بررسی کلی روش‌های رمز سیگنال‌های آنالوگ

دکتر سیداحمد معتمدی

استادیار دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر

مهندس سیدمحمد احدی — مهندس ناصر صدقی

مربیان دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر

چکیده

استفاده از رمز برای پنهان نگاه داشتن اطلاعات مهم سیاسی، نظامی، و تجاری از جمله مواردی است که تاکنون مورد بررسی و مطالعهٔ فراوانی قرار گرفته است. در این مقاله ضمن برشمردن مواردی که باید در ایجاد رمز بآنها توجه نمود، تکنیک‌های رمز سیگنال های آنالوگ با استفاده از پردازش دیجیتال و آنالوگ مورد بررسی قرار گرفته و مقایسه‌ای از نظر پیچیدگی رمز، افزایش پهنای باند سیگنال رمز شده، وضوح باقیمانده و سایر مشخصات بین این روش ها انجام شده است.

Analysis of Analog Signal Ciphering Methods

S.A. Motamedi, P.h.D.

&

S.M. Ahadi, MSc

&

N. Sedghi, MSc

Elect. Eng. Dept.,Amirkabir Univ. Of Tech.

ABSTRACT

Cryptography of signals and texts is one of the most important matters dealt throughout the history of human civilization In this paper modern techniquesinvented by the use of electronics, specially in the ciphering of signals have been recognized, and due to the complexity of the ciphered signal and ease of implementing provided by different methods, the best of them is introduced

۱. مقدمه

استفاده از رمز برای پنهان داشتن اطلاعات در مخابرات امروزین جایگاه ویژه‌ای یافته است. آنچه موجب‌گشته که چنین جایگاهی برای رمزکننده بوجود آید ، نیاز به‌داشتن یک کانال امن ارتباطی است. چنین کانالی می‌تواند در موارد مختلف نظامی‌و سیاسی ،تجاری و شخصی کاربرد داشته باشد. قدرت و پیچیدگی روش مورد استفاده نیز بسته به‌مورد می‌تواند تغییر کند.

مقـاله‌ای کـه در ذیـل می‌آید، براساس کاری که به‌عنوان پروژه کارشناسی ارشد دردانشکده برق دانشگاه صنعتی امیر کبیر انجام شده تنظیم‌گردیده است. به‌لحاظ گستردگی کار و عدم‌امکان ارائه آن در اینجا، سعی شده تنها به یک بررسی اجمالی برروی روش های گوناگون مورداستفاده در رمز کردن یاخصوصی کردن ارتباطات بسنده گردد.

آنچـه دراین مقاله مطـرح می‌گردد، نگاه کوتاهی است به آنچه تحت عنوان روش‌های مختلف رمز کردن سیگنال‌های آنالوگ شناخته می‌شوند. این روشها که صرفا" در رمز کردن ارتباطاتی که از این گونه سیگنالها استفاده می‌نمایند به‌کار برده می‌شوند، طیف وسیعی را تشکیل می‌دهند که هر بخشی از آنها به‌گونه‌ای متفاوت با سیگنال مورد رمز برخورد می‌نماید. در ادامه مقاله، مقایسه‌ای کوتاه ازنظر مشخصات مختلفی که هریک از این رمزها ایجاد می‌کنند، و مزایا و معایب‌هریک ارائه خواهدشد.

۲. نیاز به‌رمز:

نیاز به‌استفاده از رمز درارتباطات، از آن زمان که ابتدایی‌ترین

اشکال‌جوامع بشری به‌وجود آمدند کم‌کم احساس گردید با ایجاد جوامع ، ارتباط میان آنها نیز مطرح می‌شد ، و با مطرح شدن و به‌وجود آمدن این ارتباطات به‌تدریج مساله رمز مطرح شد . آنچه که به‌عنوان اولین رمز در تاریخ ثبت شده، رمزی است که ژولیوس سزار در جنگ‌های گالیک به‌کار برد . در این روش وی با جایگزینی بعضی‌حروف الفباء با برخی دیگر، توانست پیغامی را به‌صورت رمز شده ارسال نماید . این‌نوع رمز که به رمز تک الفبایی موسوم است ، قرن‌ها به‌عنوان روش منحصر به‌فرد در رمز کردن مطرح بود . بررسیهای بیشتر، روش های کاملتری را در چندین قرن بعد ارائه نمود . با کوششهایی که در طول قرون متمادی در جهت بهبود کیفیت و ایمنی رمزها به‌کار برده شده تکنیک‌های جدیدی در زمینه رمز ابداع گردید .

تا قرن اخیر که روش های نوین مخابرات به‌وجود آمده و فراگیر شدند ، ارتباط تنها به‌طریق نامه (و یا در این اواخر به‌وسیله تلگراف) انجام می‌شد و بنابراین روش های رمز به‌وجود آمده، همگی برروی نوشته‌ها قابل اعمال بودند.استفاده از مخابرات جدید ، سیگنال‌های مختلفی را معرفی نمود که نقش کلیدی را در ایجاد ارتباطهای‌امروزین ایفا می‌نمایند . چنین ارتباط های غیرنوشتاری، روی آوردن به روش های رمز جدیدی را برای این گونه سیگنال ها ایجاب نموده است .

سیگنال هایی که در مخابرات امروزین کاربرد دارند می‌توانند عموما" به دو گروه آنالوگ و دیجیتال تقسیم گردند . بعضی ارتباطات اصولا" دیجیتال بوده و تکنیک‌های رمزی نیز که در مورد آنها به‌کار می‌روند ، عموما" تکنیک های دیجیتال می‌باشند ، این روش ها که در سالهای اخیر پیشرفت‌های فراوانی داشته‌اند امروز به‌صورت گسترده‌ای در رمز کردن سیگنالهای دیجیتال کاربرد دارند .

