رمزنگاری تصاویر با استفاده از توابع آشوب

الهه حسینی ، شهریار برادران شکوهی

دانشگاه علم و صنعت ایران، دانشکده برق

hoseini_1377@yahoo.com و bshokouhi@iust.ac.ir

چکیده:در این مقاله سعی بر این بوده که با استفاده از ویژگیهای بسیار خوب سیستمهای آشوب به طرح یک روش رمزنگاری آشوبگون تصویر بپردازیم. در اینجا از سیستم آشوب لورنز استفاده کرده ایم . الگوریتم حاصل هم بر روی تصاویر خاکستری و هم تصاویر رنگی قابل اجرا است.

کلید واژه : رمزنگاری ، تئوری آشوب ، منحنی جذب عجیب، پردازش تصویر

۱- مقدمه :

با توجه به کاربرد روزافزون کامپیوتر حفظ امنیت و تأیید صحت تصاویر نیز روز به روز اهمیت بیشتری می یابد . تصاویر مخابره شده ممکن است کاربردهایی چون کاربرد تجاری ، نظامی و یا حتی کاربردهای پزشکی داشته باشند که در هر صورت حفظ امنیت آنها و جلوگیری از دسترسی های غیر مجاز به این تصاویر رمزنگاری آنها را قبل از ارسال روی شبکه ضروری می کند ولی به دلیل ویژگیهای تصاویر خصوصاً حجم زیاد داده های تصویری و ویدئویی استفاده از الگوریتمهای کلاسیک رمز نگاری متن مانند RSA ، DES و ... در این موارد ناکارآمد، چون اولاً رمزکردن حجم زیاد داده های تصویری به این طریق بسیار وقتگیر خواهد بود و خصوصاً در کاربردهای بلادرنگ عملی نیست و دومین مشکلی که این الگوریتمها دارند طول کلید آنهاست که با توجه به حجم داده های رمزشده استفاده از کلیدهای با طول محدود باعث ضربه پذیری روش در برابر حملات متن رمزشده می گردد.برای غلبه بر این مشکلات افراد بسیاری به ارائه روشهای نوینی در رمزنگاری تصویر پرداخته اند. [۱،۲و۳]

در این مقاله سعی بر این بوده که با استفاده از ویژگیهای توابع آشوب و امکان تولید کلیدهایی با طول بینهایت (بسیار بزرگ) الگوریتمی ساده ، سریع و ایمن برای رمزنگاری داده های تصویری ایجاد شود.همچنین با توجه به فضای بزرگ کلید در توابع آشوب این روش در برابر حملاتی چون حمله Brute force نیز بسیار مقاوم است. در انتها باید گفت که علاوه بر حملات عمدی این الگوریتم نسبت به تغییراتی بسیار کوچک در کلید بسیار حساس بوده حتی با در دست داشتن مقادیر تقریبی کلید امکان شکستن رمز برای حمله گران وجود ندارد.

بخش دوم این مقاله به بیان ویژگیهای سیستمهای آشوب و سیستم آشوب لورنز اختصاص یافته است. در بخش سوم روشهای رمزنگاری تصویر و ویژگی های خاص تصویر از نظر رمزنگاری را مورد بررسی قرار داده است. در بخش چهارم روش رمزنگاری پیشنهادی بیان شده است.در بخش پنجم نتایج شبیه سازی ارائه شده و بخش ششم به جمع بندی کار اختصاص یافته است.

۲- سیستمهای آشوب

آشوب پدیده ای است که در سیستمهای غیر خطی تعریف پذیر رخ می دهد که حساسیت زیاد به شرایط اولیه و رفتار شبه تصادفی از خود نشان می دهند. چنین سیستمهایی در حالتی که شرایط معادلات نمایی لیاپانوف را برآورده سازند در مد آشوب به حال پایدار باقی خواهند ماند. ویژگی مهمی که باعث شده این پدیده برای رمزنگاری بسیار مورد توجه قرار بگیرد تعریف پذیری سیستم در عین رفتار شبه تصادفی آن است که باعث می گردد خروجی سیستم از دید حمله گران تصادفی به نظر برسد در حالی که از دید گشاینده رمز سیستمی تعریف پذیر بوده و لذا قابل رمزگشایی است.

