INTERNATIONAL CONFERENCE ON
RESEARCH IN SCIENCE AND TECHNOLOGY
14 December 2015, Kualalumpur –Malaysia

نهان نگاری متن در تصاویر دیجیتال به کمک نگاشت های آشوبگون

الناز قاسمی
کارشناسی ارشد، دانشکده فنی و مهندسی ،دانشگاه آزاد واحد آیت الله آملی ،آمل،
elnaz.ghsemi64@gmail.com

علی برومندنیا
استادیار، دانشکده فنی و مهندسی،دانشگاه آزاد واحد تهران جنوب ،تهران
broumandnia@gmail.com

چکیده
در نهان نگاری هدف حفاظت از اطلاعات پنهان شده از دسترس مهاجمین است. درصورتیکه یک ویژگی محرمانه در کانال ارتباطی به صورت آشکار منتقل شود بدیهی است مورد حمله قرار خواهد گرفت، هدف ازاین پژوهش انتقال امن اطلاعات سری است. جهت داشتن یک نهان نگاری تنومند از نگاشتهای آشوبگون استفاده شده است، زیرا برخلاف روشهای کلاسیک، الگوریتمهای مبتنی برآشوب راه حلهای ساده و کم هزینه ای برای حل مشکل امنیت ارائه میدهد. نتایج شبیه سازی نشان داد نسبت نویز به سیگنال تصاویر بین ۴۲/۱۳ و ۴۲/۶۶ بود که نسبت به روش مقایسه شده نتایج بهتری را نمایش داد. همچنین ظرفیت جاسازی ۱۰۲۴ بیت بود. پارامتر TAF مقدار ۰ را برگرداند که نشان دهنده ی بازیابی کد QR بدون هیچگونه تغییری است. میزان آنتروپی تصویر استگو مقادیر بین ۷/۱۲ و ۷/۶۴ را بازگرداند که بسیار به مقدار ایده آل که عدد ۸ است نزدیک بود . بررسی های کیفی نشان داد در روش پیشنهادی کیفیت رسانه حامل در حد قابل قبولی حفظ شده است. همچنین در بخش تست امنیت مشخص شد بخاطر استفاده از کد QR و نگاشت آشوب روش پیشنهادی از امنیت بسیار بالایی برخوردار است.

واژگان کلیدی: نهان‌نگاری، نگاشت آشوب ، کد QR، TAF ، آنتروپی.

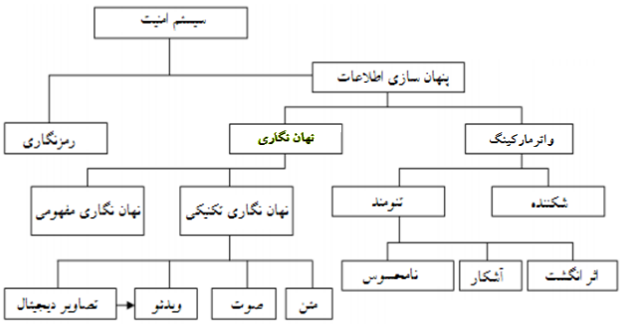
مقدمه

با توجه به گسترش فناوری و امکان انجام عملیات از راه دور، همچنین عدم لزوم تمرکز همه داده‌ها در یک محل و نیاز به حفظ امنیت اطلاعات در زمان ارسال و دریافت، اهمیت مسئله نگهداری اطلاعات از دسترسی های غیر مجاز بیش از پیش آشکار می شود(Altaay et al,2012) . باتوجه به اینکه امروزه روش های زیادی برای ارسال امن اطلاعات در بستر فضای مجازی وجود دارد استفاده از روش های نهان نگاری می تواند کمک شایانی جهت ارسال و دریافت داده ها نمایند (Anderson et al, 1998). در بسیاری از مقالات برای بالا بردن امنیت از محاسبات طولانی و وقت گیر استفاده می کنند، برخلاف اکثر روش های کلاسیک، الگوریتم هایی که بر مبنای سیستم های آشوب طرح می شوند، روش کاملاً متفاوتی را برای حل مشکلات امنیت ارائه می کنند. این الگوریتمها اغلب بسیار ساده بوده و هزینه های محاسباتی کمی دارند. استفاده از نگاشت آشوب در عین سبک بودن الگوریتم امنیت بالاتری را شامل می شود (اسمعیلی،۱۳۹۳).

