوگ خواهد بود. امروزه سیستمهای رمزنگاری دیجیتالی بیشتر بکار می رود. لیکن نحوه انتخاب روش به زمینه کاربرد سیستم و محدودیتهای عملی مخصوصاً کانال ارتباطی بستگی خواهد داشت. برای مثال اگر امنیت به میزان بالا مهمترین پارامتر باشد و کیفیت و اعتبار گوینده چندان مهم نباشد، معمولاً روشهای دیجیتالی بکار می رود. بهرحال در این مقاله خواننده را با انواع رمزکننده‌های آنالوگ سیگنال گفتار آشنا کرده و نتایج حاصل از آزمایشها از جهت پیچیدگی اجرای هر یک از رمزکنندها، کیفیت سیگنال ارسالی، تاخیر زمانی بوجود آمده و امنیت ایجاده شده ارایه خواهد شد.

۲- هدف از رمز کردن سیگنال صحبت

بطور کلی هدف رمز کردن صحبت رامی توان در موارد زیرخلاصه کرد:

۱- ایجاد تغییرات در سیگنال صحبت به طوری که از راه شنیدن قابل درک نباشد

۲- کلیه اطلاعات اصلی صحبت حفظ شود

۳- تغییرات ایجاد شده قابل رفع و گفتار قابل دستیابی دوباره باشد

۴- پهنای باند سیگنال رمز شده محدود باشد (قابلیت انتقال پیام)

۵- انرژی سیگنال رمز شده محدود باشد

۶- تآخیر زمانی برای بازیابی مجدد سیگنال محدود باشد. در سیستمهای بلادرنگ این تآخیر باید مستقل از پیام و ثابت باشد.

بمنظور افزایش کیفیت عمل رمز کردن صحبت باید موارد زیر رعایت شود:

۱- عمل تغییر مشخصه سیگنال صحبت ثابت نباشد و با زمان تغییر کند.

۲- ترتیب انجام تغییرات ، صرفا تابع کلید خاصی باشد که فقط استفاده کننده مجاز از آن آگاه باشد

۳- شکل سیگنال زمانی صحبت تا حد امکان فقط در فواصل کوچک زمانی حفظ شود (معمولا کمتر از ۷۰میلی ثانیه و برای سیستمهای پیشرفته ۳۰ میلی ثانیه)

۴- زمان لازم برای رمز گشایی با وجود دسترسی دشمن به الگوریتم کار بدون اطلاع از کلید با استفاده از بهترین ابزارهای موجود طولانی باشد

۵- شکل مشخصه فرکانس صحبت تا حد امکان حفظ شود(جز در فواصل کوچک و معمولا کمتر از ۳۰۰هرتز)

۶- کشف بخشی از پیام بدست دشمن حتی المقدور به کشف بقیه پیام کمک نکند

۷- کیفیت صحبت باز سازی شده از حد معینی تنزل نکند

۸- کل سیستم رمز و کشف صحبت با توجه به کاربرد دستگاه حجم و وزن معقول داشته باشد

۹- کیفیت سیستم تا حد امکان مستقل از صحبت ورودی باشد

۱۰- در مقابل اغتشاشهای محیط و اختلالهای کانال انتقال مقاوم باشد

۱۱- علی رغم ازدست دادن بخشی ازپیام در کانال انتقال بازسازی بقیه پیام ممکن باشد

۱۲- ایجاد اختلال از سوی دشمن در کانال انتقال تأثیرمهمی برباسازی سیگنال نداشته باشد.