الگوریتمهای رمزنگاری بسیاری بر اساس تئوری آشوب طرح شده اند [۴،۵و۶] و برخی از آنها به گونه ای گسترش یافته اند که علاوه بر داده های متنی قادر به رمزنگاری تصاویر هم هستند ولی چون رمزنگاری تصویر باید قابلیت های خاصی همچون سرعت مناسب برای رمزکردن داده های تصویری با حجم زیاد را داشته باشند

اغلب ، روشهای رمزکردن متن برای پیاده سازی روی تصویر مناسب نیستند .

دو روش عمده در رمز نگاری آشوبگون تصویر وجود دارد ؛ رمزنگاری بلوکی و رمزنگاری پی در پی که رمزنگاری بلوکی بیشتر مورد توجه بوده ولی هر دو شیوه مزایا و شایستگی های خاصی را دارا می باشد و در کاربردهای مختلفی تحت شرایط مختلف می توانند به کار گرفته شوند .

۲-۱- تحلیل سیستم لورنز :

سیستم لورنز از اولین سیستمهای شناخته شده آشوبگون است که در ابتدا برای تحلیل جریانات هوایی و پیش بینی وضع هوا ابداع شد ولی بسیاری از سیستمهای هیدرو دینامیکی ، مکانیکی ، دینامیکی و مسائل لیزری و نوری نیز می توان به وسیلهٔ آن مدل و تحلیل کرد .معادلات حاکم بر سیستم به این شرح است :

$$\frac{dx}{dt} = \sigma(-x + y)$$
$$\frac{dy}{dt} = rx - y - xz$$
$$\frac{dz}{dt} = -bz + xy$$

این سیستم شامل سه پارامتر کنترلی σ ، r و b است که هر سه مقادیر مثبتی اختیار می کنند .

پارامتر r ؛ برای عدد رایلی ، σ به عنوان عدد پرانتل[1] و نسبت هندسی یا b این سیستم با تغییر هر یک از پارامترها رفتارهای گوناگونی از خود بروز می دهد . سیستم لورنز یک سیستم دینامیکی غیرخطی زمان پیوسته است که با مقادیر خاصی برای پارامترهایش رفتار آشوبگون از خود بروز می دهد . در حالتی که پارامتر r به بازهٔ $[0,1]$ محدود شده باشد منبع $(0,0,0)$ در حالت عمومی پایدار خواهد بود . در $r=1$ سیستم بین دو نقطهٔ ایستای متقارن C_1 و C_2 با مختصات $\left(\pm\sqrt{b(r-1)},\pm\sqrt{b(r-1)},r-1\right)$ دو شاخه می گردد البته در صورتی که C_2 در ناحیهٔ $x>0$ قرارگرفته باشد .

این نقاط ایستا تا مقدار $r = r_H = \frac{\sigma(\sigma+b+3)}{\sigma-b-1}$ پایدار می مانند . [۷]

۳- سایفرهای رمزنگاری تصویر

برخلاف پیامهای متنی داده های تصویری ویژگی های خاص خود را همانند حجیم بودن ، اضافات زیاد[2] و همبستگی زیاد بین نقاط تصویر دارند که باعث می شود که اجرای روشهای رمزنگاری سنتی روی تصاویر بسیار سخت و کند باشد گاهی اوقات کاربردهای تصویر نیازهای خاصی دارند همانند بلادرنگ بودن ، نگهداری همسان[3] ، یکنواختی شکل تصویر[4] ، فشردگی داده ها برای انتقال و نظایر آن . گاهی اوقات برآوردن این نیاز ها به همراه نیاز به امنیت زیاد و کیفیت بالا مشکلاتی را برای بلادرنگ بودن ارسال تصاویر ایجاد می کند برای مثال اگر نیاز باشد تصویری را رمز کرده و فشرده نیز بکنیم برای روشهای سنتی رمزنگاری تصویر قابلیت فشرده سازی بسیار کمی وجود دارد به عبارت دیگر فشرده سازی باعث عدم صحت رمزگشایی و اتلاف در شیوهٔ رمزگشایی می شود خصوصاً اگر از یک روش رمزنگاری با امنیت بالا استفاده شده باشد حل مشکل ناسازگاری بین قابلیت فشرده سازی و امنیت اگر ممکن نباشد بسیار سخت است . ویژگی های رمزنگاری تصویر را می توان به صورت زیر خلاصه نمود :