در سالهای اخیربسیاری از روشهای نهان نگاری و رمزنگاری و یا ترکیبی از این دو روش مورد بررسی قرار گرفته است. در سال ۲۰۱۲ پی.آر.رودرامات و پروفسور مادکی از نگاشت لجستیک برای جاسازی با ظرفیت بالا استفاده کردند که هم کیفیت بهتری برای تصویر حامل فراهم آورد هم نرخ جایگذاری متن را بالا برد(Rudramath and Madki, 2012) . در سال ۲۰۱۴ میترا دانشمند از از لبه های تصویر و نگاشت لجستیک برای نهان نگاری متن استفاده کرد (دانشمند،۱۳۹۳) که کیفیت و سرعت جایگذاری را بالا برد. درسال ۲۰۱۵ اس.اوما ماهسواری و دی.جود همانت نهان نگاری در دامنه فرکانس بر اساس تکنیک تبدیل فوریه (FT) را مورد بررسی قرار داد (Maheswari and Hemanth, 2014) که برای ناخونا ساختن الگوریتم از متد جابجاسازی، ضرایب فوریه وکدهای QR کردند.

در این پژوهش هدف بالابردن امنیت در مخفی نمودن داده های سری است، و جهت داشتن یک نهان نگاری تنومند که مقاوم در مقابل حملات امنیتی باشد از نگاشت آشوبگون گربه آرنولد و کدهای QR استفاده شده است. همچنین در این تحقیق سعی شد در تمای مراحل نهان نگاری برای حفظ امنیت، بدون داشتن کلیدهای استفاده شده امکان کشف اطلاعات سری نباشد. در همین راستا پارامترها به گونه ای در نظر گرفته شده است که پویا بوده و شخص نهان نگارنده بتواند به آسانی کلیدهای استفاده شده در نهان نگاری را تغییر دهد.

نهان نگاری روشی است که می‌توان اطلاعات مورد نظر را در قالب یک عامل پوشاننده و با بیشترین میزان دقت به امنیت، بین نقاط موردنظر جابجا نمود ، به گونه‌ای که حتی اگر در طی مسیر، اطلاعات از طریق افراد غیرمجاز مورد دسترسی قرار گرفت امکان دستیابی به داده‌های پنهان شده وجود نداشته باشند.نهان نگاری شاخه ای از دانشی به نام ارتباطات پوشیده است. که خود شامل واترمارکینگ و رمزنگاری نیز می شود (ماهنامه دولت الکترونیکی، ۱۳۹۲) .



شکل ۱:جایگاه نهان نگاری در سیستم امنیت

در نهان نگاری می توان از تمام رسانه ها استفاده کرد. که ما در این پژوهش از تصویر برای انجام عملیات نهان نگاری استفاده کرده ایم. اطلاعات به روش های خیلی متفاوتی می توانند در عکس مخفی شوند. بوسیله رمز کردن هر بیت از اطلاعات می توان آن را مستقیما در عکس قرار داد. در روش های پیچیده تر می توان اطلاعات را فقط در قسمت هایی از عکس که پیچیدگی بیشتری دارد قرار داد تا توجه کمتری جلب کند. همچنین پیغام می تواند به شکل تصادفی در عکس پوشاننده پراکنده شود(Li et al,2011) . معمول ترین روش های مخفی کردن اطلاعات در عکس عبارتند از:

- جایگذینی بیت کم ارزش یاLSB
- ماسک ها و فیلترها روی عکس
- الگوریتم ها و تبدیلات روی عکس

ما در این پژوهش از تبدیل کوسینوسی گسسته(DCT) که زیرشاخه الگوریتم ها و تبدیلات است استفاده کرده ایم.

آشوب

آشوب از نظر لغوی به معنای هرج و مرج و بی نظمی است. اما با پیدایش نگرش جدیدی تحت عنوان تئوری آشوب تعریف آن به این شکل تغییر کرد که آشوب نوعی نظم در بی نظمی است. و پدیده ای که در یک مقیاس محلی، کاملا تصادفی و غیرقابل پیش بینی به نظر می رسد، چه بسا در مقیاس بزرگتر، کاملا پایا و قابل پیش بینی باشد. مانند: ضربان قلب، حرکت پاندولی ساعت، نوسانات اقتصادی و میزان خطای ر خ داده در یک سیستم. مزایای سیگنالهای آشوب در حساسیت نسبت به شرایط اولیه، رفتار ظاهرا تصادفی و عملکرد قطعی آن است. سیگنال آشوب رفتاری شبه نویز دارد(Gao et al, 2006) .

