دومین کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات
I4C 2017
Homepage: http://i4c.iust.ac.ir

رمزنگاری تصاویر ماهواره مبتنی بر توابع آشوبی و ارتقای امنیت با استفاده از کدگذاری DNA

عاطفه ذوقی*[۱] ، آزاده قجر جزی*[۲] ، کیان کیقباد*[۳]

۱- دانشجوی کارشناسی ارشد دانشکده امنیت و اطلاعات دانشگاه صنعتی مالک اشتر، تهران
۲- دانشجوی دکترا گروه مهندسی پزشکی دانشکده برق دانشگاه علم و صنعت، تهران
۳- استاد یار دانشکده امنیت و اطلاعات دانشگاه صنعتی مالک اشتر،تهران

چکیده

در این مقاله، برای ایجاد امنیت در تصویر برداری ماهواره ای یک سیستم رمزنگاری کلید متقارن مبتنی بر آشوب پیشنهاد شده است که از کلید مخفی با استفاده از چندین نگاشت آشوبگونه به نام های لجستیک، هنون، تنت، کیوبیک، سین و چبی چف توسعه داده شده است. همچنین از فضای DNA برای ارتقای عملکرد سیستم رمزنگاری استفاده شده است.در الگوریتم پیشنهادی رمزگذاری در دو مرحله انجام می‌شود. در مرحله اول کلید آشوبگونه تولید شده به اعداد باینری تبدیل می‌شود سپس هر دو عدد به یک عدد صحیح (۰ تا ۳) تبدیل می‌گردد. این اعداد تعداد دفعات متمم شدن هر کاراکتر متناظر تصویر که در فضای DNA قرار دارد را تعیین می‌نماید. خروجی این مرحله یک تصویر متمم شده DNA است. در مرحله دوم این تصویر به معادل دسیمال خود تبدیل گردیده و هر بلوک آن با کلید XOR می‌شود تا بلوک رمز تولید شود. برای ارزیابی امنیت سیستم، تست‌هایی ازجمله مقدار آنتروپی، میزان همبستگی بین پیکسل‌های تصویر، هیستوگرام وحساسیت کلید محاسبه شده است. نتایج نشان می‌دهد که الگوریتم پیشنهادی دارای امنیت رمزگذاری قابل قبول و فضای کلید بزرگی است. همچنین با استفاده از قوانین متمم گیریDNA به امنیت بالاتر و استحکام بیشتری نسبت به طرح‌های پیشین رسیدیم که برای کارهای آینده می‌توان از آن بهره گرفت.

کلمات کلیدی: تصاویر ماهواره ای، توابع آشوبی، رمزنگاری، متمم گیری DNA

۱- مقدمه

رمزنگاری دانشی است که به بررسی روش‌های انتقال و دخیره‌ی اطلاعات به صورت امن می‌پردازد. در اصل رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید و با استفاده از یک الگوریتم است. به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی باشد. رمزنگاری دو جزء اصلی دارد، الگوریتم و کلید. الگوریتم یک مبدل با فرمول ریاضی است. کلید یک رشته از ارقام دودویی (صفرویک) است که بخودی خود بی معنی است.

* atefeh_zoghi@yahoo.com
* a_ghajarjazy@iust.ac.ir
* keyghobad.kiyan@gmail.com

در این مقاله، الگوریتمی مبتنی بر ترکیب آشوب و DNA به منظور رمزنگاری اطلاعات به کاربرده شده است که در ادامه دلایل استفاده از این دو نوع روش رامطرح و به توضیح مختصری در مورد آن می‌پردازیم.

آشوب پدیده ای است که در سیستم های غیر خطی رخ می دهد که حساسیت زیاد به شرایط اولیه و رفتار شبه تصادفی دارند. چنین سیستم هایی در حالتی که شرایط معادلات نمایی لیاپانوف را برآورده سازد در مد آشوب باقی خواهند ماند. ویژگی مهمی که باعث شده این پدیده برای رمزنگاری بسیار مورد توجه قرار بگیرد [۲-۱] تعریف پذیری سیستم در عین رفتار شبه تصادفی آن است که باعث می گردد خروجی سیستم از دید مهاجم، تصادفی به نظر برسد در حالی که از دید گشاینده رمز تعریف پذیر بوده و قابل رمزگشایی است. در سال ۱۹۴۹ شانون دو ویژگی انتشار[1] و پخش[2] را برای سیستم‌های رمزنگاری [۳] برای به دست آوردن سطح امنیت بالا مطرح کرد و تعیین کرد که توابع آشوبی این دو پارامتر را دارا هستند.

رمزنگاری DNA یک زمینه جدید در امنیت اطلاعات است که ازمحاسبات DNA برای رمزنگاری اطلاعات استفاده می‌کند. راه‌های متفاوتی با استفاده از رمزنگاری DNA وجود دارد[۵-۴]. اطلاعات امنیتی را می‌توان در اندازه‌ی میکروسکوپی DNA به وجود آورد و در میان مقادیر بزرگ ساختارهای دیگر DNA پنهان کرد. DNA به عنوان یک خود مونتاژگر در نظر گرفته می‌شود. چون دارای پایه‌های متمم[3] است که در فرایند پوندزنی با یکدیگر پیوند می‌خورند.

بخش‌های مختلف مقاله به شرح زیر است. در بخش ۲ تئوری پایه ای الگوریتم شامل توضیح کدگذاری DNA و توابع آشوبی مورد استفاده در الگوریتم می‌باشد. در بخش ۳ الگوریتم پیشنهادی شرح داده می‌شود. بخش ۴ به تجزیه و تحلیل نتایج اختصاص یافته است و در بخش ۵ ارائه‌ی نتیجه گیری آمده است.

