پنجمین کنفرانس انجمن رمز ایران
انجمن رمز ایران
Iranian Society of Cryptology
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

طراحی جعبه جایگزینی(S-box) سیستم رمزنگاری AES با استفاده از نگاشت آشوبی

پیام امانی
دانشکده مهندسی برق
دانشگاه صنعتی خواجه نصیرالدین طوسی
p_amani@ieee.org

حمیدخالوزاده
دانشکده مهندسی برق
دانشگاه صنعتی خواجه نصیرالدین طوسی
h_khaloozadeh@kntu.ac.ir

محمدرضا عارف
آزمایشگاه تئوری اطلاعات و مخابرات امن
دانشکده مهندسی برق، دانشگاه صنعتی شریف
aref@sharif.edu

چکیده: جعبه‌های جایگزینی عموما به عنوان تنها عضو غیرخطی سیستمهای رمزنگاری بلوکی از اهمیت ویژه‌ای برخوردار هستند تا جائی که امنیت اینگونه‌سیستمها به مقاوم بودن این بخش تا حد زیادی وابسته است. با توجه به خواص مناسب سیستمهای آشوبی برای طراحی جعبه‌های جایگزینی تحقیقات زیادی در این زمینه در حال انجام است. در این مقاله به ارائه روشی برای طراحی جعبه جایگزینی مناسب برای سیستم رمزنگاری *AES* پرداخته می‌شود. معیارهای مناسب بودن یک جعبه جایگزینی تعریف و عملکرد جعبه جایگزینی طراحی شده با استفاده از این معیارها بررسی می‌شود. نشان داده می‌شود که جعبه جایگزینی طراحی شده بر مبنای نگاشت آشوبی برای کاربرد در سیستم *AES* مناسب بوده و عملکرد بهتری نسبت به جعبه جایگزینی سیستم *AES* از خود نشان می‌دهد. نشان داده می‌شود که جعبه جایگزینی پیشنهادی نسبت به حمله‌های خطی و تفاضلی مقاوم می‌باشد.

واژه های کلیدی: رمز بلوکی، جعبه جایگزینی، نگاشت آشوبی، سیستم آشوبی لورنتس

۱- مقدمه

در دهه‌های اخیر، رمزهای بلوکی نقشی اساسی را در تامین امنیت در رمزنگاری مدرن بازی کرده‌اند. جعبه‌های جایگزینی عموما تنها بخش غیرخطی این سیستمها می‌باشند که وظیفه ایجاد خاصیت گیجی[1] مطرح شده توسط شانون در [1] را در این سیستمها به عهده دارند. این جعبه‌های جایگزینی در حقیقت به عنوان هسته اصلی، به گستردگی در سیستمهای رمزنگاری بلوکی مانند *DES*[2] و *AES*[3] و غیره به کار رفته‌اند.

طراحی یک سیستم رمزنگاری بلوکی مقاوم مستلزم طراحی یک جعبه جایگزینی مقاوم می‌باشد و وجود ضعف در جعبه جایگزینی باعث ضعف سیستم رمزنگاری بلوکی مربوطه در مقابل حملات گوناگون خواهد شد. از اینرو طراحی یک جعبه

[1] Confusion

[2] Data Encryption Standard
[3] Advanced Encryption Standard

جایگزینی مقاوم از موضوعات مورد توجه محققین رمزنگاری می‌باشد.

یک جعبه جایگزینی $n \times m$ در حقیقت یک نگاشت غیر خطی از V_n به V_m است که در آن V_n و V_m به ترتیب فضای برداری از n و m عضو میدان $GF(2)$ می‌باشند.

تحقیقات زیادی در زمینه نحوه تولید جعبه جانشینی مناسب برای بکارگیری در رمزهای بلوکی در دهه‌های اخیر انجام گرفته است. جعبه‌های جایگزینی در حالت کلی به دو دسته ایستا[1] و پویا[2] دسته بندی می‌شوند. جعبه جایگزینی ایستا جعبه‌ای است که توسط طراح تولید شده و عناصر آن قبل از شروع عملیات رمزنگاری معین بوده و در طی مراحل رمزنگاری ثابت باقی می‌مانند و در حقیقت تحت تاثیر کلید رمزنگاری قرار نمی‌گیرند. در [2-8] روشهائی برای تولید این گونه جعبه جایگزینی ارائه شده‌اند که از آن جمله می‌توان به جستجوی کامل[3] [5]، استفاده از توابع تقریبا خمیده[4] [4] به منظور مقاومت در برابر حمله تفاضلی[5] نام برد. در سالهای اخیر استفاده از توابع آشوبی به منظور تولید جعبه‌های جایگزینی مورد توجه محققین در زمینه توابع آشوبی و رمزنگاری قرار گرفته است. خواص حساسیت شدید به شرایط اولیه و پارامترها، و نیز خاصیت مخلوط کنندگی[6]، این توابع را به عنوان نامزدی مناسب برای تولید جعبه‌های جایگزینی مطرح ساخته‌اند.