نگاشت گربه آرنولد

نگاشت گربه آرنولد، یکی از معروف ترین نگاشت های آشوب گون معکوس پذیر دوبعدی است. این نگاشت توضیح و بیان ساده و زیبایی از برخی اصول آشوب یعنی نظم نهفته در دگرگونی ظاهراً تصادفی یک سیستم است(Chen et al, 2004) . یک تصویر (نه لزوماً گربه) با تبدیلی برخورد می کند که ظاهراً سازمان دهی اصلی پیکسل هایش را تصادفی می کند . به‌هرحال، اگر این کار به تعداد کافی تکرار شود ، مثل اینکه با یک جادو تصویر اصلی دوباره نمایان می شود (جواهری پور، ۱۳۹۱). اگر فرض کنیم $X = \begin{bmatrix} x \\ y \end{bmatrix}$ یک ماتریس n× n از یک تصویر باشد، تبدیل آرنولد به صورت رابطه (۱) خواهد بود:

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \ mod\ n \qquad (۱)$$

نگاشت آرنولد دوبعدی می تواند به صورت زیر تعمیم داده شود :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N \qquad (۲)$$

در رابطه (۲) ماتریس کمکی است. چهار شکل از ماتریس کمکی A پیشنهاد شده است و یکی از موارد $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ، $\begin{bmatrix} bc+1 & b \\ c & 1 \end{bmatrix}$ ، $\begin{bmatrix} a & 1 \\ ad-1 & d \end{bmatrix}$ و $\begin{bmatrix} a & ad-1 \\ 1 & d \end{bmatrix}$ می تواند به عنوان ماتریس کمکی در پنهان سازی مورد استفاده قرار گیرد $\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$ (Guan et al, 2005). پارامترهای ماتریس کمکی باید به گونه ای تنظیم شوند که|A|=ab-cb=1 باشد .

کدهای پاسخ سریع

QR مخفف عبارت «کدهای واکنش سریع» است که به صورت مربعی شکل بوده ، که اطلاعات در آن به صورت نقطه های مربعی کوچک مشکی که به آن ها واحد گفته می شود، بر اساس الگوی استاندارد (ISO/IEC 18004:2006) ایجاد و می‌تواند حاوی نشانی وب، پیامک، اطلاعات تماس با فرمت کارت ویزیت، شماره تلفن، قیمت و مشخصات یک کالا به صورت همزمان باشد. کدهای QR تنها توسط ماشین قابل رمزگشایی هستند (ملک محمدی، ۱۳۹۲) .

ظرفیت ذخیره داده ها

ظرفیت ذخیره داده های در QR های کاربردی نمونه ۲ که برای آخرین نسخه این QR (۴۰) در نظر گرفته شده، به شرح جدول زیر می باشد. لازم به ذکر است که یکی از اصلی ترین ویژگی های کدهای پاسخ سریع، ظرفیت بالای ذخیره داده های مختلف است که برای اعداد ۷۰۸۹ و برای حروف پارسی حدود ۱۹۰۰ حرف می باشد (ملک محمدی، ۱۳۹۲).

جدول ۱ : ظرفیت کدهای پاسخ سریع

عددی	حداکثر ۷،۰۸۹ کاراکتر
الفبای پارسی	حدود ۱،۹۰۰ حرف
الفبای لاتین	حداکثر ۴،۲۹۶ کاراکتر
دودویی (۸ بیتی)	حداکثر ۲،۹۵۳ بایت

ظرفیت تصحیح خطا

کدهای پاسخ سریع (QR-code) از یک فناوری تصحیح خطا به نام Reed-Solomon استفاده می کند، که در سطح های مختلف توانایی آن برای رفع خطا متفاوت می باشد. به طور کلی این بارکدها از ۷ تا ۳۰ درصد قابلیت تصحیح دارند و خوانش و رمزگشایی آن‌ها دچار مشکل نمی‌شود. لازم به ذکر است که با چرخش کدهای پاسخ سریع در هر جهتی نیز می توان بدون هیچ مشکلی اطلاعات موجود در آن ها را خواند (ملک محمدی، ۱۳۹۲).

روش پیشنهادی

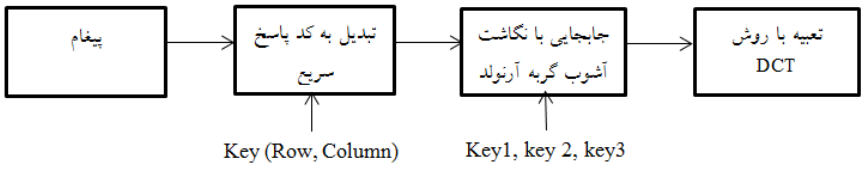
مراحل جاسازی متن در تصویر منبع در این پژوهش به ترتیب زیر است .

گام ۱: ابتدا پیغام سری را تبدیل به کد پاسخ سریع می کنیم. استفاده از QR از مزایای این پژوهش است زیرا ظرفیت بالایی دارد.