۲- ابزارها و روش‌ها

۲-۱- کدگذاری و کدگشایی DNA

یکی از جدیدترین و موفق‌ترین روش‌های رمزگذاری تصویر رمزگذاری مبتنی بر DNA است. توسعه‌ی رمزنگاری DNA ناشی از پیشرفت محاسبات DNA می‌باشد[۶]. در علوم اطلاعات، کدگذاری دیجیتالی دودویی[4] بنیادی‌ترین روش کدگذاری است که هر نوع اطلاعاتی را می‌توان به وسیله دو حالت ۰ یا ۱ یا ترکیبی از آن‌ها کدگذاری کرد[۷]. در رشته‌ی DNA دو نوع باز آلی وجود دارد. که ساده‌ترین کدگذاری متناظربا کدنویسی چهار باز نوکلئوتید (A,C,G,T) استفاده از چهاررقم ۰ (۰۰) و۱ (۰۱) و۲ (۱۰) و۳ (۱۱) می‌باشد. بنابراین ۲۴(تعداد جایگشت‌ها: !۴) الگوی کدنویسی با این قالب وجود دارد [۵۱]. همچنین مطابق با قاعده‌ی مکملی واتسون–کریک، در یک رشته‌ی دوگانه از DNA دو زنجیره به وسیله‌ی پیوندهای هیدروژنی ما بین زوج بازها به یکدیگر متصل شده اند، به طوری که همیشه آدنین[5] با تیمین[6] (دو پیوند هیدروژنی) و گوانین[7] با سیتوزین[8] (سه پیوند هیدروژنی) پیوند برقرار می‌کند. بنابراین برای رعایت مشخصات

[1] diffusion
[2] confussion
[3] complement
[4] Binary
[5] Adenin
[6] Cytosine
[7] Guanine
[8] Thymine

بیولوژیکی ۴ باز نوکلئوتید، قانون مکملی (۰=۱) و (۱=۰) در کدگذاری دیجیتال پیشنهاد می‌شود[۸]. بنابراین مطابق با این قانون ۰(۰۰) با ۳ (۱۱) و ۱(۰۱) با ۲ (۱۰) مکمل است. لذا از میان این ۲۴ نوع الگو تنها ۸ نوع الگوی CTAG ، CATG ، GATC ، TCGA ، TGCA، ACGT وAGCT ساختاری متناسب با قانون مکملی بازهای نوکلئوتید دارند [۹] که در جدول (۱) نشان داده شده است.

برای مثال ، اگر مقدار اولین پیکسل تصویر اصلی ۱۷۳ باشد، آن را به دنباله باینری (10101101) تبدیل کنیم، با استفاده از قاعده کد گذاری DNA می‌توانیم دنباله DNA را به صورت (GGTC) دریافت کنیم. بطوریکه 00,01,10,11 به ترتیب نشان دهنده‌ی A=00, C=01, G=10, T=11 هستند. جدول 1 (قوانین نگاشت کدگذاری و کدگشایی برای دنباله DNA را نشان می‌دهد.[۱۰].

جدول۱: قوانین کدگذاری و کد کشایی برای دنباله‌ی DNA

	A	T	C	G
حالت 1	00	11	10	01
حالت2	00	11	01	10
حالت3	11	00	10	01
حالت4	11	00	01	10
حالت5	10	01	00	11
حالت6	01	10	00	11
حالت 7	10	01	11	00
حالت 8	01	10	11	00

۲-۲- توابع آشوبی

از دهه ۱۹۹۰ تعدادی الگوریتم رمزگذاری تصویر و متن مبتنی بر آشوب [۱۴-۱۱] و با کلید متقارن به منظور دستیابی به انتشار و اغتشاش برای ایمن سازی اطلاعات ارایه شده است. این الگوریتم ها بر مبنای یک نگاشت آشوبگونه تکی برای تولید کلید مخفی مورد استفاده قرار می‌گرفتند.

این مقاله به طور عمده بر ایده‌ی استفاده از چندین نگاشت آشوبگونه برای تولید کلید مخفی تاکید دارد. که از طریق بهبود اغتشاش و انتشار در رمزگذاری، سطح امنیت الگوریتم را ارتقا می‌دهد.

الگوریتم پیشنهادی از ۶ نگاشت آشوبگونه متفاوت به نام های لجستیک، تنت[۹]، هنون[۱۰]، سین[۱۱]، کوبیک[۱۲] وچپیشف[۱۳] استفاده می‌کند. دلیل انتخاب این نگاشت‌ها، اثبات کارایی و امنیت آنها توسط بسیاری از محققان است [۱۵]. همچنین باتوجه به اینکه به استفاده از توابع آشوبی در الگوریتم رمزنگاری تصاویر ماهواره دارای محدودیت است بنابراین باید از توابعی استفاده شود که دارای قابلیت پیاده سازی ساده‌ای باشد. توابع آشوبی چند بعدی دارای پیچیدگی بیشتری

[9] Tent
[10] Henon
[11] Sine
[12] Cubic
[13] Chebyshev

نسبت به توابع تک بعدی بوده لذا برای استفاده در الگوریتم تصاویر ماهواره پیشنهاد نمی‌شود. توابع مورد استفاده در این الگوریتم، از نوع توابع تک بعدی هستند. جدول (۲) نگاشت های آشوبگونه، روابط و پارامترهای آن ها نوشته شده است. دنباله‌های آشوبگونه تولید شده با هر نگاشت آشوبگونه به صورت اعداد حقیقی هستند، ابتدا این اعداد حقیقی را به دنباله ای از بیت ها و سپس به فرمت بایت تبدیل می‌کنیم.

جدول۲: نگاشت‌های آشوبگونه، روابط و مقادیر پارامترهای آن‌ها

نگاشت آشوبی	معادلات	مقدار پارامتر
چبیشف	$x_{n-1} = \cos(\lambda cos^{-1}(x_n))$	$\lambda = 4$
لاجستیک	$x_{n+1} = \lambda x_n(1 - x_n)$	$\lambda = 4$
کوبیک	$x_{n+1} = \lambda x_n(1 - x_n^2)$	$\lambda = 2.59$
سین	$x_{n+1} = \lambda\ sin(\pi x_n)$	$\lambda = 0.99$
هنون	$x_n = 1 + \lambda(x_{n-2} - x_{n-3}) + \alpha x_{n-2}^2$	$\lambda = 0.3 \quad 1.07 \leq \alpha \leq 1.09$
تنت	$x_{n+1} = \begin{cases} x_n/\mu & if x_n \leq \mu \\ 1 - x_n/1-\mu & if x_n \geq \mu \end{cases}$	$\lambda = 0.4$

۳- شرح الگوریتم

برای رمزگذاری/ رمزگشایی، تصاویر اصلی و خروجی رمز را به بلوک هایی با طول ۲۵۶ بیت (که ابعاد بلوک BS بیت نامگذاری شده) تقسیم می‌کنیم.

$$O = O_1O_2O_3O_4O_5 \dots O_m \quad (۱)$$

$$C = C_1C_2C_3C_4C_5 \dots C_m \quad (۲)$$

الگوریتم مورد استفاده در [۱۶] از کلید مخفی ۲۵۶ بیتی (باید با بلوک تعریف شده با ورودی یکسان باشد) استفاده می‌کند که پیش از عملیات رمزگذاری و رمزگشایی به فرمت بایت تبدیل می‌کند. کلید مخفی به صورت معادله (۳) نشان داده می‌شود:

$$K = bK_1bK_2bK_3bK_4bK_5 \dots bK_n \quad (۳)$$

که در آن، $n = BS/8$ و BS ابعاد بلوک به بیت است بنابراین ابعاد کلید مخفی K بستگی به ابعاد بلواک دارد. برای مثال اگر ابعاد بلوک BS برابر ۲۵۶ بیت باشد، ابعاد کلید مخفی K به بایت برابر ۳۲ می‌شود (یعنی $256/8$).