۳- تقسیم بندی سیستمهای رمزآنالوگ

سیستمهای رمزآنالوگ به سه دسته عمده تقسیم می شوند:

۱- رمز کننده های حوزه زمانی

۲- رمزکننده های حوره فرکانسی

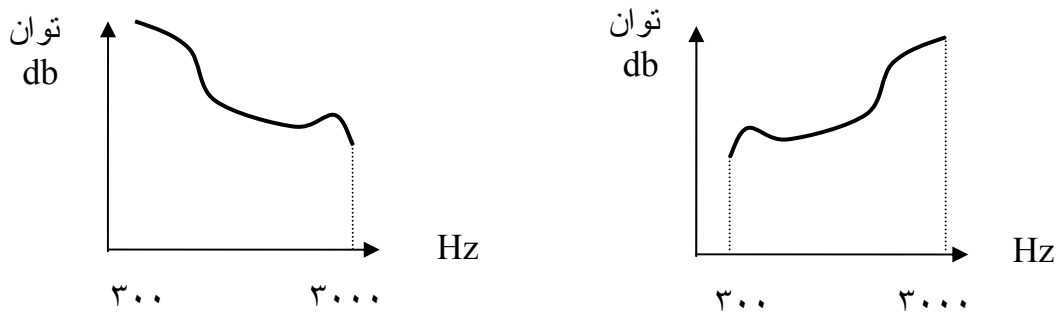
۳- رمزکننده ها براساس طیف گسترده که در حوزه زمانی یا فرکانسی صورت می گیرد.

شایان ذکراست که دربعضی سیستمها هردوحوزه زمان وفرکانس باهم نیز بکارمی روند. دراین گزارش تنها به سیستمهای آنالوگ خواهیم پرداخت.

۴- رمزکنندهای آنالوگ صحبت در حوزه فرکانس

۴-۱- وارونگی طیف فرکانس

در این روش چگالی توان صحبت معکوس می شود. شکل(۱) نحوه عملکرد این روش را نشان می دهد(در ترسیم این شکل فرض شده است که سیگنال دارای باند فرکانسی ۳۰۰تا۳۰۰۰هرتز است).



الف) سیگنال اصلی **ب) سیگنال رمزشده**

شکل(۱) نحوه عملکرد سیستم وارونگی طیف فرکانسی

۴-۱-۱- میزان امنیت

این روش ازروی طیف سیگنال به راحتی قابل تشخیص است و از نظر مقاومت در مقابل حمله های متفاوت عملکرد بسیار ضعیفی دارد زیرا فرکانس زیر و بمی در سیگنال اصلی و رمز شده برابر است و از طرفی چون گوش انسان معمولاً به فرکانسهای بالا حساس است و بدلیل انتقال انرژی صحبت به فرکانسهای بالا دراین روش تشخیص پیام گوینده با گوش دادن به سیگنال رمز شده ساده است