در این مقاله به ارائه روشی برای تولید یک جعبه جایگزینی ایستا برای بکارگیری در سیستم رمزنگاری *AES* می‌پردازیم.

ساختار مقاله به شرح زیر است. در بخش دوم به معرفی سیستم آشوبی به کار رفته در طرح ارائه شده پرداخته می‌شود. در بخش سوم، معیارهائی برای تشخیص مناسب بودن یک جعبه جایگزینی برای کاربرد در سیستمهای رمزنگاری بلوکی معرفی خواهند شد. بخش چهارم به معرفی نحوه تولید جعبه جایگزینی و ملاحظات مربوطه اختصاص دارد. در بخش پنجم به بررسی عملکرد جعبه جایگزینی تولید شده با استفاده از معیارهای معرفی شده در بخش سوم پرداخته می‌شود. بخش ششم به نتایج شبیه سازی سیستم رمزنگاری *AES* با استفاده از جعبه جایگزینی لورنتس تخصیص یافته است. در بخش هفتم به بیان نتایج پرداخته می‌شود. در بخش هشتم به تشکر و قدردانی از حامیان این پژوهش پرداخته شده و بخش پایانی به ارائه مراجع اختصاص یافته است.

۲- معرفی سیستم آشوبی لورنتس

سیستم لورنتس یکی از نگاشت‌های متداول آشوبی است که برای مدل کردن حرکت دینامیکی یک سیال جوی در ۱۹۶۳ توسط لورنتس معرفی شد [9]. این معادلات دینامیکی توسط رابطه (۱) مشخص شده‌اند:

$$\begin{aligned} \dot{x}_1 &= \delta (x_2 - x_1) \\ \dot{x}_2 &= r x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 &= x_1 x_2 - b x_3 \end{aligned} \qquad (۱)$$

در این روابط δ، r و b پارامترهای مثبت حقیقی سیستم هستند. بازه تغییر این پارامترها محدود به مجموعه اعدادحقیقی است. این معادلات به تغییر پارامترها و شرایط اولیه بسیار حساس هستند. در کاربردهای آشوبی محدوده تغییر این مولفه‌ها باید به‌گونه‌ای باشد که تغییرات معادلات کاملاً آشوبی باشد. در این راستا پژوهش‌های گسترده‌ای در [10,11] انجام شده است که در آنها پارامترهای b و δ ثابت، و پارامتر r متغیر است. مقادیر نامی b و δ به ترتیب $\frac{8}{3}$ و 10 بوده حال آنکه $0 < r < \infty$ است. این مقادیر (b و δ) نوعی بوده و در بازه‌های دیگری نیز معادلات آشوبی هستند.

۳- معیارهای تشخیص یک جعبه جایگزینی خوب

از آنرو که جعبه جایگزینی مورد نظر در این مقاله با هدف بکارگیری در سیستم رمزنگاری *AES* طراحی می‌شود، در این بخش به بیان معیارهای معمول برای تشخیص یک جعبه جایگزینی خوب $n \times n$ می‌پردازیم. خوب بودن یک جعبه جایگزینی بصورت قابلیت استفاده در سیستمهای رمزنگاری بلوکی مقاوم در برابر حملات تعریف می‌شود.

[1] Static
[2] Dynamic
[3] Exhaustive Search
[4] Near Bent Functions
[5] Differential Cryptanalysis
[6] Mixing

آدامز، تاوارس و داوسون در [6,12] با استفاده از خواص مهمی که برای طراحی جعبه‌های جایگزینی خوب از نظر قابلیت کاربرد در سیستمهای رمزنگاری بلوکی ضروری می‌باشند، روشهایی را برای طراحی جعبه‌های جایگزینی $n \times n$ ارائه نمودند. مقاومت جعبه جایگزینی در مقابل حمله تفاضلی و حمله خطی[1] از معیارهای بسیار مهم در تشخیص یک جعبه جایگزینی خوب می‌باشند. در زیر به بیان تعدادی از این معیارها می‌پردازیم:

- خاصیت تعادل[2]
- درجه غیرخطی بودن[3]
- درجه مصونیت از همبستگی[4]
- خاصیت دوسویی[5]
- خاصیت بهمنی اکید[6]
- مرتبه جبری توابع بولی
- حداقل و حداکثر تعداد تک‌جمله‌ای[7]های توابع بولی
- بهترین تقریب آفینی[8] توابع بولی
- مقاومت در برابر حمله خطی
- مقاومت در برابر حمله تفاضلی

٤- روش تولید جعبه جایگزینی آشوبی

در این بخش به شرح روش استفاده شده به منظور تولید جعبه جایگزینی با استفاده از سیستم آشوبی پیوسته لورنتس می‌پردازیم. همانگونه که می‌دانیم جعبه جایگزینی سیستم *AES*، یک کلمه ۸ بیتی را به عنوان ورودی گرفته و کلمه ۸ بیتی دیگری را جایگزین آن می‌نماید. کلمات این جعبه جایگزینی به تعداد ۲۵۶ کلمه و از ۰ تا ۲۵۵ می‌باشند. در این پژوهش حالت اول سیستم آشوبی لورنتس به عنوان خروجی انتخاب شده است. شرایط اولیه و پارامترهای سیستم به گونه‌ای انتخاب می‌شوند که سیستم آشوبی باقی بماند. خروجی سیستم آشوبی را به ۲۵۶ سطح بصورت یکنواخت چندسطحی می‌کنیم. این سطوح را از صفر تا ۲۵۵ به ترتیب افزایش شماره‌گذاری می‌کنیم. در هر زمان نمونه برداری، خروجی سیستم چندسطحی شده برابر سطح متناظر مقدار دامنه خروجی سیستم آشوبی لورنتس در آن زمان در نظر گرفته می‌شود. با شبیه سازی سیستم به مدت کافی، دنباله خروجی سیستم تشکیل می‌شود. در این حالت جعبه جایگزینی به صورت یک آرایه تک بعدی ۲۵۶ عضوی در نظر گرفته می‌شود. از ابتدای این دنباله اعضای دنباله به ترتیب انتخاب می‌شوند. عضو اول در خانه اول آرایه جعبه جایگزینی قرار خواهد گرفت. اعضای بعدی به شرطی در خانه‌های بعدی به ترتیب قرار داده می‌شوند که تا کنون در هیچ‌یک از خانه‌های قبلی قرار نگرفته باشند. بدین ترتیب آرایه جعبه جایگزینی تشکیل می‌گردد. این جعبه جایگزینی نیز یک کلمه ۸ بیتی مانند i را به عنوان ورودی می‌گیرد. در این حالت مقدار متناظر خانه شماره $i+1$ جعبه جایگزینی را به عنوان خروجی اعلام می‌نماید. با توجه به اینکه در این روش از چندسطحی کردن خروجی یک سیستم آشوبی پیوسته به منظور تولید عناصر جعبه جایگزینی استفاده شده‌است، توجه به نکات عملی زیر به منظور دستیابی به یک جعبه جایگزینی خوب ضروری به نظر می‌رسد.

- زمان نمونه‌برداری در این روش می‌بایست مناسب انتخاب شود. انتخاب مقادیر کوچک برای این زمان به ایجاد الگوهای خطی در جعبه جایگزینی خواهد انجامید که به هیچ وجه مناسب نمی‌باشد. انتخاب زمان نمونه‌برداری بزرگ نیز باعث می‌شود که سیستم تغییرات خروجی را نبیند که این نیز خود اثر مشابهی خواهد داشت.
- شرط اصلی در انتخاب پارامترها و شرایط اولیه سیستم آشوبی در این روش، تنها آشوبی باقی ماندن خروجی سیستم آشوبی می‌باشد.
- از میان سیستمهای آشوبی موجود تنها سیستم‌هائی که دارای تغییرات آشوبی در دامنه حالت سیستم آشوبی هستند برای این کاربرد مناسب هستند.
- با توجه به اینکه چندسطحی کردن با توجه به بیشینه و کمینه مقادیری که خروجی سیستم آشوبی در بازه شبیه سازی شده اختیار نموده است انجام می‌شود، احتمال دارد با توجه به عدم

[1] Linear Cryptanalysis
[2] Balance
[3] Nonlinearity Degree
[4] Correlation Immunity Degree
[5] Bijection
[6] Strict Avalanche Criterion (SAC)
[7] Monomials
[8] Best Affine Approximation

