پنهان کردن تصویر با استفاده از تابع آشوب

رسول عنایتی فر[۱]؛ محمد رضا میبدی[۲]

چکیده

در این مقاله یک روش جدید برای پنهان کردن تصویر با استفاده از تابع آشوب پیشنهاد شده است بطوریکه از تابع آشوب برای تعین موقعیت هر پیکسل از تصویر نمونه در تصویر پوشاننده استفاده شده است. خصوصیت آشوبگونه تابع آشوب باعث توزیع متعادل پیکسلهای تصویر نمونه برای پنهانی کردن در تصویر پوشاننده می شود که این توزیع متعادل، مقاومت روش پیشنهادی در برابر انواع صدمات وارده را افزایش می دهد.

بررسی مقاومت روش پیشنهادی در برابر انواع صدمات وارده مانند خرابی تصویر، برش از تصویر، اعمال نویز و از طرفی مقدار بالای PSNR در این روش(حدود ۴۴.۴۱) حاکی از کارایی مناسب روش پیشنهادی می باشد.

کلمات کلیدی

پنهان کردن تصویر، تصویر اصلی، تصویر پوشاننده، تابع آشوب

Image Encryption via Chaotic Function

*Rasul Enayatifar; ×Mohammad Reza Meybodi

*Computer Engineering Department ,Azad Islamic University,Firoozkuh,Iran

×Computer Engineering and Information Technology Department,Amirkabir University,Tehran,Iran

ABSTRACT

In this paper a new method for image encryption via chaotic function proposed. For determine of each pixel of main image inside cover image used chaotic function. Quality chaotic function cause equal distribution of main image pixels for encryption inside cover image that the equal distribution increases resistance of the proposed method in face of types of attack.

Study of the proposed method resistance in face of types attacks such as cutting image, noisy image, peak signal to noises ratio and high value of PSNR has shown a suitable efficiency in the proposed method.

KEYWORDS

Image Encryption, Main Image, Cover Image, Chaotic Function

۱. مقدمه

با رشد سریع تولیدات چند رسانه ای و پخش گسترده محصولات دیجیتالی بر روی اینترنت محافظت از اطلاعات دیجیتالی در برابر کپی و توزیع غیر مجاز هر روز اهمیت بیشتری پیدا می کند. برای رسیدن به این هدف الگوریتم های گوناگونی برای پنهان کردن تصویر[۱] پیشنهاد شده است[۱,۲,۳,۴]. ایراد اصلی وارده به روشهای پیشین مقاومت پایین این روشها در برابر حملاتی متداول در این حوزه می باشد. به عنوان مثال در [۴] یک روش در حوزه Wavelet برای پنهان کردن تصویر پیشنهاد شده است که به علت ترتیبی قرار دادن پیکسلهای تصویر اصلی در تصویر پوشاننده این روش در برابر حمله برش از تصویر بسیار ضعیف عمل می کند. .از این رو در سالهای گذشته محققین بیشتر بر روی روشهایی متمرکز شده اند که به توزیع متعادل پیکسلهای تصویر اصلی در تصویر پوشاننده بپردازد[۵,۶,۷].

---

۱. دانشگاه آزاد اسلامی واحد فیروزکوه، r.enayatifar@iaufb.ac.ir و ۲- دانشکده مهندسی کامپیوتر دانشگاه صنعتی امیر کبیر تهران- ایران، mmeybodi@aut.ac.ir

در این مقاله یک روش جدید با استفاده از توابع آشوب پیشنهاد شده است. در گذشته از خصوصیت آشوبگونه سیگنال های آشوب در مباحثی از پردازش تصویر مانند پنهانی کردن تصویر [۸,۹] استفاده زیادی شده است. در صورتیکه از این خصوصیت آشوبگونه در زمینه پنهان کردن تصویر استفاده چندانی نشده است.

در این روش از خصوصیت آشوبگونه توابع آشوب برای تعیین موقعیت هر پیکسل از تصویر اصلی در تصویر پوشاننده استفاده می شود. استفاده از خصوصیت آشوبگونه توابع آشوب، باعث توزیع متعادل پیکسلهای تصویر اصلی در تمام سطح تصویر پوشاننده می شود که این عمل مقاومت روش پیشنهادی را در برابر صدمات مختلف از جمله خرابی تصویر، برش از تصویر و اعمال نویز در تصویر را افزایش می دهد.