۳-۱- چگونگی تولید کلید

حالت هگزادسیمال برای کلید مخفی برای شرایط اولیه IC (برای هر نگاشت آشوبگونه) استفاده می‌شود که دنباله های بیتی متفاوتی را از اعداد حقیقی تولید می‌کند. کلیدهای مخفی با استفاده از معادلات (۴) و (۵) بدست می‌آیند:

$$N = \sum_{i=1}^{BS/8} (bK_i/256) \quad (۴)$$

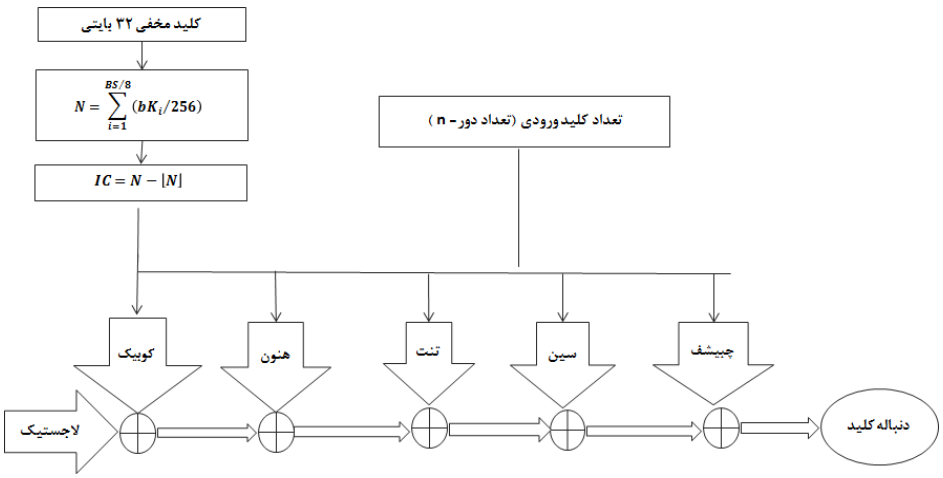
$$IC = N - \lfloor N \rfloor \quad (۵)$$

جاییکه bK_i مقدار iامین مقدار کلید در معادل دسیمال کلید مخفی، $\lfloor N \rfloor$ رند شده‌ی مقدار N، BS ابعاد بلوک با طول ۲۵۶ بوده و IC مقدار شرایط اولیه است که دوباره به اعداد حقیقی تبدیل شده است.

اگر از کلید مخفی و ابعاد بلوک یکسان برای هر نگاشت آشوبگونه در الگوریتم استفاده کنیم، شرایط اولیه برای همه نگاشت های آشوبگونه مطابق جدول (۲) تولید می شود. این الگوریتم از شش ترکیب متفاوت نگاشت های آشوبگونه برای تولید کلید استفاده می‌کند که در معادله (۶) و شکل (۱) بیان شده است که در هر نگاشت ممکن است n تعداد کلید (دور) داشته باشیم و n باید بزرگتر یا مساوی یک باشد.

$$K_i = BK_i \oplus LK_i \oplus CK_i \oplus SK_i \oplus HK_i \oplus TK_i \quad (۶)$$

که در آن $i = 1,2,3,\dots,n$ و $n \geq 1$ است.



شکل ۱-بلوک دیاگرام فرایند تولید کلید

۳-۲- ارتقای امنیت رمزنگاری توسط DNA

برای ارتقای امنیت از الگوریتمی به نام DNA استفاده می‌کنیم[۱۷]. در الگوریتم پیشنهادی رمزگذاری در دو مرحله انجام می‌شود. در مرحله اول، کلیدهای ایجاد شده با استفاده از توابع آشوبگونه به همراه تصویر بلوک بندی شده به فضای باینری انتقال داده می‌شود و به منظور ارتقای سطح امنیت از قوانین متمم گیری DNA استفاده می‌شود. در مرحله بعد، بلوک های تصویر با کلید آشوبگونه XOR می‌شود.

۳-۲-۱- قانون متمم گیری DNA

در استفاده از فضای DNA دو رویه وجود دارد [۱۹-۱۸] که باید تعیین شود: اول قانون کد باینری که اعداد باینری را به کد DNA و یا بالعکس تبدیل می‌کند. دوم قانون متمم‌گیری که نحوه تبدیل هر کد باینری را به کد دیگر معین می‌نماید. معادل باینری و قانون متمم گیری در جدول (۳) و (۴) نمایش داده شده است.

جدول ۳-معادل باینری کد DNA

کد DNA	عدد باینری	عدد صحیح	Nucleotides
Adenosine	۰۰	۰	A
Cytidine	۰۱	۱	C
Guanine	۱۰	۲	G
Thymidine	۱۱	۳	T

بر اساس قانون متمم گیری انتخابی تابع f(.) باید به نحوی انتخاب گردد که روابط زیر برقرار گردد:

$$f'(x) \neq f(x)$$
$$f'(f'(x)) \neq f(x)$$
$$f'(f'(f'(x))) \neq f(x)$$
$$f'(f'(f'(f'(x)))) = f(x)$$