نوع دیگری از سیگنال های معمول در مخابرات امروز ، سیگنال‌های آنالوگ‌هستند که مخابرات آنالوگ امروزین با استفاده از آنها انجام می‌شود . در بررسی روش های رمز مورد استفاده، می‌توان روش‌های رمز کردن سیگنال های آنالوگ را به دو گروه مهم تقسیم نمود . اولین گروه ، روش هایی را شامل می‌گردد که عمل رمز این سیگنال ها را توسط پردازش آنالوگ آنها به‌انجام می‌رسانند .

گروه دوم روشهایی هستند که عمل پردازش را برروی سیگنال دیجیتال به‌دست آمده از سیگنال آنالوگ اولیه (پس از تبدیل آنالوگ به دیجیتال) به‌انجام می‌رسانند گروه اول در مقایسه با گروه دوم ، دارای سابقه تاریخی بیشتری هستند و اولین روش های مورد استفاده در رمز کردن سیگنالهای‌آنالوگ را شامل‌می‌گردند . در مقابل گروه دوم روش های جدیدتری را شامل شده و عموما" نیاز به‌سخت‌افزار نسبتا" پیچیده‌ای دارند .

۳. نکات مهم در ایجاد رمز :

روش های گوناگونی که در رمز کردن سیگنالها کاربرد دارند ، علاوه بر مشخصاتی که بسته به‌مورد مصرف‌باید دارا باشند (از قبیل حجم و پیچیدگی سخت افزار و نرم‌افزار لازم ، وجود کیفیت قابل قبول در سیگنال رمزگشایی شده، تامین مشخصات مورد نیاز کانال ارتباطی و ...) از نظر وضعیت سیگنال رمز شده نیز باید مشخصاتی را به‌وجود آورند که امنیت لازم را تامین می‌نماید . امنیت موردنیاز بسته به مورد استفاده فرق می‌کند . در بعضی روش ها که رمز کردن تنها برای پنهان داشتن ارتباط از دسترسی اتفاقی افراد دیگر انجام شده و سیگنال مورد رمز اهمیت نظامی، سیاسی‌و یا تجاری چندانی ندارد ، کافی است که سیگنال مورد رمز آنچنان تغییر یابد که توسط‌افراد غیر مجاز قابل درک نباشد . این گونه روش های رمز، به‌روش های خصوصی کردن (۱) اطلاعات موسومند . در مقابل، در بعضی دیگر از موارد استفاده، لازم است که سیگنال رمز شده تا حد امکان دارای پیچیدگی فراوان باشد به‌نحوی که طرف‌مقابل چنانچه درصدد شکستن رمز برآید نیز موفق به‌آن نگردد . البته در این حالت، پیچیدگی رمز دقیقا" بستگی به‌میزان اهمیت آن دارد . این که با شکسته شدن رمز چه مسائلو مشکلاتی به‌وجود می‌آیند مستقیما" میزان این پیچیدگی را تعیین می‌کند. اینکه سیگنال مورد رمز اهمیت تجاری، سیاسی، نظامی تاکتیکی و یا استراتژیک دارد، مشخص می‌نماید که پیچیدگی رمز باید در چه حدی باشد . علم رمزشکنی که به‌موازات پیشرفت تکنیک‌های رمز پیشرفت کرده نیز باعث می‌گردد تا در موارد بااهمیت بالا، هرنوع رمز پیچیده‌ای مورد قبول نبوده و خود رمز از جهات مختلف مورد بررسی قرار گیرد تا به‌آسانی قابل شکستن نباشد ، طرف مقابل (دشمن) خود را به‌امکانات بیشتری برای شکستن آن از قبیل دستگاههای مختلف ضبط، بررسی فرکانسی ، کامپیوترهای قوی، و افراد متخصص مجهز می‌سازد و بنابراین در این‌شرایط رمز باید بتواند در مقابل این عوامل مقاومت نماید .

مدت زمانی که یک سیگنال‌معتبر است نیز در ایجاد یک سیستم رمز کننده باید درنظر گرفته شود . بسته به‌مورد استفاده ، یک سیگنال باید برای مدت مشخصی محفوظ بماند . مثلا" در یک کار تجاری شاید پنهان ماندن یک خبر مهم حداکثر برای یک‌هفته کافی باشد در حالی که در یک‌مورد نظامی این مدت ممکن است بیشتر بوده و برای یک مساله سیاسی‌ممکن است بسیار بیشتر (چندین سال یا چند ده سال) باشد ، از آن جا که هر رمزی زمان مشخصی برای اعتبار دارد و برای آن زمانی تعریف می‌گردد که با توجه به‌امکانات موجود در مقابل رمز شکنی معمولی مقاومت خواهد نمود ، لازم است حداقل ایمنی هر رمز به‌این ترتیب‌تامین گردد که زمان شکسته شدن آن با توجه به‌پیشرفت امکانات در آینده و سایر روش های قابل استفاده در شکستن رمز ، از حداکثر زمان برای اعتبار سیگنال بیشتر باشد و هرچه زمان اول نسبت به‌زمان اخیر بیشتر باشد ، رمز دارای ایمنی بیشتری خواهد بود . البته باید توجه داشت که ایمنی تنها با توجه به روش های معمول رمزشکنی تعریف نشده چرا که برخی روش های غیرمعمول مانند روش های آماری باعث می‌گردند که بعضی رمزها بسیار زودتر از زمان مورد انتظار شکسته شوند .