در ادامه ساختار مقاله ابتدا در بخش ۲ توضیح مختصری در مورد توابع آشوب داده می شود، شرح روش پیشنهادی در بخش ۳ قرار می گیرد. در بخش ۴ به بررسی آزمایش های انجام شده بر روی روش پیشنهادی پرداخته می شود و در نهایت در بخش ۵ نتیجه گیری از بحث انجام می گیرد.

۲. سیگنال های آشوب

سیگنال آشوب ظاهری شبیه به نویز دارد ولی در عین حال کاملا قطعی است. یعنی با داشتن مقادیر اولیه و تابع نگاشت می توان دقیقا همان مقادیر را دوباره تولید کرد. مزایای این سیگنال را در سه بخش بررسی می کنیم.

الف) حساسیت نسبت به شرایط اولیه

منظور از حساسیت نسبت به شرایط اولیه این است که هر تغیر جزیی در مقادیر اولیه باعث ایجاد اختلاف فاحشی در مقادیر بعدی تابع خواهد شد. به این معنی که اگر مقادیر اولیه سیگنال کمی تغییر کند سیگنال حاصل تفاوت بسیاری با سیگنال اولیه خواهد داشت .

ب) رفتار ظاهرا تصادفی

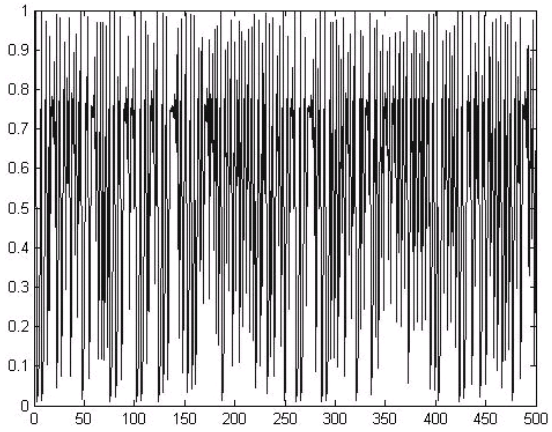
در قیاس با تولید کننده های اعداد تصادفی طبیعی که در آنها رشته اعداد تصادفی تولید شده قادر به باز تولید نیستند، روشهای مورد استفاده برای تولید اعداد تصادفی در الگوریتم های بر مبنای توابع آشوب، این امکان را به ما می دهند که در صورت داشتن مقدار اولیه و تابع نگاشت، همان اعداد تصادفی را دوباره باز تولید کنیم.

ج) عملکرد قطعی

در عین اینکه توابع آشوب ظاهری تصادفی دارند اما کاملا قطعی هستند. یعنی همواره با داشتن تابع نگاشت و مقادیر اولیه می توان یک مجموعه از مقادیر را که به ظاهر هیچ نظمی در تولید آنها وجود ندارد را تولید و دوباره همان مقادیر را بازتولید کرد. معادله۱، یکی از معروفترین سیگنالهایی که رفتار آشوب گونه دارد و به سیگنال Logistic Map معروف است را نشان می دهد.

$$X_{n+1} = rX_n(1 - X_n) \qquad (1)$$

سیگنال*Logistic Map* با مقدار اولیه $X_0 \in (0,1)$ و r = ۳.۹۹۹۹ رفتاری آشوب گونه خواهد داشت. در شکل۱ می توان رفتار این سیگنال را با مقدار اولیه $X_0 = 0.5$ و r = ۳.۹۹۹۹، مشاهده نمود.



شکل ۱– رفتار آشوب گونه سیگنال (۱) در ۵۰۰ تکرار اول

۳. شرح روش پیشنهادی

ایده کلی روش: سطح خاکستری[۲] هر پیکسل از تصویر اصلی به مبنای باینری تبدیل کرده و برای تعیین موقعیت هر بیت از این پیکسل در تصویر پوشاننده از یک تابع Logistic Map با دو مقدار مختلف برای p *(در ادامه این پارامتر شرح داده خواهد شد.)* استفاده می شود. بعد از تعیین پیکسلی از تصویر پوشاننده برای پنهان کردن یک پیکسل در آن، از ۳ بیت کم ارزش این پیکسل و از یک کلید برای رمز کردن بیتهای تصویر اصلی قبل از پنهان کردن، استفاده می شود.

