مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۳، پاییز ۱۳۹۶، ص ۷۷-۶۹

طراحی الگوریتم سریع جهت رمزکردن تصاویر با استفاده از قضیه باقی‌مانده چینی و خم بیضوی

غلامرضا کرمعلی[1*]، عیسی کاوند[2]

۱- استادیار، ۲- دانشجوی کارشناس ارشد، دانشگاه علوم و فنون هوایی شهید ستاری

(دریافت: ۹۵/۰۸/۲۵، پذیرش: ۹۵/۱۱/۲۵)

چکیده

ارسال و دریافت اطلاعات، به‌صورت محرمانه همواره از اهمیت بالایی برخوردار است. علم رمزنگاری نقش عمده‌ای در تبادل اطلاعات به‌صورت امن ایفا می‌کند. به همین منظور، الگوریتم‌های رمزنگاری متعددی طراحی و پیاده‌سازی شده است. از میان الگوریتم‌های طراحی شده، الگوریتم رمزنگاری خم بیضوی، به‌دلیل ویژگی‌های منحصر به‌فردش، جایگزین مناسبی برای الگوریتم‌های قدیمی‌تر از قبیل RSA و دیفی هلمن می‌باشد. در این مقاله، روش کارآمدی برای رمزنگاری تصویر با استفاده از خم‌های بیضوی ارایه خواهد شد. این طرح پیشنهادی در مقایسه با روش‌های فعلی دارای سرعت بالاتری در رمزنگاری و رمزگشایی تصویر است. برای این منظور، از روش گروه‌بندی پیکسل‌های تصویر با استفاده از قضیه باقی‌مانده چینی، استفاده شد. روش پیشنهادی قابل اعمال بر روی سایر داده‌ها از قبیل متن، صدا و ویدیو می‌باشد.

واژه‌های کلیدی: پردازش تصویر، رمزنگاری تصویر، رمزگشایی تصویر، رمزنگاری خم بیضوی، قضیه باقی‌مانده چینی.

۱- مقدمه

الگوریتم‌های رمزنگاری به دو دسته کلید متقارن و کلید نامتقارن تقسیم‌بندی می‌شوند. در سامانه مزنگاری کلید متقارن، فرستنده و گیرنده از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کنند. این سامانه رمزنگاری دارای بار محاسباتی کم‌تری نسبت به رمزنگاری کلید نامتقارن است [۱]. در سامانه رمزنگاری کلید نامتقارن عملیات رمزنگاری و رمزگشایی با دو کلید متفاوت صورت می‌پذیرد. به سامانه رمزنگاری کلید نامتقارن، سامانه رمزنگاری کلید عمومی نیز گفته می شود. سامانه رمزنگاری برپایه خم بیضوی[1]، یک سامانه رمزنگاری کلید عمومی است. این سامانه رمزنگاری توسط کوبلیتز[2] [۲] و میلر[3] [۳] معرفی گردید. خم‌های بیضوی در مقایسه با پروتکل[4] RSA[5] از کلیدی کوتاه‌تر با همان میزان امنیت استفاده می‌کند [۴]. استفاده از طول کلید کوتاه‌تر، نیازمند پردازش ساده‌تر و مصرف توان پایین‌تر است که این الگوریتم را برای پیاده‌سازی در وسایلی نظیر تلفن همراه، کارت‌های هوشمند ایده‌آل کرده است. با توجه به مزایای بیان‌شده، از این سامانه برای رمزنگاری تصاویر استفاده شد. در این مقاله، از روش رمزنگاری الجمال [۵] برای رمزنگاری تصویر و از قضیه باقی‌مانده چینی[6] جهت گروه‌بندی پیکسل‌ها استفاده شده است. رمزنگاری تصویر در دو حوزه فرکانس و مکان انجام می‌گیرد. رمزنگاری در حوزه فرکانس به این صورت انجام می‌گیرد که ابتدا با استفاده از تبدیل DCT، تصویر را به حوزه فرکانس منتقل کرده و سپس ضرایب DCT را رمز می‌کنند. اما رمزنگاری در حوزه مکان، مستقیم بر روی مقادیر پیکسل‌ها انجام می‌گیرد و با اجرای الگوریتم رمزنگاری سطوح خاکستری تصویر تغییر خواهند کرد. الگوریتم رمزنگاری پیشنهادی در این مقاله در حوزه مکان بر روی تصاویر اعمال می‌شود.