علاوه بر مسائل فوق ، در برخی موارد نیاز به‌این است که به‌بعضی مسائل دیگر نیز توجه خاصی مبذول گردد چرا که عدم توجه به‌آنها موجب خواهد شد که مشکلات دیگری بروز نماید . از جمله این مشکلات می‌توان به‌وضوح باقیمانده (۲) درمتن رمز شده، تاخیر رمزکردن (۳) و افزایش پهنای باند فرکانسی (۴) که موجب کاهش کیفیت و یا گاه اصولا" عدم امکان استفاده از رمز می‌گردند ، اشاره نمود . این موارد خواهند شد .

۴. رمز سیگنال های آنالوگ بااستفاده از پردازش آنالوگ :

روش های رمز با استفاده از پردازش آنالوگ ،از جمله اولین

روش های رمز استفاده شده برای سیگنال های آنالوگ می‌باشند. این روش ها انواع مختلفی دارند که در میدان زمانی یا فرکانسی برروی سیگنال عمل نموده و انواع مختلفی از بسیار ساده تا بسیار پیچیده را شامل می‌شوند. روش های ساده به‌کار رفته در این محدوده اگرچه ایمنی چندانی را ایجاد نمی‌نمایند ولی به‌راحتی قابل ساخت بوده و در کاربردهای خصوصی کردن ساده به‌آسانی و ارزانی قابل استفاده می‌باشند. در مقابل برخی روش های پیچیده مورد استفاده در این محدوده ایمنی فراوانی را می‌توانند فراهم نمایند ولی نیاز به سخت‌افزار پیچیده‌ای برای ساخت دارند. به‌همین دلیل و به‌دلیل بعضی‌مزایایی که بعدا" ذکر خواهد گردید، این روش ها هنوز هم مورد استفاده فراوانی دارند.

ساده‌ترین روش در میان این روش ها، معکوس کردن فرکانس(۵) می‌باشد. این روش که خود یکی از قدیمی‌ترین روش های مورداستفاده می‌باشد، به‌آسانی قابل ساخت می‌باشد. در اینجا سعی می‌شود که باند فرکانسی سیگنال‌معکوس گردد به‌نحوی که قسمت بالای باند فرکانس به‌پایین باند و قسمت پایین آن به‌بالای باند منتقل گردد (شکل۱). این عمل با انجام مدولاسیون از نوع DSB برروی سیگنال پایه و توسط فرکانس موج حاملی که به‌درستی انتخاب شده باشد قابل انجام است. در این صورت قسمت منفی باند فرکانسی دقیقا" به‌جای قبلی قسمت مثبت آن منتقل می‌گردد. سپس توسط یک فیلتر مناسب می‌توان سیگنال معکوس شده فرکانسی را به‌دست آورد.

روش دیگر، به‌روش معکوس کردن و انتقال باند فرکانسی (۶) موسوم است. در این روش فرکانس حامل در عمل مدولاسیون بیش از فرکانس لازم برای معکوس کردن است. در این صورت قسمت اضافی خارج از باند از انتهای سیگنال جدا شده و به‌قسمت خالی‌ابتدای باند فرکانسی انتقال می‌یابددر این صورت سیگنال آشکار شکل ۲ ــ الف به شکل ۲ ــ ب درخواهد آمد. افزایش موج حامل موجب تغییر این سیگنال رمز شده به‌صورت‌شکل های ۲ــ پ تا ۲ ــ ج خواهد شد. روش دیگر این خواهد بود که با درنظر گرفتن چندین فرکانس‌حامل و سوئیچ کردن به‌صورت شبه‌اتفاقی (۷) بین آنها، عمل رمز را به‌انجام رساند. به‌این روش، معکوس‌کردن و انتقال باند دوره‌ای (۸) گفته می‌شود.

یکی دیگر از روش های معمول و پراستفاده، درهم ریختن‌باند فرکانس (۹) ــ است در این روش، باند فرکانسی سیگنال به چندین قسمت‌شده و این زیرباندها (۱۰) به‌صورت‌شبه‌اتفاقی جابه‌جا می‌گردند. در این صورت طیف فرکانسی‌سیگنال آشکار شکل ۳ــ الف به‌صورت شکل ۳ ــ ب درخواهد آمد. برای افزایش پیچیدگی رمز می‌توان این روش را با روش معکوس کردن باند فرکانسی نیز درهم آمیخت. به‌این ترتیب بعضی از زیرباندها به‌صورت اتفاقی می‌توانند معکوس گردند. نتیجه سیگنالی مشابه شکل ۳ــ پ خواهد بود. دراین مثال باند فرکانسی به‌پنج قسمت تقسیم شده و چنانچه عمل معکوس کردن نیز انجام شود، جمعا" $۵! \times ۲^۵ = ۳۸۴۰$ حالت مختلف به‌وجود خواهد آمد. در این روش معمولا" به‌خاطر محدود بودن پهنای باند و مشکل‌بودن مساله فیلتر کردن تعداد زیرباندها بسیار اندک بوده و از پنج تجاوز نمی‌نماید.

روش هایی که تاکنون دیدیم همگی برروی باند فرکانس سیگنال عمل می‌کردند. روش های دیگری نیز وجود دارند که‌در حوزه زمان عمل‌می‌کنند و اینک به‌بررسی‌آنها می‌پردازیم.