شرح جزء به جزء مسئله: برای به دست آوردن مقدار اولیه تابع Logistic Map از یک کلید ۸۰ بیتی استفاده شده است. این کلید را می توان به فرم اسکی و به صورت زیر تعریف نمود(فرمول۲).

$$K = K_0, K_1, ..., K_9 (Ascii) \qquad (2)$$

که در این کلید، K_i مشخص کننده یک بلاک ۸ بیتی از کلید خواهد بود. کلید ذکر شده با فرمول۳ به فرم دودویی تبدیل می شود.

$$K = \begin{pmatrix} K_{01}, K_{02}, K_{03}, K_{04}, K_{05}, K_{06}, K_{07} \\ , K_{08}, ..., K_{91}, K_{92}, K_{93} \\ , K_{94}, K_{95}, K_{96}, K_{97}, K_{98} (Binary) \end{pmatrix}$$

که K_{ij} نشان دهنده j امین بیت از i امین بلاک از کلید می باشد.

مقدار اولیه از روی فرمول۴ به دست می آید :

$$X_0 = \begin{pmatrix} K_{01} \times 2^{79} + K_{02} \times 2^{78} + \\ .... \\ K_{11} \times 2^{71} + K_{12} \times 2^{70} + \\ .... \\ + K_{97} \times 2^{1} + K_{98} \times 2^{0} \end{pmatrix} / 2^{80}$$

همان طور که در شکل ۱ مشاهده می شود، بازه تغییرات این سیگنال [۰,۱] می باشد. این محدوده را به P بخش تقسیم می شود که اندازه هر بخش از فرمول زیر به دست می آید :

$$\varepsilon = 1/P$$

بنابراین محدوده مربوط به بخشی مانند u از فرمول زیر به دست می آید :

$$((u-1)\varepsilon \ , u\varepsilon \ )$$

مرحله ۱: بعد از تبدیل سطح خاکستری اولین پیکسل از تصویر اصلی به مبنای باینری، سری زیر بدست می آید:

$$B = B_7, B_6, B_5, B_4, B_3, B_2, B_1, B_0 (Binary) \qquad (7)$$

مرحله۲: برای رمز کردن اولین بیت از سری بدست آمده در مرحله قبل، از یک تابع Logistic Map با P برابر ۸۰ (طول کلید) استفاده می شود.

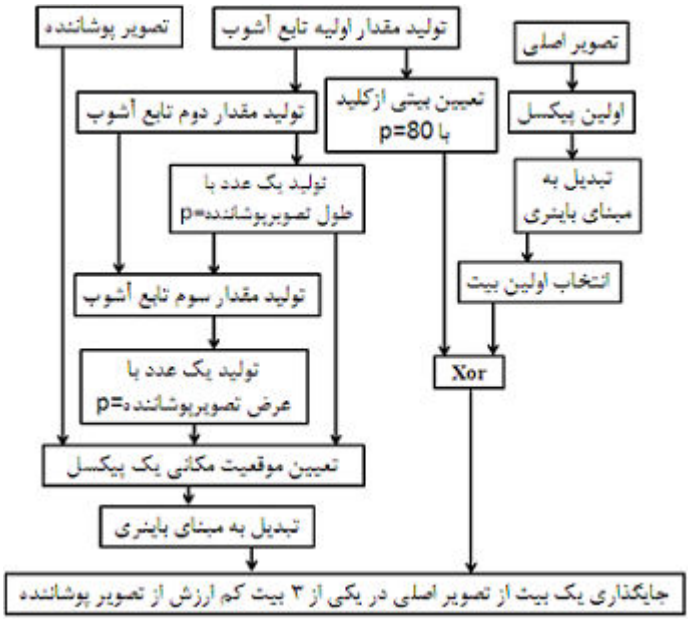
با کمک فرمول ۵ و ۶ ، بازه اولین مقدار تولیدی از تابع *Logistic Map* (X_0)تعیین می شود، که با توجه به$P=۸۰$ به طور یقین عدد بدست آمده در بازه طول کلید قرار می گیرد. بیت قرار گرفته در این بازه از کلید با اولین بیت سری B ، *xor* می شود.

مرحله ۳: تعین موقعیت طولی(عرضی)، برای مخفی کردن خروجی مرحله قبل(حاصل *xor* یک بیت از تصویر اصلی و یک بیت از کلید) در تصویر پوشاننده از یک تابع Logistic Map با Pی برابر طول تصویر (عرض تصویر) پوشاننده و فرمول های ۵و۶ استفاده می شود.