اضافات زیاد وظرفیت حجیم عموماً داده های تصاویر رمزشده را در مقابل تحلیل گران و حملات آسیب پذیر می کند . به دلیل ظرفیت حجیم رقبا می توانند نمونه هایی کافی از متن رمز شده را برای تحلیلات آماری حتی از یک تصویر بدست آورند در حالی که داده های تصویری اضافات بسیار زیادی دارند نقاط مجاور هم تصویر احتمالاً مقادیر خاکستری شبیه به همی را دارا هستند ، یا بلوکهای تصویر الگوهای مشابه ای را دارند ، که اغلب

[1] Prandtl

[2] High Redundancy
[3] Fidelity Reservation
[4] Image Format Consistence

تصاویری با الگوهای خاص در خود جای می دهد که منجر به نشت اسناد می شود .
در بین نقاط مجاور هم داده های تصویری همبستگی های بسیار خوبی وجود دارد که باعث می شود در هم ریزی داده های تصویری بسیار کند باشد . تحلیل آماری روی تعداد زیادی از تصاویر نشان داده است که نقاط مجاور هشت تا شانزده تایی به شکل افقی ، عمودی و حتی قطری ، هم در تصاویر طبیعی در گرافیکهای کامپیوتری به شدت با هم بستگی دارند . مطابق تئوری اطلاعات شانون سیستم رمزنگاری ایمن باید شرایطی را روی انتروپی اطلاعات اجرا کند .

$$E(p \mid c) = E(p)$$

P متن ساده و C متن رمز شده است ، که طبق آن تصویر رمز شده نباید هیچ اطلاعاتی در مورد تصویر رمز نشده بدهد . برای برآورده شدن این نیاز تصویر رمز شده باید تا حد امکان تصادفی باشد از آنجا که یک پیام که توزیع غیر یکنواختی دارد یک پیشینهٔ عدم قطعیت دارد ، یک تصویر رمزشدهٔ ایده آل باید یک هیستوگرام متعادلی داشته باشد و هر دو نقطهٔ مجاور باید از نظر آماری کاملاً غیر همبسته باشند این هدف ، تحت تعداد محدودی دورهای جابجایی و پخشی به سادگی قابل دستیابی نیست .
ظرفیت حجیم داده های تصویری رمزنگاری بلادرنگ تصاویر را بسیار سخت می کند . در مقایسه با متن ، داده های تصویری بصورت غیر قابل باوری بزرگ هستند برای مثال یک تصویر رنگی بیست وچهار بیتی با اندازهٔ نقاط ۵۱۲×۵۱۲ به فضایی برابر با ۷۶۸=۸÷۲۴×۵۱۲×۵۱۲ کیلو بایت نیاز دارد و لذا یک ثانیه تصویر متحرک نوزده مگا بایت حافظه نیاز خواهد داشت و این در حالی است که پردازشهای بلادرنگ برای اغلب کاربردهای تصاویر مانند ویدئو کنفرانس ، مراقبتهای تصویری و ... مورد نیاز است . مقادیر زیاد داده های تصویری پردازشهای بسیار زیادی را برای رمزنگاری و رمزگشایی تصاویر ایجاب می کند رمزنگاری در طی کدینگ فاز و بعد از آن و رمزگشایی در طی دیکد کردن فاز یا بعد از آن مشکل را پیچیده تر می کند . اگر یک الگوریتم رمزگشایی با وجود امنیت زیادش بسیار کند اجرا شود برای کاربردهای بلادرنگ تصویری ارزش عملی کمی خواهد داشت به همین علت است که الگوریتمهایی همچون RSA ،IDEA و DES برای این منظور انتخاب مناسبی به شمار نمی آیند .
رمزنگاری تصویر اغلب به همراه فشرده سازی داده ها انجام می شود. تقریباً در همهٔ موارد داده ها قبل از آنکه ذخیره شوند یا انتقال داده شوند فشرده می گردند این بدلیل حجم داده های تصویری و اضافات بسیار زیاد آنهاست بنابراین آمیختن نیازهای امنینی با سیستمهای فشرده سازی داده اهمیت بسیار دارد . مشکل اساسی این است که چگونه در حالی که هزینهٔ محاسبات را بدون کاهش کیفیت عملکرد فشرده سازی کاهش می دهیم از امنیت مناسب نیز اطمینان حاصل کنیم .
در کاربرد تصویر تبدیل شکل فایل یک عمل همیشگی است . رمزنگاری تصویر نیز باید بشکلی طرح شود که چنین اعمالی بر روی آن اثر نداشته باشد . به همین علت محتویات داده ها ی تصویر رمزشده و سرآیند[5] و داده های کنترلی رمز نشده باقی می مانند .
بینایی انسان نسبت به نویز و تخریب جزئی تصویر مقاومت زیادی دارد و برای محافظت از تصویر باید بیت هایی که با هم همبستگی زیادی دارند بخوبی رمز گردند . در صورتی که در روشهای سنتی رمزنگاری به همهٔ بیتهای داده به شکل یکسانی نگریسته می شود و بنابراین لازم است که توان محاسباتی زیادی برای رمزنگاری همهٔ بیتهای تصویر صرف شود که اغلب اوقات این حجم محاسبات غیر ضروری است .
در رابطه با امنیت ، داده های تصویری به اندازهٔ دادهٔ متنی حساس نیستند . امنیت تصویر کاملاً با موقعیت واقعی آن در کاربرد تصویر تعریف می شود. در اکثر موارد به غیر از کاربرد های جاسوسی ، نظامی ، ویدئو کنفرانسها و کاربردهای تجاری خاص داده های تصویری ارزش خیلی زیادی ندارند و لذا حملاتی با هزینهٔ زیاد به داده