جدول ۴- قانون متمم گیری از کد DNA

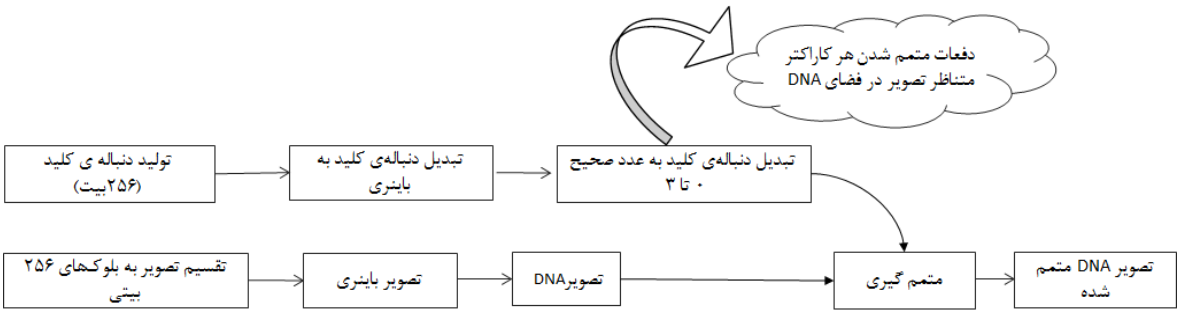
کد DNA	متمم
A	G
C	T
G	C
T	A

۳-۳- نحوه‌ی رمزنگاری

در مرحله اول کلید آشوبگونه تولید شده ابتدا به اعداد باینری تبدیل می‌شود سپس هر دو عدد به یک عدد صحیح (۰ تا ۳) تبدیل می‌گردد. این اعداد تعداد دفعات متمم شدن هر کاراکتر متناظر تصویر که در فضای DNA قرار دارد را تعیین می‌نماید. خروجی این مرحله یک تصویر متمم شده DNA است. در مرحله دوم این تصویر به معادل دسیمال خود تبدیل گردیده و هر بلوک آن b_i با کلید k_i XOR می‌شود تا بلوک رمز c_i تولید شود که در آن $i = 1,2,3,\dots,m$ است

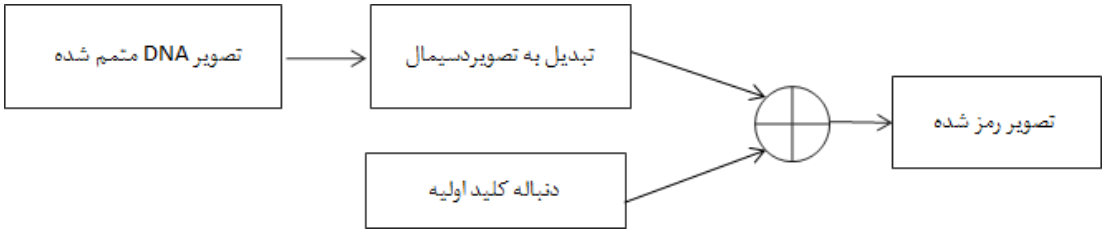
بلوک دیاگرام فرآیند رمزگذاری/رمزگشایی در شکل(۲) ، (۳) و (۴) نشان داده شده است. الگوریتم پیشنهادی وابسته به کلید مخفی است بنابراین زمان رمزگذاری همیشه بستگی به زمانی دارد که صرف تولید تعداد n کلید (دور) در رمزگذاری یا رمزگشایی می‌شود. در این مقاله، ویژگی های رمزگذاری با استفاده از ۱ تا ۱۰ کلید (دور) بررسی شده است. پارامترهای استفاده شده برای تصویر ماهواره ای بوستون در جدول (۵) تعریف شده است.

مرحله‌ی اول:

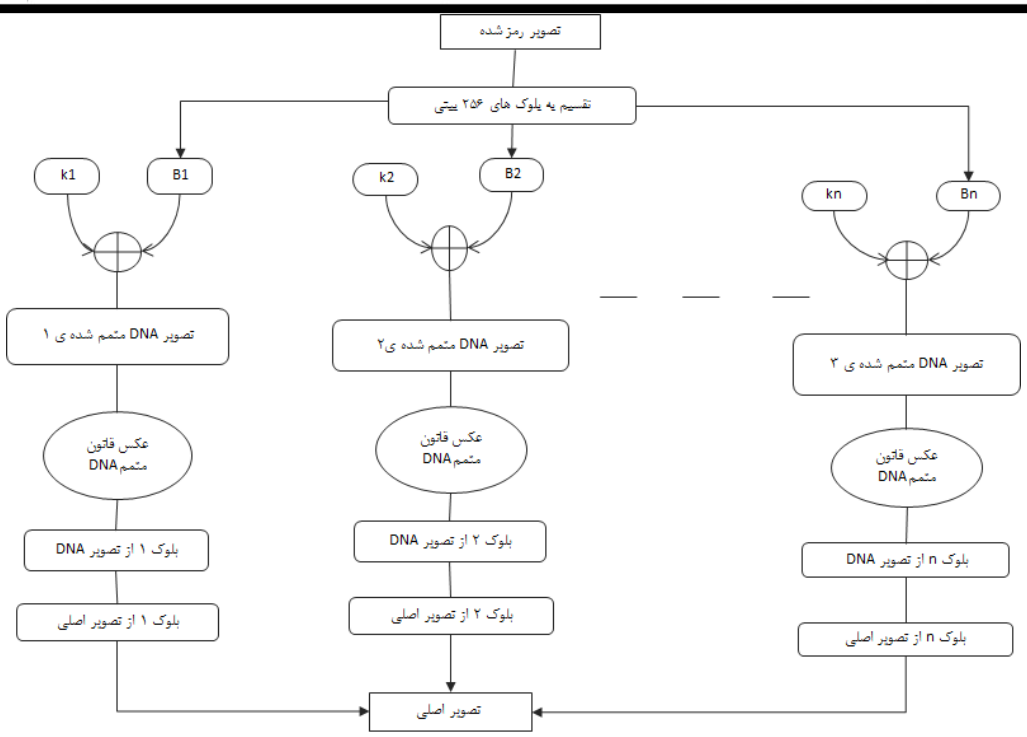


شکل ۲- بلوک دیاگرام تشکیل تصویر متمم شده‌ی DNA

مرحله‌ی دوم:



شکل ۳-بلوک دیاگرام تشکیل تصویر رمز شده



شکل ۴- بلوک دیاگرام فرایند رمزگشایی

تعداد کل عملیات لازم برای رمزگذاری یکسان باقی می‌ماند (اگر از تعداد کلید یکسان استفاده کنیم). درنتیجه در اجرای عملیات رمزگذاری و رمزگشایی بر روی یک تصویر ماهواره ای معین، افزایش طول کلید مخفی در پردازش کلی و زمان محاسبات تاثیری ندارد. اگرچه در رمزگذاری زمان موردنیاز برای محاسبه کلید مخفی (یکبار در الگوریتم) ممکن است تغییر کند اما در فرآیند رمزگذاری/ رمزگشایی تنها یکبار نیاز به انجام این محاسبات داریم. بنابراین این تغییر اندک در زمان می تواند نادیده گرفته شود و تاثیر بزرگی بر کارایی کلی الگوریتم ندارد.