مرحله ۴: بعد از تعیین پیکسل مورد نظر از تصویر پوشاننده(مرحله ۳) برای پنهان کردن، بیت بدست آمده از مرحله ۲(بیت رمز شده از تصویر اصلی) در یکی از ۳ بیت کم ارزش این پیکسل جایگذاری می شود به شرطی که این موقعیت قبلا انتخاب نشده باشد..

مرحله ۵: مراحل ۱ تا ۴ برای تمام پیکسلها از تصویر اصلی انجام می شود.

نمودار زیر عملکرد روش پیشنهادی را برای یک پیکسل نشان می دهد(شکل۲).



شکل۲. نمودار اجرای روش پیشنهادی

۴. نتایج تجربی

در این بخش برای ارزیابی روش پیشنهادی و توانایی مقاومت این روش در برابر حملات مختلف، به انجام چند آزمایش مختلف پرداخته می شود.

۴-۱. مقاومت در برابر انواع صدمات تصویر پوشاننده

در ادامه انواع صدمات وارده به فایل پوشاننده تصویر، بعد از پنهان کردن تصویر اصلی در آن با روش پیشنهادی مورد بررسی قرار می گیرد.

سه صدمه رایج که ممکن است به تصویر بعد از پنهان شدن، وارد شود، شامل:

خرابی تصویر[۳]، بریده شدن از تصویر[۴] و اعمال نویز در تصویر[۵] می باشند.

برای آزمایش مقاومت روش پیشنهادی در برابر صدمات فوق از تصویر ۳ استفاده می شود. تصویر a.۳ تصویر Lena برای پنهان شدن می باشد(۱۲۸*۱۲۸) و در شکل b.۳ از تصویر Pepper به عنوان پوشاننده استفاده می شود(۲۵۶*۲۵۶).

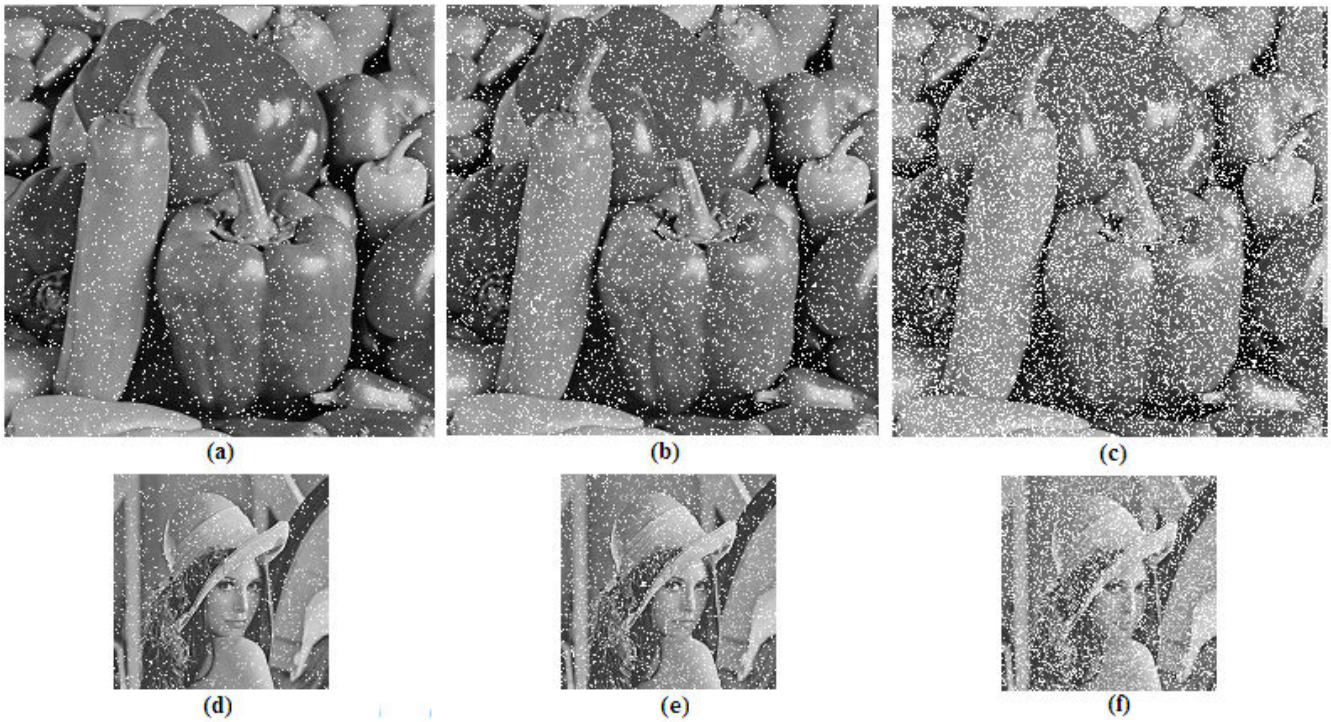
(a)