[5] Header

های تصویری اغلب ارزشمند نیستند غالباً محافظت همانندهی و کیفیت تصاویر از محافظت از امنیت اطلاعاتشان مهمتر است . در برخی شرایط حتی امکان دارد بخشهایی از داده نیز نشت کند ولی این امر در داده های متنی کاملاً غیر مجاز است چون پس از نشت بخشی از داده حمله به کل داده ها و شکستن رمز آنها کاری کاملاً ساده خواهد بود . در حال حاضر الگوریتمهای رمزنگاری تصویری که قادر باشد همهٔ موارد فوق الذکر را اجرا کند ولی روشهای رمزنگاری آشوبگون ، بسیاری از این نیازها را تا حد خوبی برآورده می کند خصوصاً این روش رمزنگاری موازنهٔ خوبی بین امنیت ، سرعت و انعطاف پذیری را ایجاد می کند.[۸]

۴- الگوریتم رمزنگاری آشوبگون تصویر

الگوریتمهای رمزنگاری آشوبگون به دو صورت بلوکی و پی در پی وجود دارند که هر دو عملکرد خوبی در این زمینه از خود نشان می دهند . در این مقاله یک روش پی در پی ارائه شده است که در ادامه به شرح نحوه رمزنگاری و رمزگشایی می پردازیم.

۴-۱- الگوریتم رمزنگاری

در روش پیشنهادی ابتدا با استفاده از سیستم آشوب لورنز یک کلید رمزنگاری با ابعاد ی برابر ابعاد تصویر مورد نظر تولید کرده به گونه ای که هر یک از حروف این کلیدعددی در بازه [۱،۲۵۶] هستند سپس با استفاده از سایفر بلوکی ضربی و عملگر هنگ که در اینجا برای جلوگیری از واگرا شدن حاصل رمزنگاری ضروری است ، طبق رابطه

$$C = E(P,k)$$

تصویر اولیه رمز می گردد.[۹] البته در اینجا فقط یک بلوک داریم .این شیوه را می توان با تولید کلیدهایی با اندازه های کوچکتر در تعداد بلوکهای بیشتری هم اعمال نمود همچنین می توان با استفاده از این الگوریتم تصاویر رنگی را هم رمز نمود.

برای مدولاسیون از هنگ ۲۵۷ که عددی اول است استفاده شده و برای معکوس پذیر بودن کامل کلید بجای تمامی صفرها از ۲۵۶ استفاده شده (البته می توان برای جلوگیری از بالا رفتن فرکانس تکرار این عدد از یک الگوی معین برای پخش صفرها بین تمامی ۲۵۶ عدد دیگر استفاده کرد که با اینکار می توان کلیدی با توزیع یکنواخت تولید کرد که مناسبتر است ولی در مقابل هزینه های محاسباتی بیشتری را در رمزنگاری و رمزگشایی ایجاد می کند.