مهمترین روش رمز زمانی، روش موسوم به درهم‌ریختگی قطعات زمانی (۱۱) یا TDM (۱۲) است. این روش مشابه روش درهم‌ریختگی باند فرکانسی، ولی در حوزه زمان است. در این روش سیگنال آنالوگ به بخش هائی با طول ثابت زمانی به‌نام فریم (۱۳) تقسیم شده و هر فریم خود به‌قطعات (۱۴) کوچکتر تقسیم می‌شود. عمل رمز با جابه‌جا کردن این بخش ها در داخل هر فریم به‌انجام می‌رسد (شکل ۴). در اینجا نیز یک درهم‌ریزنده (۱۵) با استفاده از یک رشته شبه‌اتفاقی عمل درهم‌ریختن قطعات را به‌انجام می‌رساند. این روش، شاید بتواند مهمترین روش رمز با استفاده از پردازش آنالوگ نامیده شود. پیچیدگی و تعداد حالات ممکن رمز در این روش بستگی به‌طول فریم و تعداد قطعات موجود درآن دارد. چنانچه تعداد این قطعات در هر فریم m نامیده شود، تعدادحالات ممکن جابه‌جایی برابر m! خواهد بود. مثلا" برای $m = 10$ خواهیم داشت: $۱۰! = ۳۶۲۸۰۰۰$ m!

در اینجا نیز محدودیت‌هایی از نظر طول فریم، طول قطعات و تاخیر ایجاد شده در سیگنال وجود دارد که بعدا" در مورد آن‌صحبت خواهد شد. اگرچه سایر روش های رمز زمانی نیز موجودند که کم و بیش در رمز سیگنالها از آنها استفاده می‌شود. ولی به‌علت اهمیت کمتر آنها نسبت به‌روش اخیر، از ذکر آنها صرفنظر می‌گردد.

۵. رمز سیگنال های آنالوگ با استفاده از پردازش دیجیتال:

روش های دیجیتال‌در رمز کردن سیگنالهای‌آنالوگ روش هایی نسبتا" جدید و متنوع هستند. روش هایی نیز موجودند که به‌جای انجام عمل رمز برروی‌سیگنال دیجیتال شده، تنها برروی سیگنال منفصل عمل پردازش را انجام می‌دهند. در این قسمت از این روش‌ها نیز سخنی به‌میان آورده خواهد شد. توجه به‌روش های مهم تبدیل آنالوگ به‌دیجیتال و انتقال آن شرط اولیه بررسی روشهای رمز با استفاده از پردازش دیجیتال می‌باشد. یکی از معمول‌ترین روش‌ها در این جهت روش PCM (۱۶) است. در این روش ابتدا از سیگنال آنالوگ اولیه نمونه‌برداری شده و سپس نمونه‌های به‌دست آمده به یک کدچند بیتی دیجیتال تبدیل می‌گردند این کدها سپس به‌صورت یک سری پالس به‌طرف مقابل ارسال می‌شوند. در این صورت، سیگنالی با پهنای باند KHz ۴، طبق تئوری نمونه‌برداری‌حداقل باید با فرکانس KHz ۸ نمونه‌برداری شود چنانچه هر نمونه با ۸ بیت نمایش داده شود. نرخ بیت به‌دست آمده جهت ارسال برابر Kbits / s ۶۴ خواهد بود که حداقل به‌فرکانسی برابر KHz ۳۲ نیاز خواهد داشت.

بنابراین ملاحظه گردید که پهنای باند مورد نیاز کانال، برای استفاده از این روش، ۸ برابر خواهد شد و هرگونه کاهشی در این مقدار موجب کاهش کیفیت سیگنال ارسالی می‌گردد.

درروش دیگر که به‌روش مدولاسیون Δ (۱۷) موسوم است. سیگنال کد شده با استفاده از یک مجموعه پالس با فاصله زمانی T که می‌تواند دارای مقدار بالا یا پایین باشند نمایش داده می‌شود (شکل ۵). روش دیگری که برای ارسال سیگنال های صوتی (و نه تمام سیگنال های آنالوگ) به‌کار می‌رود، استفاده از Vocoder است. در این روش برخی مشخصات صوتی گوینده از قبیل فرکانس اصلی ایجاد شده توسط تارهای صوتی وی، مشخصات فیلتری مجاری صوتی و غیره تعیین شده وبه‌طرف مقابل ارسال می‌گردد. درگیرنده سعی می‌شود باایجاد فرکانس اصلی و ساختن سایر مشخصات لازم توسط فیلترهای دیجیتال صوت

اولیه بازسازی گردد این‌روش، روشی نسبتا" جدید بوده و هنوز از کیفیت مناسبی برخوردار نیست.

برای اعمال رمز به‌این سیگنال های دیجیتال شده، می‌توان از روش های ساده استفاده نمود. به‌عنوان مثال می‌توان پالس های به‌دست آمده از خروجی‌یک مدولاتور Δ را که به‌صورت یک رشته پالس مثبت یا منفی و با فاصله یکسان هستند، با استفاده از روش TDM جابه‌جا نمود. این کار درمورد سیگنال PCM نیز با تقسیم‌بندی آن به بلوک‌های n بیتی قابل انجام است (nتعداد بیت به‌کار رفته در تبدیل یک نمونه آنالوگ به‌دیجیتال است). از جمله دیگر روش های معمول در رمز کردن اطلاعات دیجیتال، استفاده از روش رمز جاری (۱۸) است. در این روش یک رشته شبه‌اتفاقی که با روش های معمول برای‌ایجاد این رشته‌ها ساخته می‌شود، با اطلاعات دیجیتال جمع مدول ۲ می‌گردد. این عمل باعث می‌شود که یک مجموعه اطلاعات رمز شده به‌دست آید که به‌کلی با اطلاعات اولیه ما متفاوت باشد. همچنین برای رمز کردن این اطلاعات می‌توان از روش رمز با فیدبک (۱۹) استفاده نمود. در این روش رشته به‌دست آمده از جمع یک رشته شبه اتفاقی با اطلاعات رمز شده وارد یک رجیستر شده و به‌عنوان فیدبک بار دیگر برروی رشته خروجی اثر می‌گذرد. شکل ۶ بلوک دیاگرام یک سیستم رمزکننده‌سیگنال آنالوگ با استفاده از روش رمز با فیدبک را نشان می‌دهد.