گام ۲ :پیغام سری مورد نظر که در مرحله قبل تبدیل به تصویر شد را در این مرحله با استفاده از نگاشت آشوب گربه آرنولد بهم می ریزیم. این مرحله باعث ایجاد امنیت بیشتر در مراحل انجام نهان نگاری می شود.

گام ۳ :و در آخر تصویر بدست آمده از نگاشت آشوب را توسط روش تبدیل کوسینوسی گسسته داخل تصویر منبع نهان نگاری می کنیم .

در شکل ۲ می توانید بلوک دیاگرام تعبیه متن داخل تصویر را مشاهده نمایید.



شکل۲: بلوک دیاگرام تعبیه متن داخل تصویر

تبدیل اطلاعات متنی

درابتدا پیغام متنی که قصد مخفی سازی آنرا داریم ، تبدیل به کد QR میکنیم . این روش باعث می شود که نهاننگاری از امنیت بالاتری برخوردار شود.

در این طرح از یک متن ساده استفاده شده است . در تبدیل متن به کد پاسخ سریع کلید سایز کد QR ی است که ساخته می شود. در شبیه سازی انجام شده سایز کد QR 32 در نظر گرفته شده است. این سایز به عنوان یکی از کلیدهای استفاده شده در تولید کد پاسخ سریع قابل تغییر است .

KEY(ROW,COLUMN)

در شکل ۳ متن Elnaz Ghasemi تبدیل به کد پاسخ سریع شده است. که توسط نرم افزارهای خواندن کدپاسخ سریع مانند نرم افزار QR Code Reader.apk قابل خواندن است .

شکل۳ : کد پاسخ سریع با متن Elnaz Ghasemi

استفاده از نگاشت آشوب گربه آرنولد

همان طور که گفته شد، آشوب نوعی رفتار شبه نویز است که در سیستم های غیر خطی و پویا رخ می دهد. در این پژوهش از متد نگاشت گربه آرنولد برای بهم ریختن تصویر QR تولید شده در مرحله قبل استفاده شده است.

همانطور که در فصل مربوط به تئوری آشوب ذکر شد ۴ ماتریس کمکی برای نگاشت گربه آرنولد وجود دارد (Wang et al, 2011) که در این پژوهش از ماتریس کمکی $\begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix}$ استفاده شده است .

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix} = \begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix} mod\ N \qquad (۳)$$

$$d = ab + 1 \qquad (۴)$$

پارامترهای ماتریس کمکی باید به گونه ای تنظیم شوند که |A| = ad-cb = 1 برقرار باشد (Shanthi and Bhuvaneswaran , 2014).

نگاشت با مقادیر کلیدی n=2 , a = 4 , b=1 در نظر گرفته شده است که هم هنگام اجرای نهان نگاری و هم در موقع جداسازی متن از تصویر حامل داشتن این کلیدها الزامی است.

تصویر حاصل از نگاشت رفتاری آشوبگون و شبه نویز از خود نشان می دهد. به عنوان ویژگی بسیار مهم این نگاشت می توان به عملکرد قطعی آن اشاره نمود. چرا که در عین ظاهر تصادفی این سیگنال، همواره با داشتن تابع نگاشت و مقدار اولیه می توان مجموعه مقادیری را که به ظاهر هیچ نظمی ندارند دوباره تولید کرد. این ویژگی در فرایند استگانوگرافی به منظور فراهم آوردن امنیت بیشتر و انجام معکوس عملیات برای بازیابی پیغام پنهان شده، بسیار کارامد می باشد.

تصویر زیر حاصل از ۲ بار اجرای نگاشت گربه آرنولد برروی کد QR حاصل از مرحله قبل است . که دیگر توسط ابزارهای خواندن کد QR قابل شناسایی و رمزگشایی نیست .

فضای حالت برابر {0,1,2, …, N-1} است و متغیرهای حالت، در دامنه ی صحیح از ۰ تا N-1 قرار می گیرند.