۱-۱- محاسبات خم‌های بیضوی

محاسبات برروی خم‌های بیضوی دارای قوانینی است که در زیر به آن‌ها پرداخته می‌شود. فرض می‌کنیم که خم بیضوی ما به صورت زیر روی میدان محدود F_p تعریف شده باشد.

$$E: y^2 = x^3 + ax + b \qquad (۱)$$

۱-۱-۱- قانون جمع نقاط

اگر دو نقطه مجزا P, Q متعلق به خم بیضوی E که رو میدان

* رایانامه نویسنده مسئول: g_karamali@iust.ac.ir

1- Elliptic Curve
2- Koblitz
3- Miller
4- protocol
5- Rivest-Shamir-Adleman
6- Chinese Remainder Theorem

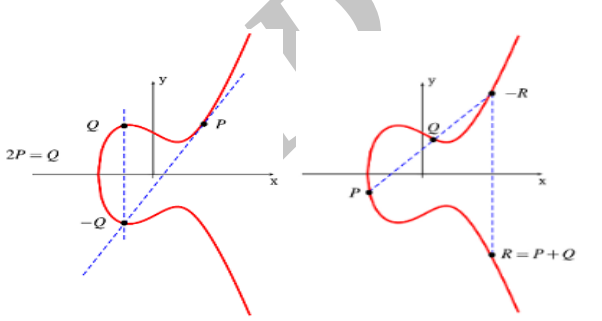
محدود p تعریف شده است، باشند. آن‌گاه این دو نقطه با استفاده از روابط زیر با هم جمع خواهند شد:

$$P(x_1,y_1)+Q(x_2,y_2)=R(x_3,y_3) \quad (۲)$$

$$x_3=(\lambda^2-x_1-x_2)\bmod p \quad (۳)$$

$$y_3=(\lambda(x_1-x_3)-y_1)\bmod p \quad (۴)$$

$$\lambda=\frac{y_2-y_1}{x_2-x_1} \quad (۵)$$



الف) جمع نقاط ب) مضاعف نقاط

شکل (۱): تعبیر هندسی جمع و مضاعف نقاط

۱-۱-۲- قانون مضاعف نقاط

اگر نقطه ای مانند $P\in E$ داشته باشیم آنگاه مضاعف نقطه به صورت زیر تعریف می شود.

$$P(x_1,y_1)+P(x_1,y_1)=R(x_3,y_3) \quad (۶)$$

$$x_3=(\lambda^2-2x_1)\bmod p \quad (۷)$$

$$y_3=(\lambda(x_1-x_3)-y_1)\bmod p \quad (۸)$$

$$\lambda=\frac{3x_1^2+a}{2y_1}\bmod p \quad (۹)$$

۱-۱-۳- قانون مضاعف نقاط

اگر نقطه‌ای مانند $P\in E$ داشته باشیم آن‌گاه مضاعف نقطه به صورت زیر تعریف می‌شود:

$$kP=P+P+\ldots+P \quad (k \quad times) \quad (۱۰)$$

تعبیر هندسی جمع و مضاعف‌سازی نقاط در شکل (۱) نشان داده شده است.

۱-۲- قضیه باقی‌مانده چینی [۶]

اگر اعداد صحیح مثبت $m_1,m_2,\ldots m_r$ دو به دو نسبت به هم اول باشند، یعنی $\gcd(m_i,m_j)=1$ و اعداد $b_1,b_2,\ldots,b_r$ اعداد صحیح اختیاری باشند، در این صورت، دستگاه هم‌نهشتی زیر دارای دقیقاً یک جواب در هنگ $M=m_1\times m_2\times\ldots\times m_r$ می‌باشد.

$$\begin{cases} x\equiv b_1 \pmod{m_1} \\ x\equiv b_2 \pmod{m_2} \\ \vdots \\ x\equiv b_r \pmod{m_r} \end{cases} \quad (۱۱)$$

برای حل این معادلات تعریف می‌کنیم:

$$M=m_1m_2\ldots m_r \quad (۱۲)$$

$$M_k=\frac{M}{m_k}\Rightarrow\gcd(M_k,m_k)=1 \quad (۱۳)$$

$$x=b_1M_1M_1'+b_2M_2M_2'+\ldots \\ \ldots+b_rM_rM_r'(\bmod M) \quad (۱۴)$$

که در این معادلات M_i' همان معکوس ضربی M_i در هنگ m_i است.

نکته: شرایط وجود جواب دستگاه هم‌نهشتی رابطه (۱۱) عبارتند از: ۱- مدول‌ها نسبت به هم اول باشند. ۲- هر یک از معادلات به تنهایی دارای جواب باشند.