روش های مختلف دیگری نیز وجود دارند که به‌کمک آنها می‌توان رشته اطلاعات دیجیتال به‌دست آمده از تبدیل سیگنال آنالوگ به دیجیتال را رمز نمود که در اینجا از ذکر آنها صرفنظر می‌گردد.

همان‌طورکه پیش از این نیز اشاره شد، غیر از روش‌های فوق، روش های دیگری نیز وجود دارند که برروی نمونه‌های به‌دست آمده از سیگنال‌آنالوگ، عمل رمز را به‌انجام می‌رسانند. این روش ها که به روش های Sample – based موسومند اخیرا "کاربرد فراوانی یافته‌اند.

یکی از ساده‌ترین این روشها، روش درهم ریختن نمونه‌ها (۲۰) می‌باشد. در این روش یک بلوک از نمونه‌های انتخاب شده و نمونه‌های موجود در آن دچار درهم‌ریختگی می‌گردند. روش مهم‌تر و جالب‌تری که در این زمینه موجود است، استفاده از تبدیل منفصل فوریه یا DFT (۲۱) می‌باشد. در این شیوه ابتدا ضرایب DFT برای یک سیگنال نمونه‌برداری شده به‌دست آورده شده و سپس بااستفاده از یک‌ماتریس درهم‌ریختگی این نمونه‌ها درهم‌ریخته و باردیگر به حوزه زمانی بازگردانده می‌شوند. ماتریس های مورد استفاده در تبدیل، و تبدیل معکوس فوریه، می‌توانند توسط روش های معمول FFT (۲۲) به‌دست آیند.

روش های فراوان دیگری نیز در این زمینه‌ها موجودند که در این مقاله امکان بررسی تمامی آنها نمی‌باشد.

۶. کاربرد تکنیک‌های دیجیتال در پردازش‌آنالوگ:

پیش از ادامه بحث و مقایسه روش های مختلف رمز لازم است از اسفاده از تکنیک دیجیتال در رمزهای با پردازش‌آنالوگ‌نیز یاد نمود. سادگی استفاده ارزانی و قدرت فراوان سیستم‌های دیجیتال موجب گشته که امروزه حتی‌در استفاده از پردازش آنالوگ در سیستم‌های رمز کننده نیز، به‌تکنیک دیجیتال توسل جست. شاید این مطلب باعث گردد که شبهه‌ای در مورد آنالوگ یا دیجیتال بودن پردازش در ذهن خواننده به‌وجود آید. لذا لازم است یک‌بار دیگر در مورد اصل مساله پردازش به‌صورت آنالوگ و یا دیجیتال توضیح داده شود.

در استفاده از پردازش آنالوگ برای رمز سیگنالهای آنالوگ، منظور ما این نیست‌که سیگنال در طول عمل‌آنالوگ باقی‌مانده و عمل‌پردازش مستقیما" برروی آن انجام می‌گیرد، بلکه منظور آن است که پردازش، یک پردازش آنالوگ‌است و مستقیما" برروی سیگنال در حوزه زمان یا در حوزه فرکانس اثر می‌گذارد. حال ممکن است راحت‌تر باشد که این عمل به‌صورت دیجیتال انجام شود. بنابراین چنین پردازشی، دیجیتال نبوده، بلکه پردازش آنالوگ است که با استفاده از تکنیک دیجیتال انجام شده، مثالی برای این مساله می‌تواند انجام جابه‌جایی زمانی قطعات در داخل یک فریم در روش TDM باشد، چنین عملی به‌صورت دیجیتال به‌راحتی قابل انجام است چرا که برای جابه‌جایی قطعات لازم است ابتدا آنها را درحافظه‌ای ذخیره نمود وسپس اقدام به‌جابه‌جا کردن آنها کرد.

متقابلا "روش های استفاده از پردازش دیجیتال در رمز سیگنال آنالوگ مستقیما" برروی سیگنال عمل ننموده بلکه با استفاده از روش هائی ویژه، پردازش دیجیتال را برروی سیگنال اعمال می‌نمایند. در واقع پردازش با استفاده از خواص سیگنال‌های دیجیتال انجام می‌گیرد.

با این همه، و به‌علت فراوانی گونه‌های رمز در هر دو روش فوق و شباهت برخی از این گونه‌ها در دو روش فوق با یکدیگر، شاید جدا سازی آنها از یکدیگر به‌خصوص در برخی از موارد خاص، کار مشکلی باشد، در هر صورت شاید بهتر باشد به‌این نکته اشاره شود که عموما" در پایان یک پردازش آنالوگ سیگنال به‌صورت آنالوگ به‌طرف دیگر مکالمه ارسال‌می‌شود، ولی در پایان یک پردازش دیجیتال، معمولا سیگنال دیجیتال به‌طرف دیگر انتقال می‌یابد.