شکل ۴: تصویر حاصل از نگاشت گربه آرنولد و کلیدهای N = 2 , A = 4 , B = 1

تعبیه تصویر رمز شده داخل تصویر حامل

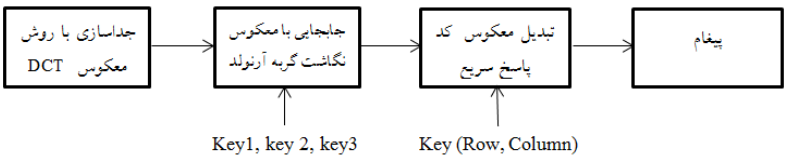
یکی از حوزه های رایج مورداستفاده برای تعبیه ی نهان نگاره، حوزه ی تبدیل کسینوسی گسسته است.
الگوریتم های نهان نگاری گوناگونی با به کارگیری این تبدیل ارائه شده اند . DCT دوبعدی یک ماتریس، ضرایب فرکانسی را به فرم ماتریسی در اختیار ما قرار می دهد. گوشه بالای سمت چپ این ماتریس جدید، ضرایب با کمترین فرکانس و گوشه سمت راست پایین، ضرایب با بالاترین فرکانس را نمایش می دهد (Singh et al, 2013) . نهان نگاری با تکنیکهای DCT در مقابل عملیات پردازش تصویر مانند فیلترینگ پایین گذر و تنظیم کنتراست، نیرومند و در مقابل در برابر حملات هندسی مانند چرخش، مقیاس گذاری و برش ضعیف هستند.
نهان نگاری با DCT میتواند به دو نوع نهان نگاری تقسیم شود(Liebling and Unser , 2004) :

- نهان نگاری DCT سراسری
- نهان نگاری DCT مبتنی بر بلوک

ما در این پژوهش از نهان نگاری DCT مبتنی بر بلوک استفاده کرده ایم .
ورودیهای مورد استفاده در تابع DCT ، تصویر رمزنگاری شده و تصویر منبع می باشند و خروجی حاصل از این عملیات ، تصویر نهان نگاری شده یا همان تصویر حامل است .

بلوک دیاگرام جداسازی متن از داخل تصویر حامل

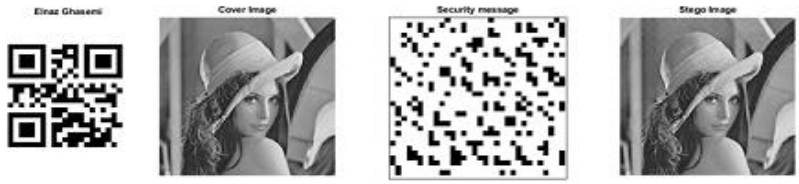
مراحل جداسازی متن از داخل تصویر حامل در این پژوهش به ترتیب زیر است .
گام۱: درابتدا باعملیات معکوس تبدیل کوسینوسی گسسته تصویر QR بهم ریخته شده توسط نگاشت گربه آرنولد را ازداخل تصویر حامل بیرون میکشیم
گام ۲ : حال با داشتن کلیدهای استفاده شده در مرحله تعبیه تصویر نگاشت شده را به حالت اصلی خود باز می گردانیم
گام ۳ : در آخر از کد QR حاصل در مرحله قبلی توسط داشتن کلید این مرحله که همان سایز کد QR است ، متن سری را استخراج می کنیم.



شکل۵: بلوک دیاگرام جداسازی متن از تصویر حامل

یافته ها

شبیه سازهای مختلفی توسط نرم افزار MATLAB برای ارزیابی روش پیشنهادی، استفاده شده است. در پیاده سازی متد پیشنهادی، از ۴ تصویراستاندارد در بحث پردازش تصویراستفاده شده است. تصاویر سیاه و سفید و باسایز ۵۱۲×۵۱۲ بوده و عبارتند از: Lena، Barbara، Baboon و Tiffany. از همین تصاویر در پیاده سازی روش تبدیل فوریه (FT) توسط اس. یوما ماهسواری و دی. جود همانت، ۲۰۱۴ استفاده شده است تا نتایج دو روش به درستی قابل مقایسه باشند.



شکل۶: از چپ به راست کد پاسخ سریع، تصویر منبع،نتیجه حاصل از آشوب و نهایتا تصویر استگو را مشاهده می نمایید.

نسبت نویز به سیگنال

نسبت نویز به سیگنال (PSNR) مقیاسی برای سنجش کیفیت تصویر استگو می باشد و با استفاده از میانگین مربعات خطا (MSE) محاسبه می شود. معادلات این دو پارامتر به صورت زیر است(Liebling et al, 2003) :

$$MSE = \frac{1}{m \times n} \sum_{x=1}^{m} \sum_{y=1}^{n} [S(x,y) - ST(x,y)]^2 \qquad (۵)$$

$$PSNR = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \qquad (۶)$$

به طوری که M و N به ترتیب تعداد پیکسل های افقی و عمودی تصویر اولیه و S(x,y) و ST(x,y) به ترتیب مقادیر پیکسل های تصویر اولیه و تصویر استگو یا تصویر حامل پیغام هستند. مقدار PSNR بالاتر معرف تصویر استگو مناسب تری است و نشان می دهد که تخریب کمتری در آن ایجاد شده است. جدول۲، مقادیر PSNR مربوط به هریک از تصاویر مورد آزمایش، در هر دو روش را مقایسه می کند.