(b)

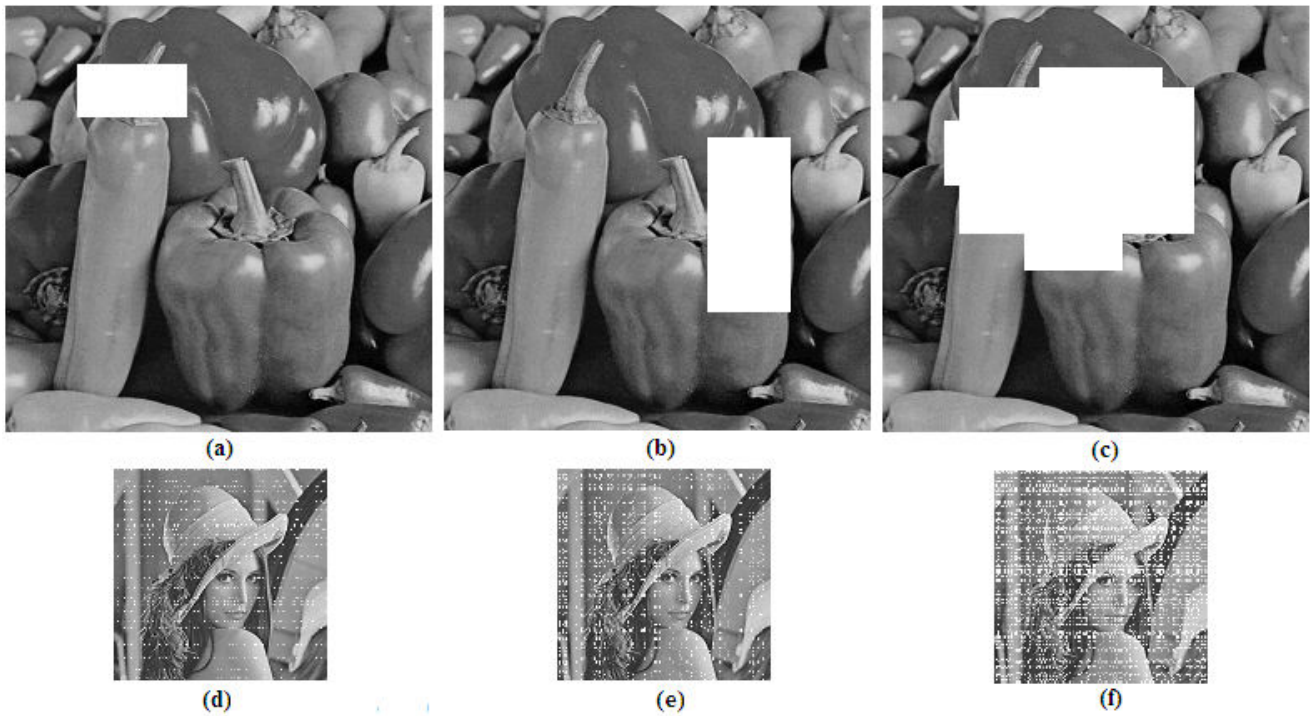
شکل۳. a)تصویر اصلی(۱۲۸*۱۲۸) b)تصویر پوشاننده(۲۵۶*۲۵۶)

a.۴ ، b.۴ ، c.۴ و a.۵ ، b.۵، c.۵ و a.۶ ، b.۶ و c.۶ به ترتیب تصاویر شکل b.۳ بعد از پنهان کردن شکل a.۳ در آن با روش پیشنهادی و با اعمال ۵ ، ۱۰ ، ۳۰ درصد نویز و ۵ ، ۱۰ ، ۳۰ درصد برش و ۵ ، ۱۰ ، ۳۰ درصد خرابی می باشند.