نکته دیگری که در اینجا باید مورد اشاره قرار گیرد، استفاده از ریزپردازنده در هر دو نوع سیستم‌های فوق است. پیشرفت علم دیجیتال و معرفی ریز پردازنده‌ها طی سالهای اخیر تحولات شگرفی را در تمامی شاخه‌های صنعت، منجمله خود صنعت الکترونیک موجب گشته است. این واحدهای پردازشگر کوچک ولی پرقدرت توانسته‌اند به راحتی‌جایگزین بسیاری از قسمتهای پیچیده مورداستفاده در سیستم‌های مختلف گردند. از جمله در رمز کننده‌ها نیز استفاده از ریزپردازنده موجب گشته که علاوه بر کاهش فراوان در حجم سخت‌افزار مورد نیاز برای ساختن این سیستم‌ها، قابلیت آنها نیز افزایش فراوانی پیدا کند، به‌ویژه در سالهای اخیر که قدرت ریزپردازنده‌ها افزایش فراوانی یافته و سیستم‌های کامپیوتری ساخته شده توسط آنها قابلیت‌هایی در حد کامپیوترهای کوچک (۲۳) ارائه می‌دهند. استفاده از آنها در این گونه سیستم‌های ایمنی تبادل اطلاعات به‌شدت رو به گسترش است.

همچنان‌که گفتیم تکنیک دیجیتال در پردازش‌آنالوگ سیگنال ها نیز کاربرد دارد و بنابراین می‌توان انتظار داشت که ریزپردازنده‌ها با قدرت بالای فعلی نیز علاوه بر مورد استفاده واقع شدنشان در پردازش دیجیتال در روش هایی که از پردازش آنالوگ استفاده می‌نمایند نیز به‌کار گرفته شده و به‌شدت مورد توجه باشند. قدرت‌فراوان آنها به‌خصوص در محاسبات Real – time موردنیاز این سیستم‌ها

می‌توانند به‌کار آیند.

۷. مقایسه روش‌های مختلف رمز:

روش های بررسی شده در این مقاله هریک دارا مزایا و معایبی می‌باشند که موجب می‌گردد استفاده از آن روش بیشتر یا کمتر انجام شود. مشخصاتی که یک سیگنال رمز شده باید ارائه نماید تا از نظر استفاده قابل قبول باشد، به‌این ترتیب قابل بیانند:

الف ــ حداقل‌وضوح باقیمانده در سیگنال رمز شده که‌باعث می‌گرددفهم آن توسط شنونده کمتر شود.

ب ــ حداقل افزایش پهنای باند که در بعضی‌موارد بسیار مهم و غیر قابل اغماض است.

پ ــ حداقل میزان تاخیر ایجاد شده.

ت ــ حداقل نویزپذیری و انتقال خطا.

ث ــ سایر مسائل از قبیل قیمت تمام‌شده، امکان ساخت آن با توجه به‌تکنولوژی موجود، حجم سیستم ساخته شده و غیره.

حال وجود این شرایط‌را در روش هایی که توضیح داده شد بررسی می‌نماییم. روش معکوس کردن فرکانسی که به‌عنوان یکی از روش های رمز آنالوگ‌مطرح گردید اگرچه از نظر ساخت ساده بوده، روشی ارزان قیمت بشمار رفته، پهنای باند را افزایش‌نداده، و نسبت به‌مسائل خط‌انتقال مانند نویز و غیره مشابه سیگنال معمولی عمل می‌نماید، ولی دارای چند اشکال مهم است. اول آن که رمز فوق تنها به‌یک صورت قابل انجام است و چنانچه کسی نوع رمز را بداند به‌راحتی می‌تواند آن را بگشاید. دوم آن که وضوح باقیمانده در این نوع رمز بسیار زیاد بوده و به هیچ وجه قابل قبول نمی‌باشد. حتی در نوع معکوس کردن و انتقال باند دوره‌ای نیز علیرغم محسنات مشابهی که دارد این عیب موجود بوده و بنابراین این روش ها تنها به‌عنوان روش های خصوصی کردن اطلاعات قابل استفاده بوده و در مورد رمز تنها با ترکیب با سایر شیوه‌ها برای بالاتر بردن قدرت رمز آنها قابل استفاده‌اند.

روش درهم‌ریختگی باند فرکانسی نیز دارای مزایایی از جمله عدم افزایش پهنای باند و عدم تاثیر زیاد نویز برآن می‌باشد. اما این روش نیز دارای وضوح باقیمانده در سیگنال رمز به‌میزان غیرقابل قبولی است (به‌خصوص اگر عمل معکوس کردن فرکانسی درآن انجام نگیرد). بنابراین، این شیوه نیز می‌تواند به‌عنوان پیچیده‌تر کننده رمز به‌همراه سایر روش ها به‌کار رود. مساله دیگر در مورد این روش عدم امکان وجود بیش از چهار یا پنج زیرباند فرکانسی به‌خاطر مسایل مربوط به فیلتر کردن می‌باشد که پیچیدگی رمز را محدود می‌نماید.

روش رمز TDM یا TSP که یکی از مهمترین روش های رمز زمانی است، برخلاف روش‌های فوق می‌تواند بر پهنای باند سیگنال اثر بگذارد. بنابراین در این روش انتخاب زمان فریم و قطعات داخل آن بسیار مهم است. تاخیر بوجود آمده در سیگنال که یکی از معایب این روش است باعث محدودیتهایی از نظر کار می‌گردد. بسته به‌مورد استفاده، تاخیر قابل قبول می‌تواند تغییر کند و حداکثر طول فریم نباید از نصف تاخیر مجاز بیشتر باشد، در ضمن باید تاخیرهای دیگر ناشی از کار سیستم نیز در این محدود گنجانده شود. افزایش طول قطعات داخلی‌موجب‌اشکالاتی از قبیل کاهش پیچیدگی رمز و کاهش طول آنها، موجب افزایش پهنای باند سیگنال می‌گردد. به‌همین جهت در این روش محدودیتهای فراوانی وجود دارند که باید با توجه به‌آنها بهترین حالت را انتخاب نمود. مساله وضوح باقیمانده در این روش نیز مطرح می‌باشد ولی میزان آن نسبت به‌روش های قبلی بسیار کمتر است. بررسی های انجام شده برروی روش های مختلف رمزهای با استفاده از پردازش‌آنالوگ نشان داده‌اند که ترکیب روش درهم‌ریختگی فرکانسی و معکوس کردن فرکانسی با روش TSP که اصطلاحا" روش TFSP (۲۴) خوانده می‌شود بهترین نتیجه را از نظر مشخصات مختلف رمز به‌دست خواهد داد. شکل ۷ بلوک دیاگرام یک سیستم رمز کننده بااستفاده از روش TFSP برروی‌یک خط تلفن را نشان می‌دهد.