جدول۲: مقادیر PSNR تصاویر در روش تبدیل فوریه و متد پیشنهادی

تصاویر	تبدیل فوریه	روش پیشنهادی
	PSNR	PSNR
Tiffany	41.15	42.51
Lena	41.16	42.46
Barbara	41.13	42.13
Baboon	41.16	42.66

همان طور که ملاحظه می کنید، متد پیشنهادی میزان تخریب کمتری را در تصویر بوجود آورده است.

ظرفیت جاسازی (برحسب بیت)

همان طور که در جدول ۳ مشاهده می نمایید، ظرفیت جاسازی (برحسب بیت) در روش پیشنهادی بیشتر است.

جدول ۳:ظرفیت جاسازی (برحسب بیت)

تصاویر	تبدیل فوریه	روش پیشنهادی
	ظرفیت جاسازی	ظرفیت جاسازی
Tiffany	۳۵۲	۱۰۲۴
Lena	۳۵۲	۱۰۲۴
Barbara	۳۵۲	۱۰۲۴
Baboon	۳۵۲	۱۰۲۴

آنتروپی

مفهوم آنتروپی در ارتباط با میزان بی نظمی و عدم قطعیت در یک سامانه فیزیکی می باشد. آنتروپی یک تصویر ، تخمینی از تصادفی بودن آن می باشد که به طور معمول برای سنجش میزان تیزی قله های هیستوگرام می باشد که این

موضوع مستقیماً در ارتباط با اطلاعات ساختاری با تعریف بهتر می باشد. هنگامی که نهان نگاری انجام می شود، آنتروپی بایستی نزدیک به مقدار ایده۸ آل باشد(Shannon, 1949) .
نتایج به دست آمده بسیار نزدیک به مقدار نظری ۸ هستند. این بدین معنی است که در روند نهان نگاری، نشت اطلاعات بسیار ناچیز است و روش پیشنهادی نسبت به حمله آنتروپی مصون است.

جدول ۴: آنتروپی تصاویر استگو

تصویر	Tiffany	Lena	Barbara	Baboon
اندازه	۵۱۲×۵۱۲	۵۱۲×۵۱۲	۵۱۲×۵۱۲	۵۱۲×۵۱۲
نوع	خاکستری	خاکستری	خاکستری	خاکستری
آنتروپی	۷,۱۲	۷,۴۶	۷,۶۴	۷,۳۸

فاکتور ارزیابی (TAF)

این پارامتر برای ارزیابی کیفیت تصویر منبع بعد از عملیات جداسازی مورد استفاده قرار می گیرد . برای اندازه گیری کیفیت بازیابی پیغام سری از کد QR آن ، از TAF استفاده می شود. مقدار بدست آمده از این فرمول باید بین ۰ و ۱ باشد تا کیفیت بالایی داشته باشد .

$$TAF = \frac{1}{m \times n} \sum_{x=1}^{m} \sum_{y=1}^{n} [Q(x.y) \oplus Q'(x.y)] \qquad (۷)$$

به طوریکه در رابطه (۷)، Q(x.y) و Q'(x.y) ، بترتیب مقادیر پیکسلهای کد QR پیغام سری و بازیابی شده ی کد QR پیغام سری هستند[6].

جدول۵:مقایسه دو پارامتر TAF در روش تبدیل فوریه و روش پیشنهادی

تصاویر	تبدیل فوریه	روش پیشنهادی
	TAF	TAF
Tiffany	0.87	۰
Lena	0.87	۰
Barbara	0.87	۰
Baboon	0.87	۰

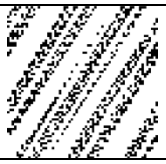
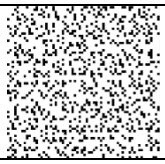
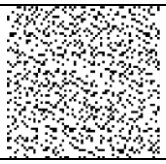
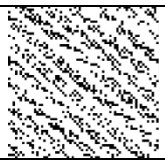
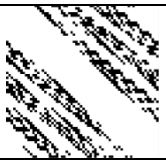
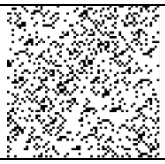
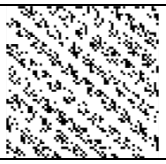
در جدول۵ مشاهده می نمایید که مقدار TAF حاصل صفر است و این بدان معناست که در مقدار و ساختار کد QR اولیه و QR بعد از جداسازی هیچ تفاوتی مشاهده نشده است و نتیجه حاصل از روش پیشنهادی بهتر از روش تبدیل فوریه است.