جدول ۵- پارامترهای اولیه‌ی استفاده شده در آزمایش

کلید رمز	123456GHIJKLMNOPQRSTUVWXYZ[/]'		
کلید رمز هگز	63676B8F939799FA3ABAFB3BGH7BBB		
اندازه بلوک	۲۵۶ بیت (۲۳ بایت)		
نگاشت	counter	lambda	شرط اولیه
کوبیک	0.0000001	2.5900005	0.734375
هنون	0.0000001	0.3000005	0.734375
لاجستیک	0.0000001	4.0000005	0.734375
سین	0.0000001	0.9000005	0.734375
تنت	0.0000001	0.4000005	0.734375
چبیشف	0.0000001	2.6000005	0.734375

سطح کارایی الگوریتم ممکن است با ابعاد کلید تغییر کند. ابعاد کلید قابل پشتیبانی ۱۲۸، ۱۹۲، ۲۵۶ و ۵۱۲ بیت است. طول کلید مخفی، زمان پردازش الگوریتم را چندان افزایش نمی‌دهد هرچند تغییرات کم در زمان پردازش قابل صرفنظر است.

۴- شبیه سازی ونتایج

الگوریتم پیشنهادی با استفاده از نرم افزار متلب پیاده سازی شده است. نتایج آزمایشات انجام شده برای اثبات کارایی و امنیت این الگوریتم رمزنگاری برای تصاویر ماهواره ای آورده شده است. تصویر سطح خاکستری ماهواره ای بوستون با ابعاد ۵۱۲X۶۰۲ به عنوان تصویر اصلی در شکل (۶) نشان داده شده است.کلید مخفی "123456GHIJKLMNOPQRSTUVWXYZ[\]^_" (کد اسکی) برای رمزگذاری و رمزگشایی استفاده شده است.

شکل ۶-تصویر اصلی بوستون

تعدادی از تصاویر رمزگذاری شده در شکل(۸)، (۹) و (۱۰) نمایش داده شده است. تصاویر رمزگذاری شده کاملا به صورت درهم از تصاویر اصلی بدست می آید.

۴-۱- ماکزیمم انحراف

ماکزیمم انحراف، عدم دقت فرآیند رمزگذاری و رمزگشایی را در ماکزیمم کردن انحراف بین نتایج رمزگذاری شده/ رمزگشایی شده با تصویر اصلی اندازه می‌گیرد.

نخست، نمودار هیستوگرام که نشان دهنده توزیع تصویر رمزگذاری شده/ رمزگشایی شده و تصویر اصلی سطح خاکستری است، تولیدشده وسپس تعداد پیکسل های هر مقدار مقیاس خاکستری در بازه ۰ تا ۲۵۵ را شمرده می‌شود.

دوم، اختلاف بین دو مقدار حاصل محاسبه می‌شود. در انتها، سطح زیر منحنی با اضافه کردن این مقادیر به سادگی اندازه گرفته می‌شود و مجموع انحراف D است.

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad (۷)$$

h_i ماکزیمم جابجایی بین دو منحنی در مقدار i است. هرچه مقدار انحراف D بیشتر (مثبت یا منفی) باشد، تصویر رمزگذاری شده از تصویر اصلی دورتر است.

نتایج ماکزیمم انحراف محاسبه شده در تصویر رمزگذاری شده/ رمزگشایی شده بوستون نسبت به تصویر اصلی با استفاده از الگوریتم پیشنهادی در جدول (۵) آورده شده است. نتایج آزمایش‌ها پیشنهاد می‌کند که الگوریتم پیشنهادی ماکزیمم انحراف بزرگتری دارد که برای یک سیستم رمزنگاری کارا و امن مطلوب است.

۴-۲- آنتروپی اطلاعات

آنتروپی شانون یا اطلاعات معیاری از عدم اطمینان یک متغیر تصادفی است که اطلاعات موجود در داده‌ها را تعیین می‌کند.

برای محاسبه ی آنتروپی $H(m)$ از منبع m:

$$H(m) = \sum_{i=0}^{2N-1} p(m)\, log_2 \frac{1}{p(m_i)} \qquad (۸)$$

که در آن $P()$ نشاندهنده ی احتمال سمبل mi است و آنتروپی در بیت بیان می شود.

آنتروپی توسط معادله‌ی (۹) محاسبه می شود.

$$H(m) = \sum_{i=0}^{255} p(m)\, log_2 \frac{1}{p(m_i)} \qquad (۹)$$

مقادیر به دست آمده از آزمایش به مقدار نظری ۸ به شدت نزدیک است. نشتی اطلاعات در فرایند رمزگشایی تصویر ناچیز است و سیستم رمزنگاری پیشنهادی در برابر حمله‌ی آنتروپی مقاوم است.

با توجه به نتایج بهینه‌ی بدست آمده از ترکیب شش نگاشت، در الگوریتم پیشنهادی مقدار ماکزیمم انحراف و آنتروپی را با تعداد کلیدهای اولیه‌ی مختلف (دورهای مختلف) در ترکیب شش نگاشت بدست می‌آوریم. جدول (۶) نتایج حاصل را نشان می‌دهد.

جدول ۵- ماکزیمم انحراف و آنتروپی برای ترکیب نگاشت های آشوبگونه Chebyshev, Cubic, Henon, Logistic, Tent, SINE در الگوریتم پیشنهادی با تعداد دورهای اولیه متفاوت

تعداد کلید اولیه	ماکزیمم انحراف (D)	آنتروپی
۱	۲۵۷۶۱۷	۷/۹۹۶۶
۲	۲۷۳۲۳۴	۷/۹۹۷۲
۳	۲۶۳۷۹۶	۷/۹۹۹۴
۴	۲۶۳۷۹۶	۷/۹۹۹۰
۵	۲۶۵۴۲۸	۷/۹۹۹۲
۶	۲۶۵۳۲۰	۷/۹۹۹۴
۷	۲۶۰۷۲۰	۷/۹۹۷۲
۸	۲۶۴۲۹۹	۷/۹۹۹۳
۹	۲۶۳۱۳۰	۷/۹۹۹۳
۱۰	۲۶۰۲۴۳	۷/۹۹۹۱

جدول۶- مقایسه‌ی نتایج مقادیر ماکزیمم انحراف و آنتروپی قبل و بعد از استفاده از دنباله‌ی DNA