تکرار این مقادیر در بازه شبیه‌سازی شده با توجه به زمان نمونه‌برداری انتخاب شده، تعدادی از عناصر $GF(2^8)$ تولید نگردند که این خود باعث عدم تشکیل جعبه جایگزینی مناسب خواهد شد. به منظور حل این مشکل مقدار $0.6(max(|y_{max}|,|y_{min}|))$ با توجه به شبیه سازی‌های انجام شده به عنوان بیشینه برای عمل چند سطحی کردن انتخاب می‌گردد و خروجی سیستم آشوبی در بازه $\pm 0.6(max(|y_{max}|,|y_{min}|))$ چند سطحی می‌شود.

پس از تشکیل جعبه جایگزینی و جعبه جایگزینی معکوس[1] با روش اشاره شده می‌توان این دو را در الگوریتم رمزنگاری و رمزگشائی AES به کار گرفت. نکته قابل توجه این است که جعبه‌های جایگزینی تولید شده در این روش می‌بایست خاصیتهای بیان شده در بخش سوم را برآورده نمایند. در بخش بعد به بررسی این خواص در یک جعبه جایگزینی که در تکرار سوم این روش به منظور دستیابی به یک جعبه جایگزینی مناسب بدست آمد، پرداخته می‌شود.

۵- بررسی عملکرد جعبه جایگزینی تولید شده با استفاده از روش فوق

جدول ۱ جعبه جایگزینی بدست آمده از روش مطرح شده در بخش قبل و جعبه جایگزینی معکوس آن را نشان می‌دهد. در ادامه از این جعبه جایگزینی به نام جعبه جایگزینی لورنتس یاد خواهد شد. این جدول همانند جدول جایگزینی *AES* دارای ۲۵۶ خانه می‌باشد که در آن اعداد ۰ تا ۲۵۵ در مبنای شانزده قرار گرفته‌اند. فرض کنید می‌خواهیم معکوس عدد ۲۱ را از جعبه جایگزینی معکوس لورنتس بیابیم. بدین منظور به موقعیت سطر ۳ و ستون ۲ در جدول جانشینی معکوس لورنتس مراجعه می‌نماییم. مقدار معکوس ۲۱ تحت این نگاشت برابر *fd* است. در حقیقت برای یافتن معکوس عدد *mn* به موقعیت سطر *m+1* و ستون *n+1* مراجعه می‌نمائیم.

جدول ۱: جعبه جایگزینی بدست آمده از سیستم لورنتس

52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	Fb
7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	Cb
54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f
60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	Ef
a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

جدول ۲ :جعبه جایگزینی معکوس بدست آمده از سیستم لورنتس

63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	Cf
d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	Db
e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	Df
8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

به منظور بررسی عملکرد جعبه جایگزینی لورنتس، آن را با جعبه جایگزینی سیستم *AES* با معیارهای مطرح شده در بخش ۳ مقایسه می‌کنیم.

- **خاصیت تعادل**

هر دو جعبه جایگزینی دارای خاصیت تعادل می‌باشند.

[1] Inverse Substitution Box

- **درجه غیر خطی بودن**

درجه غیر خطی بودن یک جعبه جایگزینی حداقل مرتبه غیرخطی توابع بولی سازنده آن جعبه می‌باشد. برای جعبه جایگزینی *AES* این مقدار برابر ۸۲ و برای جعبه جایگزینی لورنتس برابر ۱۱۲ می‌باشد. با توجه به این معیار عملکرد جعبه جایگزینی لورنتس نسبت به *AES* به مقدار قابل توجهی بهتر می‌باشد.

- **درجه مصونیت از همبستگی**

گوئیم تابع بولی n متغیره f دارای مصونیت از همبستگی مرتبه m ام که $m \le n-1$ ، $CI(m)$ است اگر ابهام خروجی تابع با مشخص نمودن (و ثابت نگهداشتن) هر ترکیب $m-$ بیتی ورودی (یا کمتر) و تغییر بقیه بیتها بصورت تصادفی، نسبت به حالت تغییر تمام بیتها بصورت تصادفی تفاوتی نکند. برای تمامی توابع بولی این دو جعبه جایگزینی درجه مصونیت از همبستگی برابر صفر می‌باشد.

- **خاصیت دوسویی**

هر دو جعبه‌های جایگزینی دارای خاصیت دوسوئی می‌باشند.