تست ایمنی

شاید مهمترین ویژگی طرح جدید ارائه شده، امنیت بالای آن باشد، چرا که جذاب ترین ویژگی آشوب در پنهان سازی اطلاعات، حساسیت شدید به شرایط اولیه و پارامترهای آشوب و نیز گستردگی این مقادیر در محدوده ی اعداد صحیح و اعداد حقیقی است(Shi et al, 2010) . در این بخش برای آزمودن ایمنی طرح ارائه شده، مقادیری را که در هنگام شبیه سازی به عنوان کلید معرفی شدند کمی تغییر داده و مجدداً فرآیند استخراج را انجام می دهیم. در طرح پیشنهادی دو گروه کلید وجود داشت. کلید مربوط به تبدیل کد QR و نیز کلیدهای نگاشت آشوب.
در تبدیل کد QR ، سایز به عنوان کلید مطرح می شود. و با افزایش سایز می توان اطلاعات بیشتری را جاسازی کرد. از آنجایی که کدهای QR ساختار مشخصی دارند لذا ، در تست ایمنی، به بحث در این خصوص نمی‌پردازیم.

در مورد نگاشت آشوب، کلیدها دو پارامتر a و b و تعداد تکرار در نگاشت رابطه ی (۳) هستند. در جدول (۶) با اعمال تغییرات اندکی در هر یک از این مقادیر، نتیجه ی خروجی الگوریتم آشوب مورد استفاده در نهاننگاره نشان داده شده است.
همانطور که مشاهده می شود، یک تغییر بسیار جزئی در مقدار هرکدام از کلیدها موجب عدم استخراج صحیح نهاننگاره خواهد شد و شرط استخراج نهاننگاره، داشتن کلیدهای کاملاً صحیح است.

جدول ۶: تست ایمنی طرح پیشنهادی : (الف، ب، ج) تغییر در پارامتر b – (د، ه، و) تغییر پارامتر a – (ز، ح، ط) تغییر پارامتر n – (ی) تغییر در هر سه پارامتر – (ک) تغییر در پارامترهای n و a – (ل) پارامترهای استفاده شده در شبیه سازی

		
ج : (n= 2, a=4, b=-1)	ب : (n= 2, a=4, b=10)	الف : (n= 2, a=4, b=2)
		
و : (n= 2, a=1, b=1)	ه : (n= 2, a=5, b=1)	د : (n= 2, a=-3, b=1)
		
ط : (n= 1, a=4, b=1)	ح : (n= 3, a=4, b=1)	ز : (n= 10, a=4, b=1)
		
ل : (n= 2, a=4, b=1)	ک : (n= 1, a=1, b=1)	ی : (n= 1, a=-1, b=-2)

بحث و نتیجه‌گیری

هرچند در سالهای اخیر پژوهش های فراوانی درزمینه ی نهان نگاری صورت گرفته، لیکن این تکنولوژی هنوز یک دانش نوپا است و برای رسیدن به تکامل، نیازمند کوشش های فراوان است (Shi et al, 2010) . در اینجا برای ادامه ی این تحقیق این پیشنهاد مطرح می شود که همین شبیه سازی روی تصاویر رنگی مورد بررسی قرار گیرد زیرا تصاویر رنگی از سه بلاک رنگ برای جایگذاری استفاده می کند و ظرفیت بالاتری دارند. همچنین در این پژوهش از کدهای QR با سایز ۳۲×۳۲ استفاده شده ؛سایز کدهای پاسخ سریع تا سایز ۱۷۷×۱۷۷ قابل افزایش است . با بزرگ تر کردن کد QR ظرفیت جاسازی متن سری افزایش پیدا می کند . اما باید توجه داشت که با افزایش سایز کد پاسخ سریع کیفیت نهان نگاری کاهش پیدا می کند به همین منظور پیشنهاد می شود از روش دیگری بجای DCT برای جاسازی درون تصویر استفاده شود .

مراجع

معصومه اسمعیلی و مقداد اسمعیلی، ارائه الگوریتم بهبود یافته نهان نگاری تصاویر مبتنی بر SVD به منظورکاهش مشکل تشخیص مثبت کاذب، اولین کنفرانس ملی الگوریتم های فراابتکاری و کاربردهای آن در علوم و مهندسی، مازندران، موسسه آموزش عالی پردیسان،۱۳۹۳

دانشمند م ،" استفاده از لبه های تصویر و نگاشت آشوب در استگانوگرافی "، پایان نامه، گروه ارشد مهندسی کامپیوتر ،دانشگاه آزاد اسلامی، واحد جنوب تهران، شهریور۱۳۹۳.