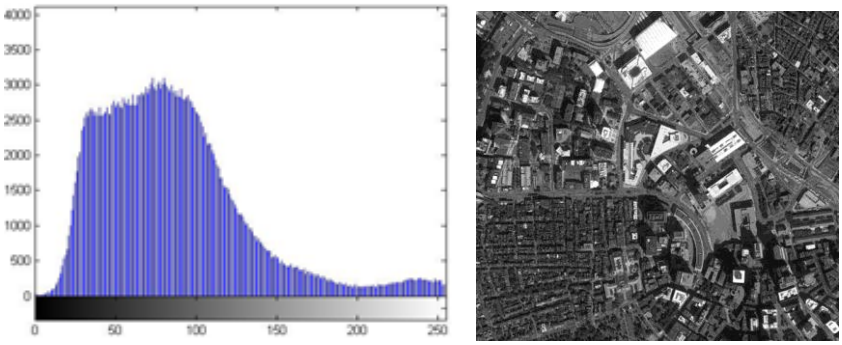
ترکیب ۶ نگاشت	ماکزیمم انحراف (D)	آنتروپی
بدون استفاده از دنباله‌ی DNA وتعداد ۱۰ دوراولیه	۲۵۶۲۷۶	۷/۹۹۷۰
با استفاده از دنباله‌ی DNA و تعداد ۲ دور اولیه	۲۷۳۲۳۴	۷/۹۹۷۲

۴-۳- آنالیز هیستوگرام

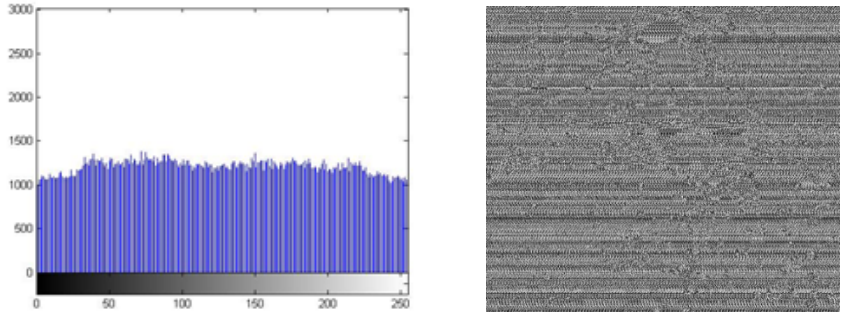
هیستوگرام تصویر نشان می‌دهد که چگونه عناصر پیکسل در یک تصویر توزیع شده‌اند. برای بررسی توزیع های آماری، آنالیزهایی بر روی نتایج آزمایش های مختلف توسط الگوریتم پیشنهادی با استفاده از آنالیز هیستوگرام انجام شده است.

$$N = \sum_{i=0}^{n} m_i \qquad (۱۰)$$

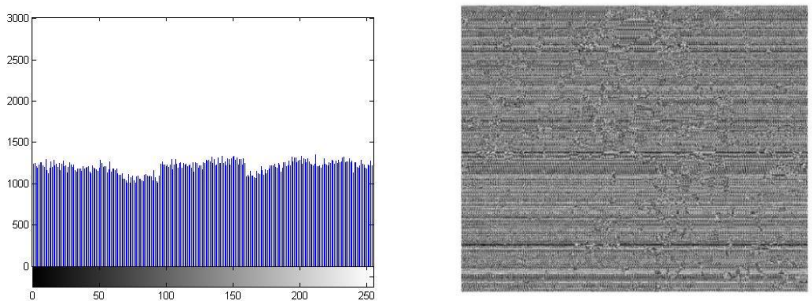
هیستوگرام تصویر رمزنگاری شده با استفاده از دنباله‌ی DNA در ترکیب شش نگاشت و تعداد دورهای اولیه‌ی متفاوت در شکل‌های (۸)، (۹) و (۱۰) نشان شده است.



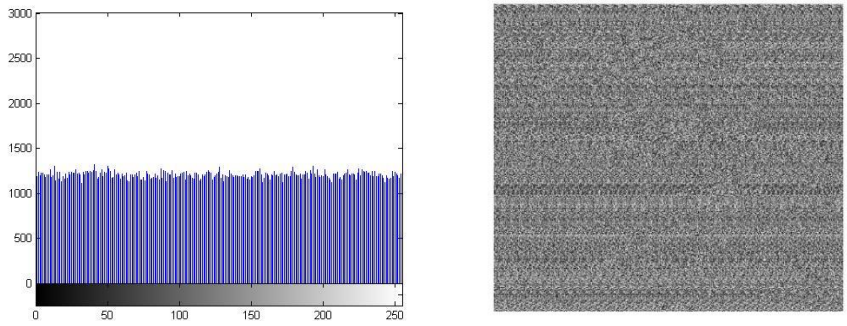
شکل ۷-تصویر ماهواره ای بوستون و هیستوگرام. سمت راست: تصویر اصلی، سمت چپ: هیستوگرام تصویر اصلی



شکل ۸-بررسی هیستوگرام تصویر ماهواره ای بوستون با استفاده از نگاشت های Chebyshev، Cubic، Henon، Logistic، Tent و Sin ویک دور. سمت راست: تصویررمز شده، سمت چپ: هیستوگرام تصویررمز شده



شکل ۹-بررسی هیستوگرام تصویر ماهواره ای بوستون با استفاده از نگاشت های Chebyshev، Cubic، Henon، Logistic، Tent و Sin و دو دور. سمت راست: تصویررمز شده، سمت چپ: هیستوگرام تصویررمزشده



شکل ۱۰-بررسی هیستوگرام تصویر ماهواره ای بوستون با استفاده از نگاشت های Chebyshev، Cubic، Henon، Logistic، Tent و Sin و هشت کلید. سمت راست: تصویررمزی شده، سمت چپ: هیستوگرام تصویررمز شده

۴-۴- آنالیز فضای کلیدی

برای الگوریتم رمزنگاری امن تصویر، فضای کلیدی باید به اندازه کافی بزرگ باشد تا حملات غیرممکن شود. الگوریتم پیشنهادی دارای ترکیبات مختلف 2^{128}، 2^{192}، 2^{256} و 2^{512} از کلید های مخفی است. رمزگذاری تصویر با چنین فضای طولانی کلید برای استفاده‌ی عملی قابل اعتماد، کافی است.