- **خاصیت بهمنی اکید**

به منظور تشخیص اینکه یک جعبه جایگزینی خاصیت بهمنی اکید را برآورده می‌نماید روشی در [2] معرفی شده است. با استفاده از این روش مشاهده می‌شود که هر دو این جعبه‌های جایگزینی تقریبا خاصیت بهمنی اکید را برآورده می‌نمایند. جدول ۴ نشان دهنده ماتریس وابستگی جعبه جایگزینی *AES* و جدول ۵ نشان دهنده ماتریس وابستگی جعبه جایگزینی لورنتس می‌باشد.

- **مرتبه جبری توابع بولی**

مرتبه جبری توابع بولی هردو جعبه جایگزینی برابر ۷ می‌باشد.

- **حداقل و حداکثر تعداد تک‌جمله‌ای‌های توابع بولی**

برای جعبه جایگزینی *AES* این مقادیر برابر ۱۰۴ و ۱۲۶ و برای جعبه جایگزینی لورنتس برابر ۱۱۰ و ۱۳۲ می‌باشند.

- **بهترین تقریب آفینی توابع بولی**

جدول ۳ نشان‌دهنده بهترین تقریب آفینی توابع بولی جعبه جایگزینی *AES* و لورنتس می‌باشد.

جدول ۳ : بهترین تقریب آفینی توابع بولی

S-box	تابع بولی اول	تابع بولی دوم	تابع بولی سوم	تابع بولی چهارم
لورنتس	1+ X1+ X3+ X4+ X6	1+ X1+ X3+ X4+ X7	X2+ X4+ X6+ X7	X1+ X3+ X5+ X6
AES	1+ X1+ X3+ X5	X2+ X5+ X7+ X8	1+ X1+ X3+ X4+ X5	X2+ X3+ X5+ X6+ X7
S-box	تابع بولی پنجم	تابع بولی ششم	تابع بولی هفتم	تابع بولی هشتم
لورنتس	X2+ X6	1+ X3	1+ X2	X1+ X4+ X5+ X6
AES	1+ X3	1+ X8	1+ X8	X7+ X8

همانگونه که مشاهده می‌شود تعداد جمله‌های این تقریبها برای جعبه جایگزینی لورنتس به طور متوسط بیشتر از جعبه جایگزینی *AES* است.

جدول ۴: ماتریس وابستگی جعبه جایگزینی *AES*

0.578	0.531	0.500	0.453	0.453	0.453	0.500	0.406
0.469	0.578	0.438	0.516	0.422	0.406	0.500	0.375
0.594	0.453	0.500	0.484	0.469	0.453	0.469	0.375
0.453	0.484	0.469	0.500	0.438	0.422	0.422	0.375
0.578	0.453	0.547	0.547	0.516	0.469	0.453	0.391
0.469	0.578	0.516	0.516	0.469	0.500	0.469	0.500
0.469	0.516	0.438	0.500	0.516	0.406	0.438	0.547
0.531	0.469	0.469	0.438	0.391	0.531	0.578	0.641

جدول ۵ : ماتریس وابستگی جعبه جایگزینی لورنتس

0.516	0.516	0.453	0.563	0.453	0.484	0.453	0.500
0.469	0.484	0.563	0.500	0.484	0.453	0.500	0.531
0.516	0.516	0.500	0.469	0.563	0.500	0.531	0.500
0.531	0.531	0.469	0.453	0.500	0.531	0.500	0.547
0.453	0.500	0.453	0.516	0.500	0.500	0.547	0.531
0.453	0.516	0.516	0.469	0.469	0.547	0.531	0.531
0.531	0.531	0.469	0.516	0.469	0.531	0.531	0.484
0.516	0.563	0.516	0.531	0.484	0.531	0.484	0.516

- **مقاومت در برابر حمله خطی:**

حمله خطی اولین بار توسط ماتسوی در [13] معرفی گردید. این حمله به عنوان یک حمله بسیار قوی به سیستم‌های رمزنگاری بلوکی با کلید متقارن مطرح است. معیار مقاومت توابع بولی