۴-۲- الگوریتم رمزگشایی

برای رمزگشایی تصویر رمزشده با استنفاده از یک سیستم آشوب مشابه در گیرنده و با بکارگیری مقدار اولیه یکسان و با توجه به روشهای معکوس کردن در حوزه هنگ اعداد اول ، کلید رمزگشایی تولید می گردد .یکی از مزایای مهم استفاده از سیستم آشوب ، تسهیلات شیوه مدیریت کلید است زیرا در این روش تنها نیاز به محافظت و انتقال ایمن کلیدهای سری (پارامترها و مقادیر اولیه سیستم آشوب) است که حجم کمی دارد و بنابراین نه تنها برای نگهداری از آن حافظه کمی نیاز است بلکه در هنگام انتقال آن هم اطمینان بیشتری وجود دارد چون امکان دسترسی غیر مجاز به کلیدهای کوتاه نسبت به کلیدهایی با طول بزرگ در هنگام ارسال و دریافت روی کانال کاهش چشمگیری دارد در واقع حروف کلید رمزگشایی معکوس شده حروف کلید رمزنگاری در هنگ اعداد اول هستند و عمل رمزگشایی با بکار گیری کلید مناسب و تکرار مجدد الگوریتم رمزنگاری بر روی تصویر رمزشده اجرا می شود یعنی

$$P = D(C,k) = E(C,k')$$

۵- نتایج شبیه سازی

برای شبیه سازی از سیستم لورنز با پارامترهای $\sigma = 10, r = 28, b = \frac{8}{3}$ و مقادیر اولیه (۰،۰،۰) و روش Runge_Kutta استفاده شده است .نتایج اعمال الگوریتم بر روی تصویرخاکستری و رنگی Lena با ابعاد ۱۲۸×۱۲۸ در شکلهای[۴-۱] آورده شده است برای مشخص شدن کیفیت الگوریتم هیستوگرام تصاویر هم در کنار آنها نمایش داده شده است . توزیع نسبتاً یکنواخت هیستوگرام تصاویر رمز شده نشان از کیفیت خوب روش دارد.

به دلیل حساسیت بسیار بالای روش به مقادیر اولیه و پارامترهای سیستم (کلید) که حتی تغییر چند ده هزارم کلید هم باعث تولید سریهای تصادفی کاملاً متفاوت می شود و با توجه به فضای کلید ، که به دلیل امکان تغییرات پیوسته طیف وسیعی را در بر می گیرد، این روش از امنیت بالایی در برابر حملات برخوردار است.

همچنین همبستگی بین نقاط تصویر رمز شده نسبت به تصویر اصلی بسیار کمتر است که نشان از امنیت خوب الگوریتم به دلیل قابلیت ایجاد گیجی و پخشی مناسب در تصویر رمزشده است.

۶- نتیجه

در این مقاله یک روش رمزنگاری تصویر با استفاده از سیستم آشوب لورنز ارائه شد و نشان دادیم که این روش نه تنها بسیار ساده است بلکه از امنیت بالایی نیز برخوردار است که این امر ناشی از ویژگیهای سیستمهای آشوب و تناسب آن با داده های تصویری با حجم زیاد اطلاعات است . از دیگر مزایای این الگوریتم امکان بکارگیری آن در تصاویر خاکستری و رنگی است.

۷- منابع

[1] Shujun Li 1 and Xuan Zheng , "On the Security of an Image Encryption Method", Proceedings of the 2002 IEEE International Conference on Image Processing (ICIP 2002), vol. 2, pp. 925- 928, 2002.

[2] H.S. Kwok, Wallace K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", Elsevier, Chaos, Solitons and Fractals,2006.

[3] Zhi-Hong Guan , Fangjun Huang , Wenjie Guan, "Chaos-based image encryption algorithm", Elsevier, Physics Letters A Vol 346 pp. 153–157,2005.

[4] Shiguo Lian_, JinshengSun, Zhiquan Wang, "Security analysis of a chaos-based image encryption algorithm", Elsevier, Physica A, Vol. 351, pp. 645–661,2005.

[5] B. Schneier, "Applied Cryptography Second Edition : protocols, algorithms, and source code in C", ISBN 9971-51-348-X, John Wiley & Sons,1996.

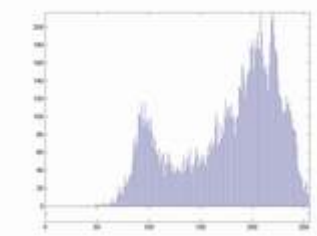
[6] Fethi Belkhouche, Uvais Qidwai, Ibrahim Gokcen, Dale Joachim, "Binary Image Transformation Using Two-Dimensional Chaotic Maps", IEEE, Proceedings of the 17th International Conference on Pattern Recognition (ICPR), 2004.

