عنوان مقاله:
سیستم مبادله اطلاعات امن مبتنی بر پنهان نگاری با قابلیت دسترسی چند سطحی

محل انتشار:
نهمین کنفرانس بین‌المللی انجمن رمز ایران (سال: 1391)

تعداد صفحات اصل مقاله: 7

نویسندگان:
سعید آهون منش - *آزمایشگاه امنیت داده ها و ارتباطات، گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد، مشهد*

عباس قایمی بافقی - *آزمایشگاه امنیت داده ها و ارتباطات، استادیار، گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد، مشهد*

احمد طوسی - *گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد، مشهد*

خلاصه مقاله:
با پیشرفت فن آوری اطلاعات نیاز به انتقال اطلاعات به صورت امن بسیار افزایش پیدا کرده است. یکی از راه های امن و مخفیانتقال اطلاعات استفاده از پنهان نگاری است. ما در این مقاله با استفاده از پنهان نگاری، سیستمی ارایه داده ایم که قادر به انتقالاطلاعات با قابلیت دسترسی چند سطحی و حجم زیاد است. با استفاده از روش گسترش تفاضل چند لایه بهبود داده شده توانستیمچندین پیام با دسترسی های متفاوت را در رسانه پوشش جاسازی نماییم که باعث به وجود آمدن یک سیستم مبادله اطلاعات امنمی گردد. نتایج پیاده سازی ظرفیت بالاتری را نسبت به سیست مهای مشابه نشان می دهد. همچنین با توجه به اضافه کردن کدتصدیق اصالت به پیا مها، سیستم ما دارای قابلیت اطمینان بیشتری نیز است. از این سیستم می توان در کاربردهای مهم نظامی وپزشکی که دارای ساختاری سلسله مراتبی هستند استفاده نمود.

کلمات کلیدی:
پنهان نگاری، گسترش تفاضل، کنترل دسترسی، مدیریت کلید، چند سطحی