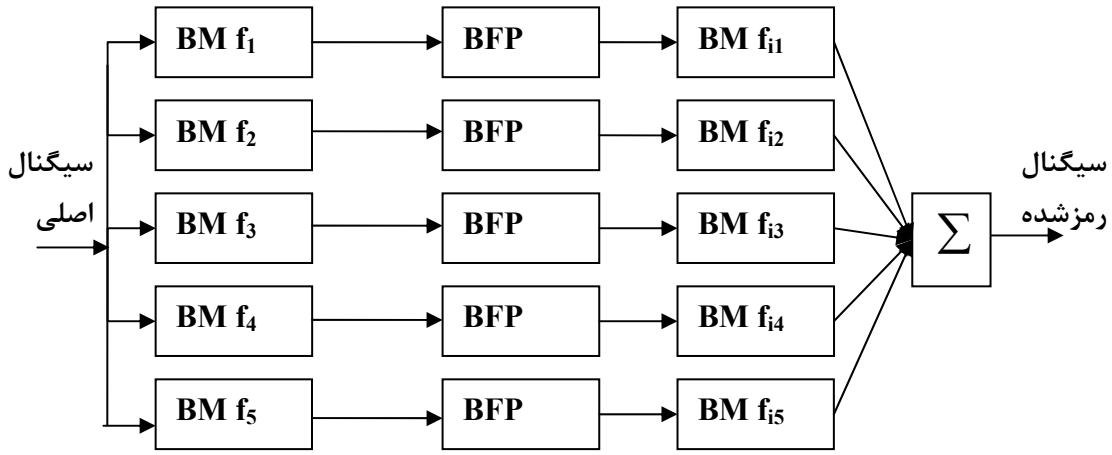
۴-۲- سیستم جایگشت باندهای فرکانسی

در این روش ابتدا طیف فرکانس سیگنال اصلی به تعدادی زیر باند تقسیم می شود که در حالت کلی طول نامساوی دارند. عمل رمزنگاری با تعویض جای زیرباندها در سیگنال رمز شده نسبت به سیگنال اصلی صورت می گیرد. در سیستمهای جدید علاوه بر تعویض جای زیر باندهای فرکانسی معمولاً بعضی از آنها را معکوس می کنند. نمودار بلوکی اجرای این روش درشکل (۲) نشان داده شده است که درآن فرض شده سیگنال صحبت باند فرکانسی از ۳۰۰هرتز تا ۳۳۰۰ هرتز رادارد. پهنای باند سیگنال اصلی به پنج زیرباند مساوی با پهنای ۶۰۰ هرتز تقسیم شده است. برای راحتی کار فرض شده است همه فیلترهای میانگذر پهنای باندی برابر با ۶۰۰ هرتز دارند و در محدوده فرکانسی (۹/۷ تا ۱۰/۳

کیلوهرتز) با فرکانس مرکزی ۱۰ کیلوهرتز واقع اند. برای آنکه زیرباند اول در محدوده فرکانس فیلترمیانگذر قرار گیرد باید فرکانس حامل اولین مودله سازمتعادل (BM) برابر ۹/۴=۹/۷-۰/۳ کیلوهرتز باشد. در اینصورت کل سیگنال اصلی به باند فرکانسی (۹/۷-۱۲/۷) کیلوهرتز منتقل می‌شود سپس بافیلترکردن سیگنال درمحدوده (۹/۷-۱۰/۳) کیلوهرتز زیرباند اول جدا می شود. به همین ترتیب برای بدست آوردن زیرباندهای دوم و سوم و چهارم و پنجم فرکانسهای حامل باید بصورت زیر انتخاب شوند:

$$f_2 = 8.8\,kHz \;, f_3 = 8.2\,kHz \;, f_4 = 7.6\,kHz \;, f_5 = 7\,kHz$$

دراینصورت در نقاط ۱،۲،۳،۴،۵ به ترتیب زیرباندهای ۵،۴،۳،۲،۱ خواهیم داشت.



شکل (۲) روش اجرای سیستم جایگشت باندهای فرکانسی

۴-۲-۱- میزان امنیت

میزان امنیت این روش به تعداد و چگونگی انتخاب تبدیل ها دارد. بدیهی است که همه تبدیلهای موجود لزوماً وضوح باقیمانده درسیگنال را به اندازه کافی کاهش نمی دهند. مثلا اگر تبدیل بکار رفته صرفاً یک جایگشت باشد، به قسمی که همه باندها به ترتیب عکس درطول باند فرکانسی کنار یکدیگر قرارگیرند(مانند روش وارونگی فرکانس)، یا آنکه محل سازه های اولیه سیگنال رمز شده مانند جای آنها در سیگنال اصلی باشد، سیگنال رمز شده دارای وضوح باقیمانده بالایی خواهد بود.نتایج تجربی بدست آمده مؤید این مطلب است.

درصورتیکه که تنها از جایگشت بدون وارونگی بعضی از زیرباندها استفاده شود تنها حدود ۱۰درصد از جایگشتها به وضوح باقیمانده کم منجر می شود.نتایج بالا بیانگر دو نکته مهم است:

۱- وضوح باقیمانده درسیگنال رمز شده نسبتاً بالا است.

۲- معیارهای مناسب بودن جایگشتهای بکاررفته درسیستم، ثابت واستاندارد نیستند

یکی دیگراز روشهای بالابردن میزان امنیت دراین روش افزایش تعداد زیرباندها ودرنتیجه کاهش پهنای باند هر زیرباند است. دراینصورت تعداد تبدیلها به میزان بسیار زیادی بالا می رود و درنتیجه تعداد تبدیلهای مناسب نیز افزایش می یابد. اما این روش نیز علاوه برافزایش پیچیدگی سیستم باعث می شود که سیگنال رمزشده شدیداً نویزی و

به تغییرات کانال حساس شود و درنتیجه کیفیت سیگنال افت پیدا کند. ازاین رو در سیستمهایی که ازاین الگوریتم برای رمزنگاری استفاده می کنند باند فرکانسی ۵ الی ۸ زیرباند تقسیم می شود.