ماهنامه دولت الکترونیکی، انجمن علمی تجارت الکترونیکی ایران، شهریور ۱۳۹۲، شماره ۳۵.

جواهری پور ص ،" واترمارکینگ تصاویر دیجیتال با استفاده از تبدیل ویولت دومتعامد "، پایان نامه، گروه ارشد مهندسی کامپیوتر ،دانشگاه آزاد اسلامی، واحد جنوب تهران، شهریور ۱۳۹۱.

حسین ملک محمدی چهارشنبه, ۱۸ اردیبهشت ۱۳۹۲ ساعت ۱۱:۰۰، http://www.zoomit.ir/howto/general/5246-qr-%DA%A9%D8%AF%، زمان دسترسی خرداد ۱۳۹۴.

A.A. Jabbar Altaay, Sh. bin Sahib, M. Zamani, "An Introduction to Image Steganography Techniques", Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference, November 2012.

R.J Anderson and F.A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and privacy Protection, Vol. 16(4), pp ,۴۸۱-۴۷۴.May 1998

P.R. Rudramath, Prof. M.R. Madki "High Capacity Data Embedding Technique Using Improved BPCS Steganography", International Journal of Scientific and Research Publications, Vol. II, Issue 7, July 2012.

S. Uma Maheswari, D. Jude Hemanth, "Frequency domain QR code based image steganography using ,Fresnelet transform", ELSEVIER, Aplied International Journal of Electronics and Communications, Int. J. Electron. Commun. (AEÜ) 69 , Pages 539–544, November 2014

B. Li, J. He, J. Huang, Y. Qing Shi "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. II, No. 2, April 2011.

Gao H., Zhang Y., Liang Sh., Li D., "A new chaotic algorithm for image encryption", ELSEVIER, Chaos, Solitons and Fractals, Vol.29,Issue 2,pages: 93-399,July 2006.

Chen, G.; Mao, Y.; Chui, C. "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps."; Chaos, Solitons & Fractals 2004, 12, 749-761.

Guan,Z; Huang,F; Guan,W."A Chaos-based Image Encryption Algorithm."; Phys.Lett.A.2005,346,153-157

Singh Y. S, Pushpa Devi B., Manglem Singh Kh., "A review of different techniques on digital image watermarking scheme", International Journal of Engineering Research,Vol.2, Issue 3, July 2013.

Liebling M, Unser M. "Autofocus for digital Fresnel holograms by use of a Fresnelet-sparsity criterion". J Opt Soc Am 2004;21(12):2424–30.

Liebling M, Blu T, Unser M, Fresnelets. "New multiresolution wavelet bases for digital holography". IEEE Trans Image Process 2003;12(1):29–43.

Shannon, C. E. "Communication Theory of Secrecy Systems."; Bell Syst. Tech. J. 1949, 28, 656-715

P. Shi, Zh. Li, T. Zhang, "A Technique of Improved Steganography Text Based on Chaos and BPCS", Advanced Computer Control (ICACC), 2010 2nd International Conference, Vol. II, March 2010.

P. Shi, Zh. Li, T. Zhang, "A Technique of Improved Steganography Text Based on Chaos and BPCS", Advanced Computer Control (ICACC), 2010 2nd International Conference, Vol. II, March 2010.

Lin,P,Chan,C,"Invertible secret image sharing with steganography".Pattern Recognition Letters31,1887–1893. 2010,

M. Nosrati, R. Karimi, M. Hariri, "An Introduction to steganography methods", World Applied Programming, Vol. I, No. 3, August 2011.

M. Raggo, Ch. Hosmer, "Data Hiding, Exposing Concealed Data in Multimedia", Operating Systems, Mobile Devices and Network Protocols", Syngress (Elsevier), 2013.

Nazeer M, Nargis B, Malik YM, Kim DG. "A Fresnelet-based encryption ofmedical images using Arnold transform". Int J Adv Comput Sci Appl 2013;4(3):131–46.

P.P. Khairnar, Prof. V.S. Ubale, "Steganography Using BPCS Technology", International Journal of Engineering and Science, Vol. III, Issue 2, May 2013.

Shanthi P.,Bhuvaneswaran R.S., "Robust chaos based image watermarking scheme for Fractal-Wavelet", Applied Mathematical Sciences, Vol.8, No.32, 2014.

Wang Y., Wong K.W., Liao X., Chen G., "A new chaos-based fast image encryption algorithm", ELSEVIER, Applied soft computing, Vol.11, Issue 1 , Pages:514–522, January 2011.