[7] Po-Han Lee,1 Soo-Chang Pei,2 and Yih-Yuh Chen1, "Generating Chaotic Stream Ciphers Using Chaotic Systems", CHINESE JOURNAL OF PHYSICS VOL. 41 , NO. 6 DECEMBER 2003.

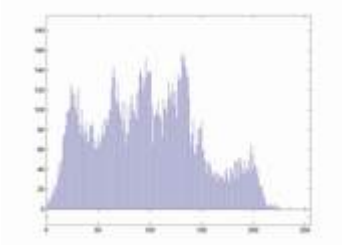
[8] Eduardo Bayro-Corrochano (Editor), "Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neural Computing and Robotics", Springer, 2003.

[۹] دکتر محمدرضا عارف، " اصول رمزنگاری، قسمت اول " ، دانشکده مهندسی برق دانشگاه خواجه نصیرالدین طوسی، گروه مخابرات، سال ۱۳۶۷.

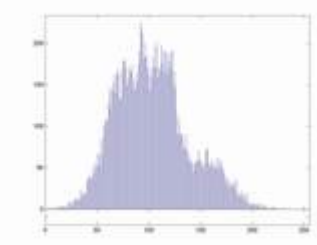
اتف



ب

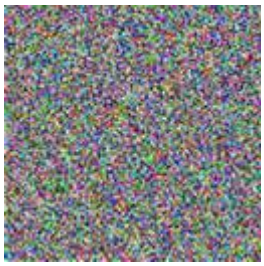


ج

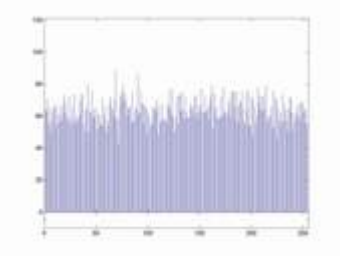


د

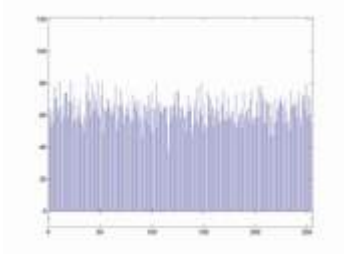
شکل (۱) : تصویر اصلی و هیستوگرام سه صفحه رنگ RGB



