ارائه یک چارچوب جدید برای رمزنگاری اطلاعات با تبدیل اطلاعات به تصویر در شبکه های حسگر بیسیم

مهدی قاضی زاده [۱]، سید مصطفی مکی [۲]، حمید رضا ناجی [۳]

[۱] دانشجوی کارشناسی ارشد، گروه فناوری اطلاعات، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته ، m.ghazizadeh.in@gmail.com
[۲] دانشجوی کارشناسی ارشد، گروه فناوری اطلاعات، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته ، seyedmostafamakki@gmail.com
[۳] استادیار، گروه فناوری اطلاعات، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته ، hamidnaji@ieee.org

چکیده

شبکه‌های حسگر بیسیم دارای کاربردهای وسیعی می‌باشند و با توجه به اینکه گره‌های حسگر همواره در محیط‌های متخاصم توزیع می‌شوند، نیاز به تامین امنیت این شبکه‌ها بسیار ضروری می‌باشد. در این مقاله هدف ما در نظر گرفتن محرمانگی داده ها در شبکه‌های حسگر بیسیم، ارائه یک چهار چوب امنیتی جدید بوده است. در این روش داده ها به صورت کدهای اسکی تبدیل گردیده و با مکانیزمی آنها را رمزگذاری اولیه نموده و سپس داده‌ها با استفاده از تابع Hash رمزگذاری دوم برای افزایش امنیت بیشتر صورت می گیرد. در نهایت با استفاده از استاندارد رنگ RGB و تبدیل کدهای رمزگذاری شده به کدهای رنگی و وارد نمودن آنها در یک ماتریس، تصویر نهایی که رمزشده داده‌های اولیه می‌باشد را تولید می‌نماید. با توجه به نتایج تحلیل انجام شده، روش ارائه شده دارای حجم محاسبات پایین‌تر، مصرف انرژی کمتر و امنیت بالاتر نسبت به روش های بررسی شده می‌باشد.

کلید واژه ها

شبکه حسگر بی‌سیم، داده در تصویر، رمزنگاری، امنیت، تبدیل داده به تصویر، رمزنگاری، Hash

۱-مقدمه

الگوریتم رمزنگاری، به هر الگوریتم یا تابع ریاضی گفته می‌شود که به علت دارا بودن خواص مورد نیاز در رمزنگاری، در پروتکل‌های رمزنگاری مورد استفاده قرار گیرد. اصطلاح الگوریتم رمزنگاری یک مفهوم جامع است و لازم نیست هر الگوریتم از این دسته، به طور مستقیم برای رمزگذاری اطلاعات مورد استفاده قرار گیرد، بلکه صرفاً وجود کاربرد مربوط به رمزنگاری مد نظر است.

در گذشته سازمان‌ها و شرکت‌هایی که نیاز به رمزگذاری یا سرویس‌های دیگر رمزنگاری داشتند، الگوریتم رمزنگاری منحصربه‌فردی را طراحی می‌نمودند. به مرور زمان مشخص گردید که گاهی ضعف‌های امنیتی بزرگی در این الگوریتم‌ها وجود دارد که موجب سهولت شکسته شدن رمز می‌شود. به همین دلیل امروزه رمزنگاری مبتنی بر پنهان نگاه داشتن الگوریتم رمزنگاری منسوخ شده‌است و در روش‌های جدید رمزنگاری، فرض بر این است که اطلاعات کامل الگوریتم رمزنگاری منتشر شده‌است.

پیشرفت‌هایی که در سال‌های اخیر در زمینه ساخت و طراحی ریز پردازنده‌ها و ابزارهای ارتباط بیسیم بوجود آمده است، توانایی فنی و اقتصادی لازم جهت تولید گره‌های حسگر کوچک و ارزان قیمت را فراهم نموده است[۱]. این حسگرهای کوچک شامل یک پردازنده، یک حسگر،