۴-۵- آنالیز حساسیت کلید

یک الگوریتم ایده آل رمزنگاری تصویر، باید به کلید مخفی ورودی حساس باشد. تغییر تک بیت درکلید باید نتایج خروجی کاملا متفاوتی را تولید کند. برای اثبات مقاومت الگوریتم پیشنهادی، آنالیز حساسیت با توجه به کلید انجام شده است.

حساسیت بالای کلید توسط تصویر رمزنگاری شده امن ماهواره مورد نیاز است که به این معنا است که اگرچه تنها تفاوت جزئی بین کلید مخفی وجود دارد تصویر رمز شده به درستی نمی تواند رمزگشایی شود. این ضمانتی برای الگوریتم پیشنهادی بر علیه حمله ی جست و جوی جامع است.

به منظور آزمودن حساسیت کلیدی الگوریتم پیشنهادی مراحل زیر اجرا شده است:

$$r_{xy} = \frac{con(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (۱۱)$$

$$con(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (۱۲)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (۱۳)$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \quad (۱۴)$$

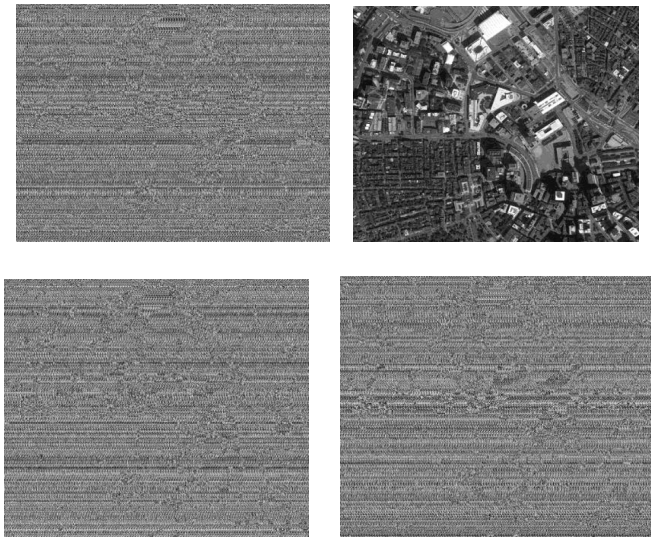
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (۱۵)$$

$$D(y) = \frac{1}{N}\sum_{j=1}^{N}(y_i - E(y))^2 \quad (۱۶)$$

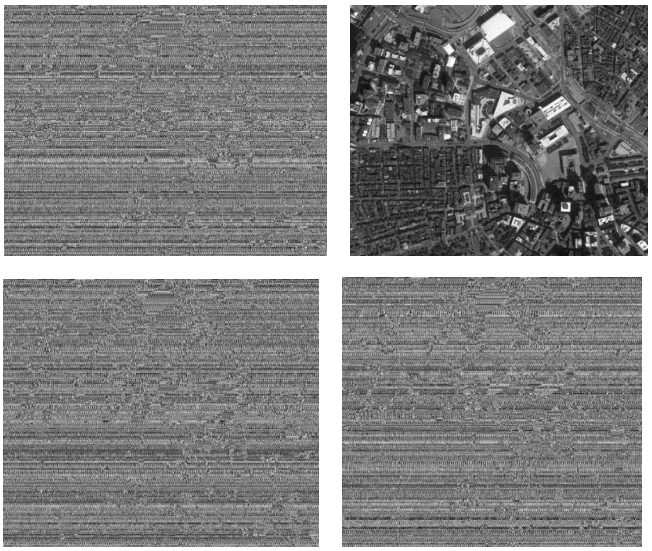
جدول (۷) ضرایب همبستگی بین پیکسل های متناظر سه تصویر رمزنگاری شده متفاوت با استفاده از کلیدهایی با اندکی تفاوت بعد از استفاده از دنباله‌ی DNA در ترکیب شش نگاشت آشوبگونه‌ی مختلف نشان می‌دهد.

جدول ۷- مقایسه‌ی ضرایب همبستگی بین پیکسل های متناظر سه تصویر رمز شده متفاوت با استفاده از کلیدهایی با اندکی تفاوت قبل و بعد از استفاده از دنباله‌ی DNA در ترکیب ۶ نگاشت

تصویر اول	تصویر دوم	ضریب همبستگی قبل از استفاده از دنباله DNA	ضریب همبستگی بعد از استفاده از دنباله DNA
شکل۱۲و ۱۱- ب	شکل۱۲و ۱۱- پ	۰/۰۱۶۱	۰/۰۰۲۲
شکل۱۲و ۱۱- پ	شکل۱۲و ۱۱- ت	۰/۰۳۴۲	۰/۰۱۵۴
شکل۱۲و ۱۱- ت	شکل۱۲و ۱۱- ب	۰/۰۰۴۹	۰/۰۰۷۴



شکل ۱۱-تست حساسیت کلید با استفاده از ترکیب ۶ نگاشت آشوبگونه‌ی Chebyshev، Cubic، Henon، Logistic، Tent و Sin. بالاراست- تصویر اصلی، بالاچپ- تصویر رمزنگاری شده با کلید ۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲، پایین راست- تصویر رمزنگاری شده با کلید۲۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲، پایین چپ- تصویر رمزنگاری شده با کلید ۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۳۳



شکل ۱۲-تست حساسیت کلید با استفاده از ترکیب ۶ نگاشت آشوبگونه‌ی مختلف Chebyshev، Cubic، Henon، Logistic، Tent و Sin و دنباله‌ی DNA، بالا راست- تصویر اصلی، بالاچپ: تصویر رمزنگاری شده با کلید۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲ ، پایین راست: تصویر رمزنگاری شده با کلید ۲۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲ ، پایین چپ: تصویر رمزنگاری شده با کلید ۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۱۲۳۴۵۶۷۸۹۰۳۳

۵- نتیجه‌گیری

رمزنگاری آشوبناک تصویر یک زمینه‌ی کاری جدید است که در طی ۲۰ سال اخیر توجهات زیادی را به خود جلب کرده است. باید الگوریتمی برای تصاویر ماهواره ای بلادرنگ پیشنهاد شود که بتواند الگوریتم را در مدت زمان کم و با حجم پردازش پایین اجرا کند. از آنجا که تصاویر ماهواره ای که به صورت بلادرنگ هستند نیاز به زمان کم و پردازش کمی دارند. همچنین با توجه به اینکه سیستم رمزنگاری ماهواره‌ای به صورت سیستم رمزنگاری روی برد است، بنابراین الگوریتم باید قابلیت پیاده سازی سخت افزاری ساده ای را داشته باشد و بتوان با توان محاسباتی کم الگوریتم را اجرا نمود. از آن جا که در سیستم رمزنگاری طول کلید تعیین کننده‌ی مقاومت در برابر حملات می‌باشد باید الگوریتمی استفاده شود که دارای طول کلید بزرگی باشد. شکستن الگوریتم با طول کلید رمزنگاری بالا توسط کامپیوترهای پیشرفته چندین سال طول می‌کشد.