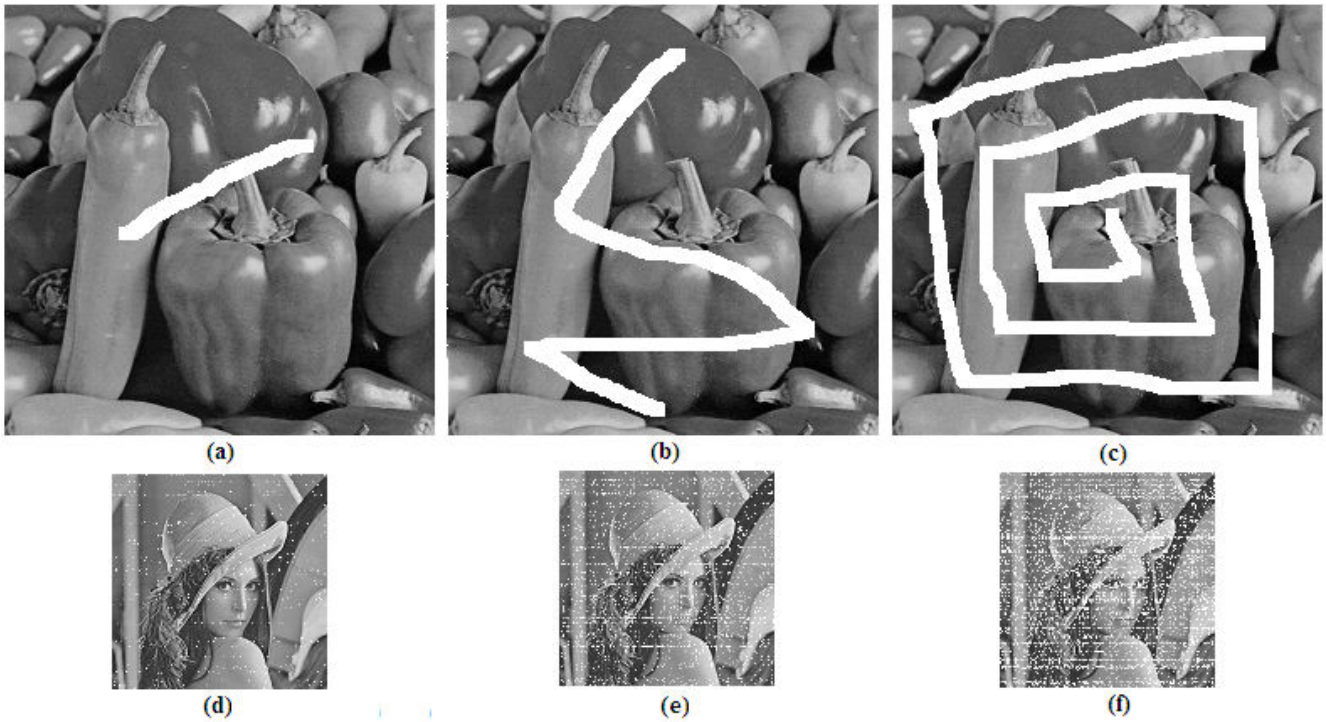
تصاویر d.۴ ، e.۴ ، f.۴ و d.۵ ، e.۵، f.۵ و d.۶ ، e.۶ ، f.۶ نیز به ترتیب نتایج آشکار کردن تصویر a.۳ از تصاویر a.۴ ، b.۴ ، c.۴ و a.۵ ، b.۵، c.۵ و a.۶ ، b.۶ و c.۶ می باشند. در تمامی تصاویر خروجی عکس Lena به وضوح قابل تشخیص می باشد و با اعمال هر کدام از صدمات وارده حتی با درصد بالا کلیات تصویر خروجی حفظ شده است و فقط جزئیاتی از تصویر از بین رفته است که تشخیص مفهوم اصلی تصویر را دشوار نمی کند. دلیل اصلی این موضوع را می توان در توزیع مناسب پیکسل های تصویر اصلی(Lena) در تصویر پوشاننده بوسیله روش پیشنهادی جستجو کرد.