تشکیل‌دهنده جعبه جایگزین در برابر حمله خطی، بایاس خطی احتمال[1] ρ_L، نامیده می‌شود. هر قدر که مقدار $\left|\rho_L - \frac{1}{2}\right|$ بزرگتر باشد، سیستم در برابر حمله خطی ضعیف‌تر بوده و حمله با تعداد کمتری متن اصلی[2] معلوم انجام می‌پذیرد. مقدار بایاس محاسبه شده برای توابع بولی جعبه جایگزینی AES به ترتیب برابر ۰،۰۹۳۸، ۰،۱۰۱۶، ۰،۰۹۳۸، ۰،۰۹۳۸، ۰،۰۸۵۹، ۰،۱۳۲۸ است درحالیکه برای توابع بولی جعبه جایگزینی لورنتس برابر ۰،۰۶۲۵ می‌باشد. همانگونه که مشاهده می‌شود، جعبه جایگزینی لورنتس عملکردی قابل قبول و تا حدی بهتر از جعبه جایگزینی *AES*، در برابر حمله خطی از خود نشان می‌دهد.

- **مقاومت در برابر حمله تفاضلی و درجه مصونیت از حمله تفاضلی**

حمله تفاضلی، که اولین بار توسط بیهام و شامیر در [14,15,16] مطرح شد، قوی‌ترین حمله به رمزهای بلوکی و به خصوص رمزهای شبیه *DES*، که بر اساس جابجائی و جایگزینی عمل می‌کنند، می‌باشد. این روش بر پایه جدول توزیع تفاضلات[3] عمل می‌نماید. در مورد جعبه جایگزینی لورنتس،جدول توزیع تفاضلات یک جدول $2^8 \times 2^8$ می‌باشد. سطرهای این ماتریس نشان دهنده تغییرات در ورودی، و ستونهای آن نشانگر تغییرات در خروجی می‌باشند. عناصر این جدول برای یک جعبه جایگزینی مقاوم در برابر حمله تفاضلی، نمی‌بایست مقادیر بزرگ را اختیار نمایند. این یک شرط لازم و نه کافی می‌باشد. در زیر به معرفی معیار ارائه شده در [17] برای مقاومت جعبه جایگزینی در برابر حمله تفاضلی می‌پردازیم. فرض می‌کنیم که $F=(f_1,f_2,...,f_s)$ یک جعبه جایگزینی $n\times s$ باشد که در آن f_i تابعی بر روی فضای بردارهای n تائی بر روی $GF(2)$ می‌باشند و $n \geq s$ است. L نشانگر بزرگترین مقدار در جدول توزیع تفاضلات جعبه جایگزینی F و R نشانگر تعداد عناصر غیر صفر در ستون اول جدول توزیع تفاضلات این جعبه جایگزینی است. در هر دو حالت مقدار 2^n در سطر اول به حساب نمی‌آید. در این حالت می‌گوئیم که F ، ε مقاوم در برابر حمله تفاضلی است که ε بصورت $\varepsilon = (1-\frac{R}{2^n})(1-\frac{L}{2^n})$ تعریف می‌شود. مقاومت زیاد تنها در حالتی که هر دوی R و L کوچک باشند حاصل خواهد شد. مقدار مقاومت برای جعبه جایگزینی *AES* برابر ۰/۹۳۷۵ و برای جعبه جایگزینی لورنتس برابر۰/۹۸۴۴ محاسبه شد.

پیچیدگی حمله تفاضلی به اندازه بزرگترین عنصر جدول توزیع تفاضلات ، تعداد صفرها در جدول توزیع تفاضلات و تعداد عناصر غیر صفر در ستون اول این جدول وابسته است [18]. در زیر جدول تکرار مشخصات تفاضلی برای دو جعبه جایگزینی *AES* و لورنتس نشان داده شده‌اند.

جدول ۶ : جدول تکرار مشخصات تفاضلی سیستم *AES*

تفاضل	تکرار
0	40165
2	19340
4	4991
6	878
8	131
10	24
12	3
14	2
16	1
256	1

جدول ۷ : جدول تکرار مشخصات تفاضلی سیستم لورنتس.

تفاضل	تکرار
0	33150
2	32130
4	255
256	1

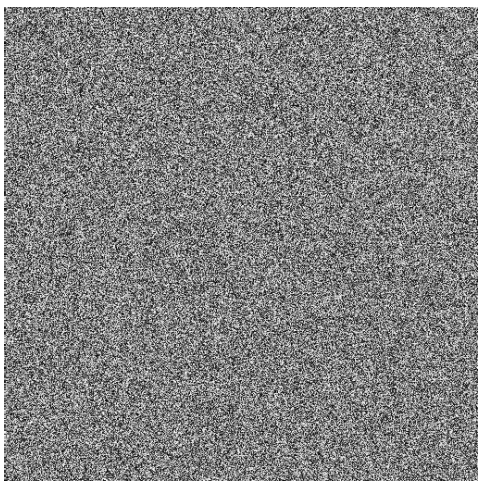
همانگونه که مشاهده می‌شود، جعبه جایگزینی لورنتس عملکردی قابل قبول و تا حدی بهتر از جعبه جایگزینی *AES*، در برابر حمله تفاضلی از خود نشان می‌دهد.