۴-۳- جایگشت نمونه‌های تبدیل فوریه گسسته

اساس کار این روش شبیه روش جایگشت باندهای فرکانسی است. با این تفاوت که به جای آنکه زیر باندها زیر بنای عملیات رمز نگاری باشند نمونه‌های سیگنال صحبت اساس عملیات خواهند بود.در این روش ابتدا سیگنال صحبت از یک فیلتر پائین گذر عبور داده می‌شود تا پهنای باند سیگنال محدود شود. معمولاً این باند فرکانسی را از ۳۰۰ تا ۳۰۰۰ هرتز در نظر می‌گیرند. سپس این سیگنال را با فرکانس مناسب نمونه‌برداری می‌کنند و پس از آنکه تعداد نمونه‌های لازم بدست آمد از آنها تبدیل فوریه گسسته می‌گیرند و سپس با انجام جایگشت روی نمونه‌های موجود در قاب آنها را رمز می‌کنند. با انجام تبدیل فوریه گسسته معکوس نمونه‌های زمانی سیگنال رمز شده بدست می‌آید که با گذراندن از مبدل (D/A) سیگنال رمز شده آنالوگ حاصل می‌شود. نکاتی که در مورد این الگوریتم باید در نظر گرفت چنین‌اند:

۱- میزان امنیت سیستم و همچنین کیفیت سیگنال رمزگشایی شده تابع طول قاب است. از طرف دیگر افزایش طول قاب باعث تأخیر بیشتر در ذخیره‌سازی نمونه‌ها است. زیرا برای عمل جایگشت روی نمونه‌ها یک قاب باید همهٔ آنها موجود باشند و از آنجاییکه ایجاد تأخیر در اثر رمزنگاری باعث افت کیفیت سیگنال رمزگشایی می‌شود انتخاب طول قاب مصالحه‌ای بین کیفیت سیگنال و میزان امنیت پیش می‌آورد. از این رو در سیستم‌هایی که بر این اساس ساخته می‌شوند طول قاب را خیلی بزرگ نمی‌گیرند.

۲- این روش پهنای باند سیگنال رمز شده را تا نصف فرکانس نمونه‌برداری افزایش خواهد داد. لذا در صورتیکه بخواهیم این روش را در کانالهای با پهنای باند محدود مثلاً تلفن بکار بریم در خروجی گیرنده کیفیت قابل قبولی نخواهیم داشت. ازاینرو در سیستمهای رمز نگاری مبتنی بر این روش نمونه‌های DFT متناظر به فرکانسهای آنالوگ خارج از پهنای باند کانال را برابر صفر در نظر می‌گیرند و این امر باعث افت کیفیت سیگنال در خروجی می‌شود.

۴-۳-۱- میزان امنیت و کیفیت سیگنال رمز شده

وضوح باقی مانده در سیگنال رمز شده با این الگوریتم به مراتب کمتر از الگوریتم جایگشت باندهای فرکانسی است. زیرا با توجه به بزرگ بودن طول قاب نمونه‌ها می‌تواند بیشتر از محل اصلی خود فاصله بگیرد و انتخاب جایگشتهایی که همبستگی بین سیگنال اصلی و سیگنال رمز شده را کم کنند نسبت به روشهای پیش به آسانی میسر است. این الگوریتم به راحتی قادر به پخش یکنواخت انرژی در طول محور فرکانسی است.