شکل۴. a,b,c)تصویر پوشاننده بعد از پنهان کردن تصویر a.۳ در ان و با اعمال ۵و۱۰و۳۰ درصد نویز d,e,f) تصویر آشکار سازی شده



شکل۵. a,b,c)تصویر پوشاننده بعد از پنهان کردن تصویر a.۳ در ان و با ۵و۱۰و۳۰ درصد برش d,e,f) تصویر آشکار سازی شده



شکل۶. a,b,c)تصویر پوشاننده بعد از پنهان کردن تصویر a.۳ در آن و با اعمال ۵و۱۰و۳۰ درصد خرابی d,e,f)تصویر آشکار سازی شده

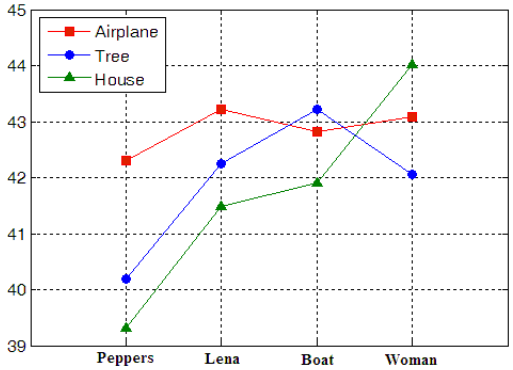
۴-۲. نسبت سیگنال به نویز[۶]

در این بخش از PSNR به عنوان مقیاس برای کیفیت تصویر Stego-Image استفاده شده است. مقدار PSNR که به معنای نسبت سیگنال به نویز می باشد، برای تصاویر از رابطه (۸) محاسبه می‌شود[۱۰,۱۱].

$$PSNR=10*\log_{10}\left(\frac{255^2}{\frac{1}{W*H}\sum_{i=1}^{W}\sum_{j=1}^{H}(O_{ij}-D_{ij})^2}\right)$$

که در این فرمول O_{ij} و D_{ij} به ترتیب مشخص کننده مقادیر سطح خاکستری پیکسل‌های تصویر اصلی و Stego-Image می‌باشند و همچنین H و W به ترتیب مشخص کننده طول و عرض تصاویر خواهند بود.

برای تعیین PSNR روش پیشنهادی از ۴ تصویر Boat،Lena،Peppers و Woman به عنوان تصویر پوشاننده با ابعاد(۲۵۶*۲۵۶) و از ۳ تصویرAirplane، Tree و House به عنوان تصویر اصلی با ابعاد (۱۲۸*۱۲۸) استفاده می شود. نتایج حاصل در شکل ۷ قابل مشاهده می باشد.



شکل۷. نمودار PSNR برای روش پیشنهادی

در ادامه، برای مقایسه PSNR روش پیشنهادی با روشهای دیگر از ۴ تصویر Airplane، Peppers،House و Boat با ابعاد(۲۵۶*۲۵۶) به عنوان تصویر اصلی برای پنهان کردن استفاده می شود. برای تصویر پوشاننده نیز از تصویر Lena با ابعاد (۵۱۲*۵۱۲) استفاده شده است. جدول۱ نشان دهنده PSNR برای روش پیشنهادی و روشهای ارائه شده در مراجع[۱,۱۲,۱۳] می باشد.
همانطور که در جدول۱ نشان داده شده است، روش پیشنهادی از روشهای ارائه شده در مراجع [۱۲,۱۳] نتایج کاملا بهتر و از روش ارائه شده در مرجع [۱] در چند حالت نتیجه بهتری می دهد.

جدول۱. مقایسه PSNR روش پیشنهادی با روشهای ارائه شده در مراجع [۱,۱۲,۱۳]

روش / تصویر اصلی	مرجع [۱۳]	مرجع [۱۲]	مرجع [۱]	روش پیشنهادی
Airplane	۳۹.۳۶	۴۱.۸۶	۴۴.۱۴	۴۴.۴۱
House	۴۱.۶۴	۴۱.۸۸	۴۱.۹۳	۴۲.۱۲
Peppers	۳۷.۶۶	۴۱.۸۷	۴۴.۱۲	۴۳.۹۹
Boat	۳۸.۷۹	۴۱.۸۷	۴۳.۷۶	۴۳.۱۵