بررسی روش های دیجیتال نشان‌داده است که روش های PCM و Δ–mod. عموما" باعث می‌گردند که به‌علت استفاده از سیگنال دیجیتال در انتقال اطلاعات نویز به سیستم اضافه شود. همچنین هر دو روش فوق نیاز به‌نرخ انتقال اطلاعات بالایی‌دارند که پهنای باند را به‌شدت افزایش می‌دهد. مساله وضوح باقیمانده در سیگنال رمز به‌علت اعمال روش های رمز برروی سیگنال دیجیتال اصولا" مطرح نمی‌باشد. راههایی برای کاهش نرخ بیت لازم برای این سیگنال ها به وجود آمده‌اند که عبارتند از: ADM ( )، APCM ( ) ADPCM ( ). ولی، کماکان نرخ بیت لازم برای استفاده از این روش ها بسیار بالا می‌باشد. مساله دیگری که این روش‌ها نسبت به آن حساس می‌باشند، نویز کانال ارتباطی می‌باشد که‌این مساله به‌خصوص برای PCM بیشتر از مدولاسیون Δ می‌باشد.

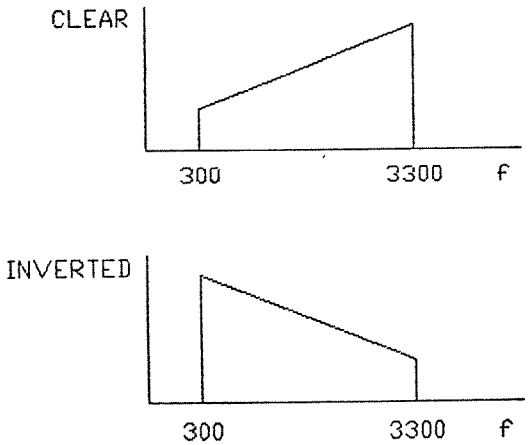
استفاده از Vocoder ها در کد کردن سیگنال صوتی‌و سپس رمز کد اخیر موجب کاهش نرخ بیت در حدود 1.2–4.8 Kbits/s می‌گردد که برای سیگنال صوتی مناسب است. اما پیچیدگی فراوان این سیستم‌ها و نیز کیفیت پایین صدای به‌دست آمده از آنها که کاملا" مصنوعی می‌باشد باعث می‌گردد تا استفاده از Vocoder تا پیشرفت بیشتر در تکنولوژی به‌عهده تعویق سپرده شود.

روش های Sample – based اگرچه نسبت به‌سایر روش های دیجیتال مزایایی را ارائه می‌دهند ولی به‌علت‌جدید بودنشان هنوز استفاده زیادی در سیستم‌های رمز نیافته‌اند. از جمله معایب این روش ها، نیاز به‌افزایش پهنای باند در اکثر این روش هاست. و برخی از آنها نیز که پهنای باند فرکانسی را افزایش نمی‌دهند عموما" از ضعف آلگاریتم رنج می‌برند. از دیگر معایب آنها می‌توان وابستگی بسیار زیاد سیگنال صوتی (از نظر ریاضی) به نمونه‌های مورد انتقال را نام برد که موجب می‌گردد که هرگونه نویزی در کانال ارتباطی اثرات بسیار نامطلوبی برروی سیگنال صوتی به‌جا بگذارد. همچنین اغلب این‌روش ها نیاز به‌مدارهای خاص و پیچیده‌ای برای پردازش سیگنال دیجیتال دارند که موجب حجیم‌و گرانتر شدن سیستم می‌گردد و برای رفع این مشکل نیاز به‌پیشرفت بیشتر تکنولوژی و به وجود آمدن مدارهای مجتمع با قابلیت‌های بیشتر می‌باشد.

۸. نتیجه

آنچه در این مقاله مورد بررسی قرار گرفت، روش های مختلف رمز کردن سیگنال آنالوگ توسط پردازش آنالوگ یا دیجیتال بود. مقایسه به‌عمل آمده در این مقاله نشان داد که علیرغم پیشرفت فراوان در تکنیک‌های دیجیتال و روش های رمز نوینی که براساس پردازش دیجیتال به‌وجود آمده‌اند، آنچه اکنون به‌عنوان یک روش

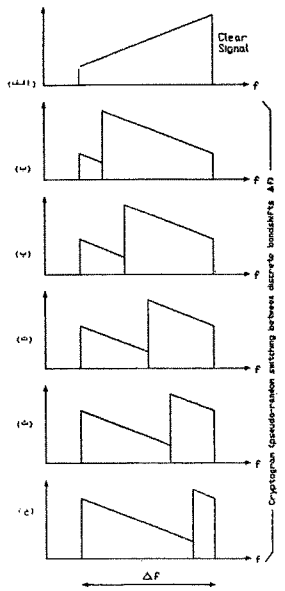
مطمئن و قابل قبول قابل استفاده می‌باشد، بیشتر می‌تواند در محدوده پردازش آنالوگ باشد تا پردازش دیجیتال، بررسی مشخصات مختلفی که برای سیگنال رمز شده تعریف می‌گردند، نشان می‌دهدکه برای داشتن کمترین افزایش درپهنـای بانـد، کمترین وضوح باقیمانده درصوت، کمتریـن نویـزپذیـری در خـط انتقـال، و حـد بالایی از امنیت در



