دومین کنفرانس انجمن رمز ایران
دانشگاه صنعتی شریف
۳۰-۲۹ مهر ماه ۱۳۸۲

آزمون خود همبستگی قالبها

بهروز پی زری(دانشجوی کارشناسی ارشدمخابرات دانشگاه صنعتی اصفهان)
b_peyzari@hotmail.com

محمد دخیل علیان(استادیار دانشگاه صنعتی اصفهان)
mdalian@cc.iut.ac.ir

چکیده: آزمونهای آماری ابزاری جهت بررسی خواص تصادفی دنباله های شبه تصادفی می باشد.در آزمونهای آماری هدف بررسی میزان شباهت دنباله های شبه تصادفی به دنباله ایده ال یعنی دنباله با توزیع یکنواخت که اعضای آن تؤاما مستقل هستند،می باشد.یکی از ویژگی های مهم در بررسی دنباله های شبه تصادفی میزان خود همبستگی اعضای دنباله می باشد.بر همین اساس در[۴] آزمونهای آماری برای سنجش میزان خود همبستگی اعضای دنباله ارائه شده است.یکی دیگر از ویژ گیهای مهم خود همبستگی زیر قالبهای دنباله شبه تصادفی می باشد.در این مقاله با نگرش مطرح شده در[۴]برای خود همبستگی دنباله های باینری ،خود همبستگی قالبها در یک دنباله باینری مورد بررسی دقیق قرار گرفته است و با بدست آوردن مدل احتمال آن از دو دیدگاه آزمونهای آماری جدیدی بر مبنای آن ارائه گردیده است.

واژگان کلیدی: خودهمبستگی ،دنباله های شبه تصادفی،آزمونهای آماری[1]

۱.مقدمه

ارزیابی آماری دنباله های شبه تصادفی در بررسی و تجزیه و تحلیل الگوریتمهای رمزنگاری از اهمیت و جایگاه خاصی بر خوردار می باشند. در واقع دنباله های تولید شده توسط الگوریتمها از دیدگاه تئوری اطلاعات باید از حداکثر بی نظمی و حداکثر آنتروپی بر خوردار باشندو برای نیل به این هدف در یک حالت ایده ال این دنباله ها باید دارای توزیع یکنواخت با اعضای تؤاما مستقل باشندو لی به دلیل اینکه در عمل تولید دنباله های ایده ال میسر نمی باشد مجبور به تولید و استفاده از دنباله های به اصطلاح شبه تصادفی می باشیم. هدف از آزمونهای آماری بررسی میزان نزدیکی دنباله های تولید شده با حالت ایده ال می باشد.در آزمونهای آماری با بدست آوردن مدل احتمال برای ویژگیهایی چون تعداد یکها،تعداد

[1] Statistical Testing