۵. نتیجه گیری

در این مقاله یک روش جدید برای پنهان کردن تصویر ارائه شده است. ایده اصلی روش پیشنهادی تعیین موقعیت پیکسلهای تصویر اصلی در تصویر پوشاننده بوسیله تابع آشوب می باشد. مزیت اصلی روش پیشنهادی در توزیع متناسب پیکسلهای تصویر اصلی در تمام سطح تصویر پوشاننده است، رمز کردن هر یک از بیتهای تصویر اصلی با یک بیت از کلید، قبل از عمل پنهان کردن، سبب افزایش امنیت روش پیشنهادی می شود . همانطور که در بخش نتایج تجربی نیز مشاهده شد، ویژگیهای ذکر شده سبب مقاومت روش پیشنهادی در برابر صدمات مختلف مثل خرابی تصویر، برش از تصویر و اعمال نویز در تصویر می شود. مقدار بالای PSNR در حدود ۴۴.۴۱ نیز یکی دیگر از دلایل مناسب بودن روش پیشنهادی است.

مراجع

[۱] Ran-Zan Wang, Yao-De Tsai, "An image-hiding method with high hiding capacity based on best-block matching and k-means clustering", Pattern Recognition, Volume ٤٠, Issue ٢, February ٢٠٠٧, pp.٣٩٨-٤٠٩

[۲] Chin-Chen Chang, Ju-Yuan Hsiao, Chi-Shiang Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition, Volume ٣٦, Issue ٧, July ٢٠٠٣, pp. ١٥٨٣-١٥٩٥

[۳] E. Besdok, "Hiding information in multispectral spatial images",AEU - International Journal of Electronics and Communications, Volume ٥٩, Issue ١, ١ March ٢٠٠٥, pp. ١٥-٢٤

[٤] Yen-Ping Chu, Yang-Kuan Chan "Image Hiding Based on a Hybrid Technique of VQ Compression and Discrete Wavelet Transformation", Int. Computer Symposium, Dec. ١٥-١٧, ٢٠٠٤, Taipei, Taiwan, pp.٣١٣-٣١٧

[٥] Chin-Chen Chang, Chi-Shiang Chan, Yi-Hsuan Fan, "Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels", Pattern Recognition, Volume ٣٩, Issue ٦, June ٢٠٠٦, pp. ١١٥٥-١١٦٧

[٦] LIU Bin, LI Zhitang, "An Image Encryption Method Based on Bit Plane Hiding Technology ",Wuhan University Journal of Natural Sciences,Vol. ١١ No. ٥, ٢٠٠٦, pp.١٢٨٣-١٢٨٦

[٧] LIU Nian-sheng, GUO Dong-hui "A New Images Hiding Scheme Based on Chaotic Sequences ",Wuhan University Journal of Natural Sciences,Vol. ١٠ No. ١, ٢٠٠٥, pp.٣٠٣-٣٠٦

[۸] رسول عنایتی فر، مرتضی صابری کمرپشتی و محمدرضا میبدی، "پنهانی سازی تصویر با کمک تابع آشوب و درخت جستجوی دودیی"، پنجمین کنفرانس بینایی ماشین و پردازش تصویر، تبریز، ایران، آبان ۱۳۸۷.

[۹] H.S. Kwok, Wallace K.S. Tang," A fast image encryption system based on chaotic maps with finite precision representation", Chaos, Solitons and Fractals, November, ۲۰۰۷, pp.۱۵۱۸–۱۵۲۹

[۱۰] Anderson, R.J., Petitcolas, F.A.P., "On the limits of Steganography" IEEE J. Select, ۱۹۹٦, pp.٤٧٤-٤٨١.

[۱۱] Bender, W., Gruhl, D., Morimoto, N., Lu, A., "Techniques for data hiding". IBM Syst. J,۱۹۹٦, pp.۳۱۳–۳۳٦.

[۱۲] Yuan-Hui Yu, Chin-Chen Chang, Iuon-Chang Lin, "A new steganographic method for color and grayscale image hiding ",Computer Vision and Image Understanding , November ۲۰۰۷, pp. ۱۸۳–۱۹٤

[۱۳] Yu-Shan Wu, Chih-Ching Thien, Ja-Chen Lin, "Sharing and hiding secret images with size constraint", Pattern Recognition, January ۲۰۰٤, pp. ۱۳۷۷ – ۱۳۸۵

زیر نویس

[۱] Image Encryption
[۲] Gray Level
[۳] Corrupted image
[٤] Cutting image
[٥] Noisy image
[٦] Peak Signal to Noise Ratio (PSNR)