۵- رمز کننده‌های آنالوگ گفتار در حوزهٔ زمان

۵-۱- الگوریتم وارونگر جزء زمانی

در این الگوریتم سیگنال به جزءهای پیوسته‌ای در حوزهٔ زمانی تقسیم می‌شود. سیگنال رمز شده از وارون کردن این جزء بدست می‌آید. برای دست آوردن سیگنال رمز شده کافی است از صحبت نمونه برداشت و به کمک یکی از روشهای کد کردن شکل موج کدهای رقمی بدست آورد. هر جزء سیگنال از پشت سرهم قرار گرفتن تعدادی از این کدها بدست می‌آید. برای رمز کردن کافیست نمونه‌های موجود در یک جزء گفتار بطور وارون به ترتیب عکس به یک مبدل دیجیتال به آنالوگ وارد شوند.

۵-۱-۱- میزان امنیت و کیفیت سیگنال رمزگشایی شده

با توجه به آنکه این الگوریتم تنها دارای یک کلید است درست مانند الگوریتم وارونگر فرکانس امنیت بسیار کمی دارد. شکستن این سیستم از طریق حمله نوع اول مثل یاد گرفتن یک زبان جدید به راحتی انجام می‌گیرد. . بنابر نتایج تجربی بدست آمده برای حداقل طول جزء ۲۰۰ میلی ثانیه وضوح باقی مانده قابل قبول است و البته این بستگی به سرعت گفتار خواهد داشت. در صورت پائین بودن سرعت گفتار حداقل طول ۲۵۰ میلی ثانیه بوضوح باقی مانده ناچیزی منجر می‌شود.

۵-۲- الگوریتم جایگشت جزء زمانی قطعه‌ای

در این الگوریتم ابتدا سیگنال آنالوگ به مدت زمانهای مساوی تقسیم می‌شود. این مدت زمان را قاب می‌نامند. سپس هر قاب به چندین جزء تقسیم می‌شود. عمل رمزنگاری بصورت جایگشت روی جزءهای موجود در یک قاب انجام می‌گیرد. با توجه به آنکه در این روش سیگنال موجود در جزءها هیچگونه تغییری نمی‌کنند و بشکل اصلی در سیگنال رمز شده باقی می‌ماند. به منظور کاهش میزان اطلاعاتیکه در سیگنال رمز شده تغییر نمی‌کنند می‌بایست طول جزء ها را کوتاه انتخاب کنیم، به‌نحوی که یک کلمه به طور کامل نتواند در طول یک جزء بیان شود. بنابر نتایج بدست آمده از آزمایش قابهای به طول ۸ تا ۱۶ جزء با طولهای ۱۰ الی ۳۰ میلی ثانیه هم از لحاظ میزان امنیت و هم به لحاظ کیفیت سیگنال رمزگشایی شده نتایج قابل قبولی ارائه می‌کند.

۵-۲-۱- میزان امنیت و کیفیت سیگنال رمزگشایی شده

چنانکه گفتیم وضوح باقی مانده در سیگنال رمز شده به طول قاب و همچنین تعداد جزءهای موجود در قاب بستگی دارد بطوریکه با افزایش تعداد جزءهای موجود در قاب وضوح باقی مانده کاهش می‌یابد. اما از طرف دیگر با افزایش تعداد جزءها پهنای باند سیگنال رمز شده بالا می‌رود. بدلیل تأخیر ایجاد شده در اثر تبدیل رمزنگاری و افزایش قابل ملاحظه پهنای باند معمولاً سیگنال رمزگشایی شده در این الگوریتم کیفیت مطلوبی ندارند. مثلاً برای تأخیر ۶۴ میلی ثانیه و افزایش پهنای باندی برابر ۸۹ درصد نسبت به سیگنال اصلی وضوح باقی مانده ۶۸ درصد است.

۵-۳- الگوریتم جایگشت نمونه‌های زمانی

یکی دیگر از روشهای ممکن برای رمز نگاری صحبت نمونه‌برداری از سیگنال اصلی و سپس جایگشت نمونه‌های موجود در یک قاب و ارسال سیگنال آنالوگ حاصل از نمونه‌های پردازش شده از طرق کانال برای گیرنده است. در گیرنده ابتدا از سیگنال دریافتی با فرکانس مناسب نمونه‌برداری می‌شود. آنگاه عکس جایگشت روی نمونه‌ها اعمال می‌شود و در پایان سیگنال آنالوگ حاصل از این نمونه‌ها به عنوان سیگنال رمز گشایی شده بکار می‌رود.