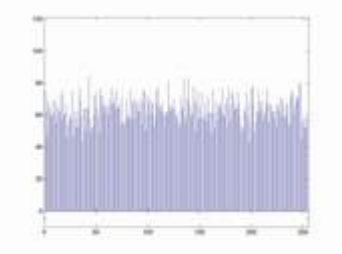
اتف



ب



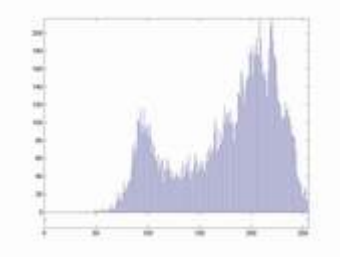
ج



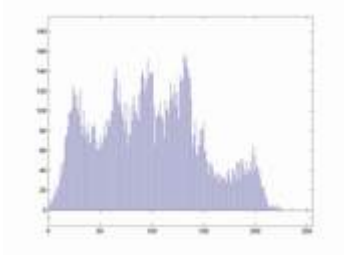
د

شکل (۲) : تصویر رمزشده و هیستوگرام سه صفحه رنگ RGB

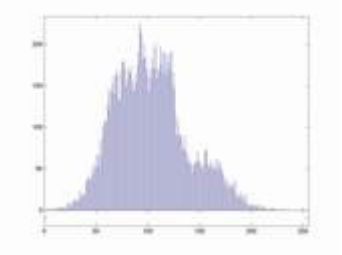
اتف



ب

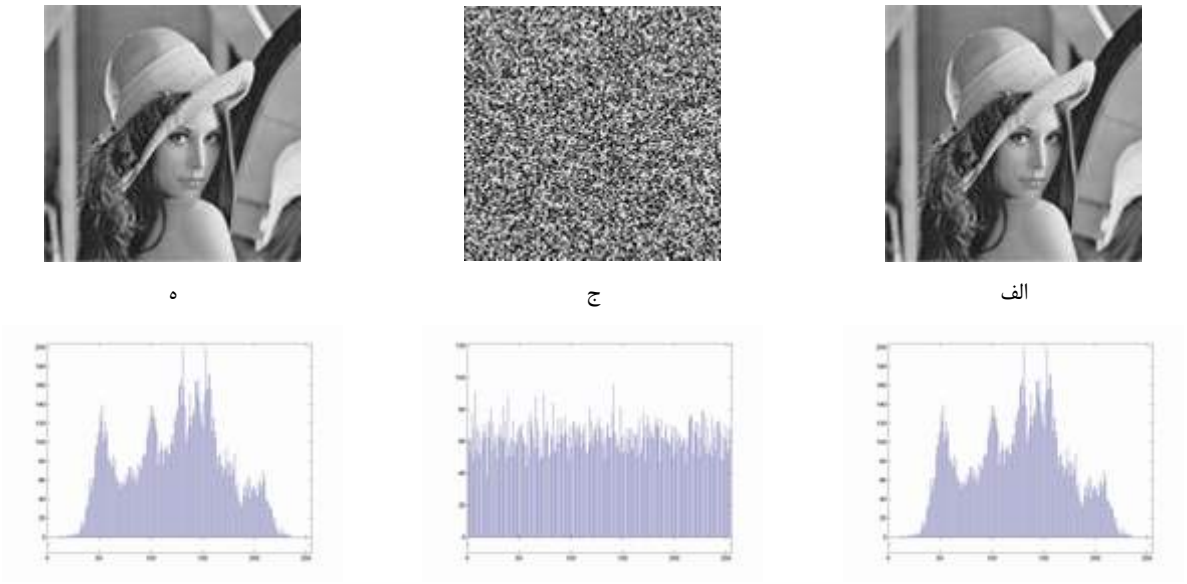


ج



د

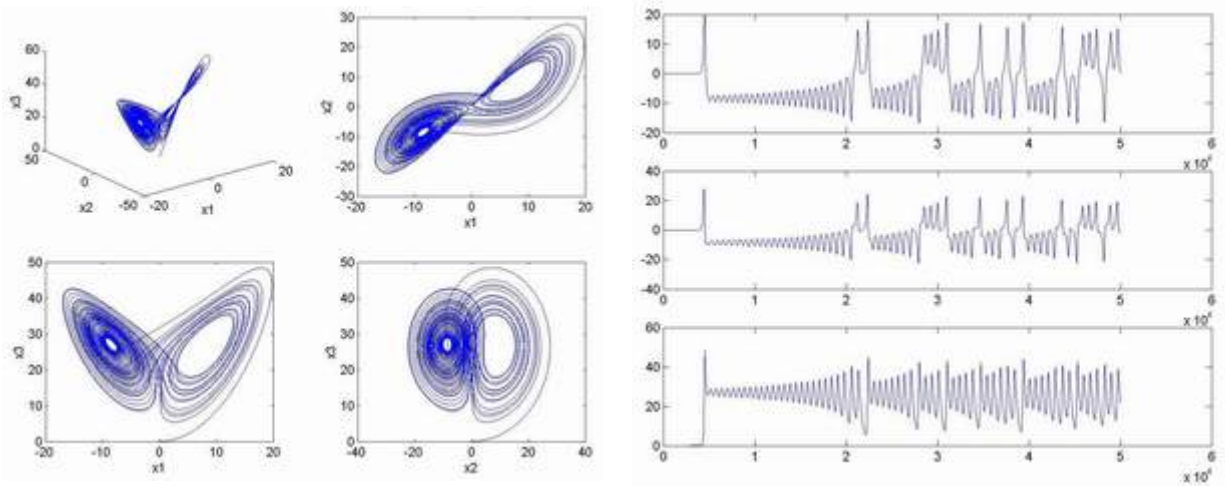
شکل (۳) : تصویررمزگشایی شده و هیستوگرام سه صفحه رنگ RGB



الف ج ه

ب د و

شکل (۴) : الف - تصویر خاکستری ، ج – تصویر رمز شده د- تصویر رمزگشایی شده ، در زیر هر تصویر هیستوگرام مربوط به آن رسم شده



الف ب

شکل (۵) : الف – سریهای آشوب زمانی مولد کلید ، ب – منحنیهای جذب عجیب مربوط به سیستم لورنز