[1] Linear Probability Bias
[2] Plain Text
[3] Difference Distribution Table

٦- نتایج شبیه سازی سیستم رمزنگاری *AES* با جعبه جایگزینی لورنتس

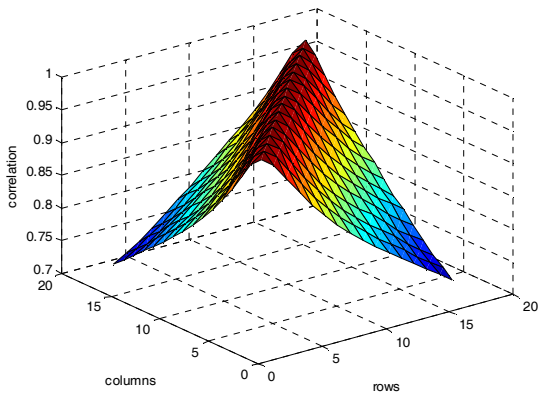
در این بخش به رمزنگاری و رمزگشائی تصویر عکاس[1] که در کاربردهای پردازش تصویر به فراوانی مورد استفاده قرار می‌گیرد، می‌پردازیم. این تصویر در شکل ۱ نشان داده شده است. شکل ۲ نشانگر تصویر رمز شده عکاس با سیستم *AES* و جعبه جایگزینی لورنتس می‌باشد.

شکل ۱. تصویر عکاس به عنوان متن اصلی.

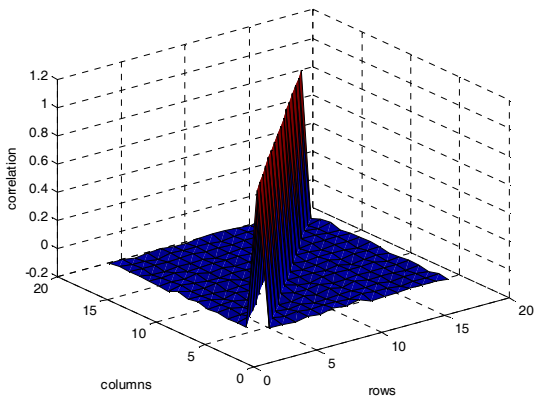


شکل ۲. تصویر رمز شده عکاس توسط سیستم *AES* با جعبه جایگزینی لورنتس.

نتایج حاصل از انجام تست همبستگی بر روی متن اصلی و رمز شده به ترتیب در شکل‌های ۳ و ۴ مشاهده می‌شوند. انتظار می‌رود که برای متن اصلی، تابع همبستگی مقادیر ماکزیمم خود را به ازای عناصر روی قطر اصلی اختیار نماید. همانگونه که مشاهده می‌شود عناصر غیر قطر اصلی هم دارای همبستگی زیادی می‌باشند. انتظار می‌رود که مقدار همبستگی بین عناصر غیر قطر اصلی در متن رمز شده[2] ناچیز باشد. این خود بدین معنی است که پیکسلهای مجاور اطلاعات زیادی از هم در اختیار قرار ندهند. این امر به وضوح در نمودارهای زیر مشاهده می‌گردد. همچنین همبستگی به ازای عناصر روی قطر اصلی ماکزیمم خواهد بود. همانگونه که مشاهده می‌شود با این معیار الگوریتم رمزنگاری عملکرد مناسبی دارد.



شکل ۳. همبستگی متن اصلی.



شکل ۴. همبستگی متن رمزشده.

۷- نتیجه‌گیری

در این مقاله به بیان خواص یک جعبه جایگزینی خوب و نیز معیارهائی برای تشخیص آن پرداخته شد. به منظور استفاده در سیستم رمزنگاری *AES*، یک جعبه جایگزینی 8×8 با استفاده از سیستم آشوبی لورنتس طراحی گردید. با استفاده از خواص و معیارهای معرفی شده نشان داده شد که جعبه جایگزینی طراحی

[1] Cameraman

[2] Cipher Text

شده برای هدف ذکر شده مناسب می‌باشد. همچنین مقاومت این جعبه جایگزینی نسبت به حمله‌های خطی و تفاضلی بررسی شد و نشان داده شد که این جعبه جایگزینی نسبت به جعبه جایگزینی *AES* در برابر حمله‌های خطی و تفاضلی مقاوم تر است. در انتها عملکرد سیستم رمزنگاری *AES* با استفاده از جعبه جایگزینی لورنتس با معیار همبستگی بررسی شد و عملکرد مناسب آن نشان داده شد.