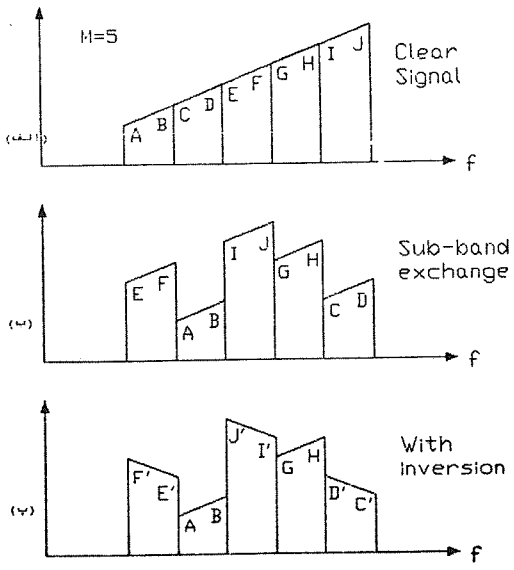
شکل ۱ – روش معکوس کردن فرکانسی

استفاده از بعضی از روش های رمز با استفاده از پردازش دیجیتال به کمک مدارهای مختلف خاص می‌تواند باعث بالاتر رفتن کیفیت رمز از نظر پیچیدگی گردد.

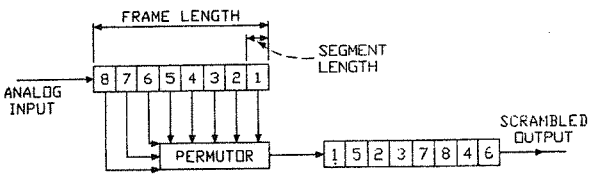
بنابراین در اغلب موارد که محدودیت های فوق موجودند، بهترین نتیجه بااستفاده از سیستم‌های دیجیتالی و ریزپردازنده‌های قوی در پردازش سیگنال آنالوگ برای‌داشتن بالاترین پیچیدگی رمز، به‌دست خواهد آمد.



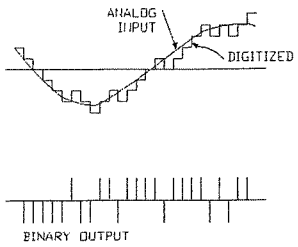
شکل ۲– روش معکوس کردن و انتقال دوره‌ای



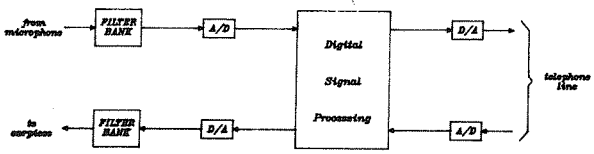
شکل ۳– روش درهم‌ریختن باند فرکانسی بهمراه معکوس کردن



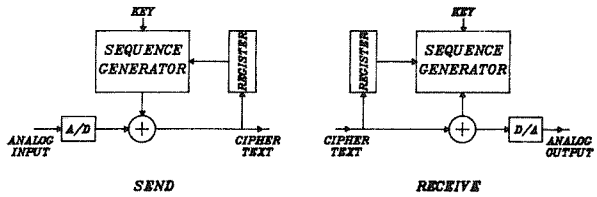
شکل ۴ – TDM



شکل ۵ ــ مدلاوسیون دلتا



شکل ۷ ــ بلوک دیاگرام یک سیستم رمز کننده با استفاده از روش TFSP بروی خط تلفن



شکل ۶ ــ بلوک دیاگرام یک سیستم رمزکننده سیگنال آنالوگ با استفاده از روش رمز با بازخورانی (فیدبک)

پاورقی

1. Privacy.
2. Residual Intelligibility.
3. Encoding Delay.
4. Bandwidth Expansion.
5. Frequency Inversion.
6. Bandshift and Inversion.
7. Pseudo –Random.
8. Cyclic Bandshift and Inversion.
9. Band Scrambling.
10. Sub – Bands.
11. Time Segment Permutation (TSP).
12. Time Division Multiplexing.
13. Frame.
14. Segments.
15. Permutor.
16. Pulse Code Modulation.
17. Delta Modulation.
18. Stream Cipher.
19. Cipher Feedback System.
20. Sample Permutation.
21. Discrete Fourier Transform.
22. Fast Fourier – Transform.
23. Minicomputers.
24. Time and Frequency Segment Permutation.
25. Adaptive Delta Modulation.
26. Adaptive Pulse Code Modulation.
27. Adaptive Differential Pulse Code Modulation.

منابع :

1. H.Beker, F.Piper, "Cipher Systems," LONDON: Northwood publications, 1982.
2. W.Diffie, M.E.Hellman, "Privacy and Authentication: An Introduction to Cryptography," proceedings of the IEEE, Vol. 67, No.3, pp. 397–427, March 1979.
3. K.H.Kirchhofer, "Secure Voice Communication–Cryptophony," International Defense Review, Vol. 9, No.5, pp. 761-767, Sept. 1976.
4. N.S.Jayant, B.J.McDermott, S,W.Christensen, A.S.Quinn, "A Comparison of Four Methods for Analog Speech Privacy, "IEEE Trans, Comm., Vol. Com–29, No.1, pp. 18–23, Jan. 1981.
5. H.J.Beker, "Cryptographic Requirements for Digital Secure Speech–Systems, "Electronic Engineering, "pp. 37–46, FEB. 1980.