در این مقاله یک روش نوین رمزنگاری کلید متقارن جهت رمزنگاری تصاویر ماهواره ای ارائه گردیده است. که از ترکیب نگاشت های چبیشف، لاجستیک، هنون، کوبیک، تنت و سین برای تولید کلید جهت افزایش فضای کلید استفاده می‌شود. همچنین از قوانین متمم گیری دنباله‌های DNA به منظور بهم ریختن پیکسل‌های تصویر استفاده شده و در نهایت از عملگر XOR به منظور رمزنگاری بهره گرفته شده است. دراین روش از خصوصیات توابع آشوب که شامل حساسیت به مقدار اولیه، تصادفی بودن و غیر متناوب بودن که منجر به تولید دنباله‌ی تصادفی شده است و دنباله‌های DNA که دارای پیچیدگی هستند، بهره گرفته شده است. جهت ارزیابی طرح پیشنهادی، مقدار آنتروپی، میزان همبستگی بین پیکسل‌های تصویر اصلی و تصویر رمزنگاری شده، هیستوگرام وحساسیت کلید را بدست آوردیم که نتایج، تأثیر طرح پیشنهادی را به وضوح نشان می‌دهد.

نتیجه‌ی آزمایش‌ها و تجزیه و تحلیل امنیت نشان می‌دهد که الگوریتم پیشنهادی دارای امنیت رمزگذاری قابل قبول و فضای کلید بزرگتری نسبت به الگوریتم‌های رایج رمزنگاری از جمله AES است. (فضای کلید مورد استفاده برای الگوریتم رمزنگاری AES ، 2^{128}، 2^{192} و 2^{256} می‌باشد.) همچنین با استفاده از قوانین کدگذاری DNA و متمم گیریDNA به امنیت بالاتر و استحکام بیشتری نسبت به طرح‌های پیشین رسیدیم که پیچیدگی رمزنگاری بیشتر شده و برای کارهای آینده می‌توان از آن بهره گرفت.

مراجع

[1] Ming-yang YU,“ Image Encryption Based on Improved Chaotic Sequences”, IEEE Trans. Academy Publisher Journal of Multimedia, Vol.8, No.6, PP. 802-808,2013.

[2] J.M. Amigó and L. Kocarev and J. Szczepanski,“Theory and practice of chaotic cryptography”,IEEE Trans. Elsevier Physics Letters A, vol. 366, No. 3,PP.211-216, 2007.

[3] M. Usama and M. Khurram Khan, "Satellite Imagery Security Application (SISA)" IEEE proceedings International Multitopic Conference, 2008.
[4] Zhi.Guan and F.Huang and W.Guan,"Chaos-based image encryption algorithm", IEEE Trans .Elsevier Physics Letters A, Vol.346, No.1-3, pp.153–157, 2005.
[5] Li.Liu and Q.Zhang and X.Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map", IEEE Trans .Elsevier Computers and Electrical Engineering, Vol.38, No.5, PP.1240-1248, 2012.
[6] DJ E. Goumidi and F. Hachouf, "Modified Confusion-Diffusion based Sattelite image cipher using Chaotic Standard ,Logistic and Sine maps" 2nd European Workshop on Visual Information Processing, PP. 204-209, 2010.
[7] G.Xiao , M.Lu , L.Qin and X.Lai "New field of cryptography:DNA cryptography" IEEE Trans .Elsevier Journal of Chinese Science Bulletin, Vol.51, No.12, pp.1413-1420, 2006
[8] Sh.Zhang and T.Gao,"An image encryption scheme based on DNA coding and permutation of hyper-image" IEEE Trans . Springer Nature Multimedia Tools and Applications, Vol.75, No.24, PP.17157-17170, 2016.
[9] X.Huang and G.Ye,"An image encryption algorithm based on hyper-chaos and DNA sequence" IEEE Trans . Springer Nature Multimedia Tools and Applications, Vol.72, No.1, PP. 57-70,2014.
[10] A.N.Pisarchik and M.Zanin,"Image Encryption with Chaotically Coupled Chaotic Maps" IEEE Trans . Elsevier Physica D: Nonlinear Phenomena, Vol.237, No.20, PP.2638-2648, 2008.
[11] A.Hussain," Image compression and encryptionscheme via satellit" Journal of Vibration and Control, Vol.22, No.13, PP. 3118-3122, 2016.
[12] S. Behnia , A. Akhshani , S. Ahadpour, H. Mahmodi and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps",IEEE Trans .Elsevier Physics Letters A, Vol.366, No. 4-5,PP.391-396,2007.
[13] A.Subiyakto and N.Andini and D.Darlis,"Security Analysis of RGB Image Encryption Based on Modified Baker Map for Nanosatellite Application" IEEE proceedings of International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications, PP.114-118, 2015.
[14] L.Liu, Q.Zhang and X.Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map" IEEE Trans. Elsevier Computers and Electrical Engineering, Vol 38, No.5, PP.1240-1248, 2012.
[15] F. Muhaya , "Chaotic and AES cryptosystem for satellite imagery" IEEE Trans. Telecommunication Systems, Vol. 52, No. 2, PP.573-581,2013
[16] M.Usamaa and M.Khurram Khana and K. Alghathbar, Ch.Lee b,"Chaos-based secure satellite imagery cryptosystem" IEEE Trans. Computers and Mathematics with Applications Vol. 60, No. 2, PP.326-337, 2010. Elsevier
[17] A.Awad and A.Miri ,"A New Image Encryption Algorithm Based on a Chaotic DNA Substitution Method" IEEE proceedings International Conference on Communications (ICC), 2012.
[18] B.Mondal and T.Mandal "A light weight secure image encryption scheme based on chaos & DNA computing" Elsevier B.V. Journal of King Saud

University – Computer and Information Sciences Vol.29, No.4, PP. 499-504, 2017.

[19] Bonny B Raj, Panchami,"DNA Based Cryptography Using Permutation and Random Key Generation Method" International Jornal of Innonative Research Science, Engineering and Technology, Vol.3, No.5, PP. 263-267, 2014.