۵-۳-۱- میزان امنیت الگوریتم و کیفیت سیگنال رمزگشایی شده

این الگوریتم مقاومترین الگوریتم یک بعدی در برابر همه انواع حملات است. البته میزان امنیت، تابع طول قاب (تعداد نمونه‌های موجود در قاب) است. با افزایش طول قاب وضوح باقی مانده در سیگنال رمز شده کم می‌شود. علاوه بر آن فضای کلید نیز افزایش می‌یابد و در نتیجه تعداد جایگشتهای مناسب بیشتر خواهد شد.

با وجود سطح امنیت قابل قبولی که این الگوریتم عرضه می‌کند دو عیب عمده باعث شده است که این روش کارایی لازم را نداشته باشد

۱- افزایش پهنای باند سیگنال رمز شده

۲- حساسیت الگوریتم به حساسیت کانال

۶- الگوریتم پوشش دامنه

در این الگوریتم دامنه سیگنال صحبت با یک دامنه تصادفی جمع می‌شود. یکی از مهمترین مزایای این روش بالا بودن میزان امنیت آن در حد الگوریتمهای رقمی است. زیرا با انتخاب دامنه تصادفی می‌توان سیگنال رمز شده را تا حد زیادی به نویز سفید نزدیک کرد. علاوه بر آن فضای کلید در این روش بی نهایت است. زیرا در انتخاب دامنه تصادفی مناسب، هنچگونه محدودیت نداریم. در صورتیکه در این الگوریتم از پردازش آنالوگ استفاده شود با محدودیتهای عمده‌ای روبرو خواهیم بود از جمله:

۱- کاهش شدید نسبت سیگنال به نویز در گیرنده: در طول کانال انتقال نویز به سیگنال رمز شده اضافه می‌شود و در نتیجه دامنه تصادفی تغییر خواهد کرد. در صورتیکه سیگنال رمز شده دامنه بزرگی داشته باشد این مسئله اهمیت بیشتری خواهد داشت. زیرا عوامل ناخطی فرستنده، گیرنده و کانال انتقال باعث افت شدید کیفیت سیگنال رمزگشایی شده خواهد شد.

۲- در این الگوریتم برای بازسازی سیگنال اصلی وجود همزمانی بین فرستنده و گیرنده ضروری است، اما این همزمانی پیچیدگی سیستم را افزایش می‌دهد.

۷- نتیجه‌گیری

با گسترش روزافزون تبادل اطلاعات و بخصوص راحتی دستیابی به دستگاههای برقرار کننده ارتباط و در مقابل راحتی دستیابی به اطلاعات دو طرفه نیاز به رمز کردن اطلاعات امری ضروری می‌باشد. آنچه که ارایه شد روشهای آنالوگ موجود جهت سری کردن ارتباطات گفتاری هستند که با پیشرفت وسایل الکترونیکی امروزه اجرای آنها بصورت عملی کاملا امکان پذیر می‌باشد. اما در میان آنها روشهای تبدیل فوریه از لحاظ ایجاد سطح امنیت بالا و اجرای آسانتر بسیار کاربرد داردند. پیشنهاد می شود که برای افزایش امنیت از ماتریس هادامار نیز جهت رمزنگاری استفاد شود.

۸- مراجع

[1].C. J. Mitchell, F. C. Piper, "A Classification of time element speech scrambling" IEEE journal of the institution of electronic and radio engineering 1957

[2].Keiichi Sakurai, Keiichiro Koga, Takuro Muratani, "A Speech scrambler Using the fast Fourier Transform Technique" IEEE journal on selected areas in commucations,1984

[3].Aaron D. Wyner, "An Analog Scrambling Scheme which Dose Not Expand Bandwidth, Part ll: Continuous Time" IEEE Transactions ON Information Theory, VOL. IT-25, 4, JULY 1979