۸- سپاسگزاری

این پژوهش طبق قرارداد شماره ۵۰۰۷۰۹۹/ت تحت حمایت مرکز تحقیقات مخابرات ایران انجام شده است. همچنین از صندوق حمایت از پژوهشگران بخاطر حمایت و تصویب کرسی پژوهشی رمز تشکر و قدردانی می‌شود.

۹- مراجع

[1] CE. Shannon, *Communication theory of secrecy systems*. Bell Syst Tech J1949;28:656–715.

[2] AF.Webster and SE.Tavares,"On the Design of S-boxes,".*In:Advancesin cryptology: Proc of CRYPTO_85*. New York: Springer-Verlag;1986.p.52-–34.

[3] M. Dawson and SE.Tavares. ," An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks,". *In: Advances in cryptology: Proc of Eurocrypt_91*. New York: Springer-Verlag; 1991. p. 352-67.

[4] J.Detombe and S.Tavares.,"Constructing large cryptographically strong S-boxes,".*In:Advances in cryptology: Proc. of CRYPTO92. In:Lecture notes in computer science;* 1992.

[5] R. Forre.,"The strict avalanche criterion, spectral properties of Boolean functions and an extended definition,". *In: Advances in cryptology:Proc of CRYPTO_88*. Berlin: Springer-Verlag; 1989.

[6] C. Adamas and S. Tavares ,"Good S-boxes are easy to find,". *In: Advances in cryptology: Proc. of CRYPTO_89. In: Lecture notes in computer science*. 1989. p. 612–5.

[7] C. Adams and S.Tavares ,"The structured design of cryptographically good S-boxes," *JCryptol vol.990;* 3(1):27–41.

[8] X. Yi,S. Cheng and X. You ,"A method for obtaining cryptographically strong 8·8 S-boxes,".*Global telecommunication conference, GLOBECOM_97* November 1997, vol. 2. New York: IEEE; 1997. p. 689-93.

[9] J. L. Lorenz and Y. Pomeau, "A simple case on nonperiodic (strange) attractor," *J. Non. Equib. Thermodyn.*, vol. 3, pp. 135-152, 1978.

[10] M. Henon and Y. Pomeau, "Two strange attractors with a simple structure," *In Turbulence and Navier-Stokes Equations*. Lecture Notes in Math., vol.565,pp. 29-68, Springer Verlag.

[11] J. K. Kaplan and J. A. Yorke, "Preturbulance: A regime observed in a fluid flow model of Lorenz,"*Commun. Math. Phys.*, vol67, pp.93-108,1979.

[12] MH. Dawson and SE. Tavares ."An expanded set of design criteria for substitution boxes and their use in strengthening DES-like cryptosystems."*In: IEEE Pacific rim conference on communications, computers and signal processing*, 9-13 May 1991. p. 191-5.

[13] M. Matsui"*Linear cryptanalysis method for DES cipher*". *Advances in Cryptology - EUROCRYPT* 1993.

[14] E.Biham and A. Shamir,"*Differential Cryptanalysis of the Data Encryption Standard,*" Springer Verlag, 1993.

[15] E.Biham and A. Shamir,"Differential Cryptanalysis of DES-like Cryptosystems". *Advances in Cryptology — CRYPTO '90*. Springer-Verlag. 2–21.

[16] E.Biham and A. Shamir, "differential Cryptanalysis of the Full 16-Round DES," *CS 708, Proceedings of CRYPTO '92, Vol. 740 of Lecture Notes in Computer Science*, december 1991.

[17] J.Seberry, X. Zhang and Y. Zheng"Systematic generation of cryptographically robust S-boxes,". *In Proceedings of the 1st ACM Conference on Computer and Communications Security* (Fairfax, Virginia, United States, November 03 - 05, 1993). CCS '93. ACM Press, New York, NY, 171-182.

[18] A. M. Youssef and S. E. Tavares."Resistance of balanced s-boxes to linear and differential cryptanalysis. ,"*Inf. Process. Lett.* 56, 5 (dec. 1995), 249-252.