۲- مروری بر کار های انجام شده

برای رمزنگاری اطلاعات با استفاده از خم‌های بیضوی کارهای زیادی انجام گرفته است که در ادامه به اختصار برخی از مهم‌ترین این کارها را بیان می‌کنیم. هنکرسون[1]، آلفرد منز[2] و وانستون[3] [۷] مطالعات خود را روی محاسبات، کاربردها و پروتکل‌های رمزنگاری خم‌های بیضوی گوناگون انجام دادند. لارنس سی واشنگتن[4] [۸] به اثبات برخی نظریه‌های مربوط به خم‌های بیضوی پرداخت. جوکو تریاهو[5] [۹] با استفاده از نرم‌افزار متمتیکا[6] جنبه‌های مختلف خم بیضوی را مورد بررسی قرار داد. احمد عبدالطیف[7] و زیامو[8] [۱۰] برای رمزنگاری تصویر از فن خم‌های بیضوی و سامانه آشوبی استفاده کردند. آن‌ها با استفاده

1- Hankerson
2- Alfred Menezes
3- Vanstone
4- Lawrence C. Washington
5- Jouko Teeriaho
6- Mathematica
7- Abd El-Latif
8- Xiamu Niu

از نقاط خم‌های بیضوی و سامانه آشوبی یک رشته کلید شبه تصادفی پیشنهاد دادند که از آن برای رمزنگاری تصویر استفاده می‌شد. هانگ لیو[1] و یانک بینگ[2] [۱۱] پیشنهادی برای رمزگشایی تصویر رمزشده با استفاده از سامانه ترکیبی آشوبی و خم‌های بیضوی ارائه کردند. آن‌ها دریافتند که با استفاده از متن آشکار و انتخاب یک تصویر که تمام پیکسل‌های آن صفر باشد، می‌توانند تصویر رمزشده را تولید کنند. ماریا[3] و مانیس وارن[4] [۱۲] الگوریتمی برای رمزنگاری تصویر با استفاده از خم‌های بیضوی ارائه کردند. آن‌ها از یک زوج مولد خطی همنهشت برای تولید کلید خصوصی و یک عدد تصادفی k استفاده کردند. برای به‌دست‌آوردن تصویر رمزشده برای هر پیکسل ضرب نقطه‌ای انجام می‌گرفت و با استفاده از مولد برروی خم بیضوی قرار می‌گرفت. در این روش یک جدول تطابق برای رمزگشایی مورد نیاز است. علی سلیمانی، جان نوردین و زولکاریان [۱۳] یک تکنیک رمزنگاری با استفاده از خم‌های بیضوی روی میدان محدود ارائه دادند. آن‌ها اعداد ۲۵۵-۰ را روی نقاط منحنی منطبق کردند و سپس با استفاده از کلید عمومی گیرنده عملیات رمزنگاری را انجام دادند. برای نمایش تصویر رمزشده دوباره از جدول تطابق استفاده می‌شد و نقاط به اعداد ۲۵۵-۰ تبدیل می‌شدند. بهیان، اخوان، اخشانی و شمس الدین [۱۴] از مختصات ژاکوبین خم بیضوی برای رمزنگاری استفاده کردند. آن‌ها با استفاده از کلید رمزنگاری و انجام اعمالی برروی ماتریس تصویر آن را به یک ماتریس یک بعدی تبدیل کردند. به این ترتیب، با استفاده از معادلات خم‌های بیضوی رمزنگاری انجام می‌شد. احمد عبدالطیف و زیامونو [۱۵] با استفاده از الگوریتم الجمال در رمزنگاری خم‌های بیضوی و برپایه تصاویر هم شکل، یک تصویر محرمانه را به اشتراک گذاشتند. آن‌ها پارامترهایی برای خم بیضوی درنظر گرفتند که در مقابل حمله پولارد[5] و هم‌چنین فولینگ هلمن[6] مقاوم بود. لویی، موافی و ولید الجوبی[7] [۱۶] از دو خم بیضوی و هم‌چنین ضرایب DCT تصویر، برای رمزنگاری استفاده کردند. دولندرو و منگ لم[8] [۱۷] با گروه‌بندی پیکسل‌ها و به‌دست‌آوردن یک عدد بزرگ، تعداد عملیات رمزنگاری را کاهش دادند. آن‌ها با استفاده از دستوری در نرم‌افزار متمتیکا[9] این گروه‌بندی را انجام دادند.

1- Hong Liu
2- Yanbing Liu
3- Maria Celestin
4- Muneeswaran
3- Pollard
4- Pohlig Hellman
7- Lo'ai Tawalbeh, Moad Mowafi and Walid Aljoby
8- Dolendro and Manglem
9- Mathematica

۳- طرح مسئله

همان‌طورکه می‌دانیم یکی از روش‌های رمزنگاری تصویر، انجام عملیات رمز برروی تک‌تک پیکسل‌هاست. اگر بتوان به‌نحوی داده‌های ورودی را کاهش داد. عملیات رمزنگاری با سرعت بیش‌تری انجام خواهد پذیرفت. برای این منظور روش گروه‌بندی پیکسل‌ها را پیشنهاد می‌دهیم. در این روش، چند پیکسل توسط یک الگوریتم با هم ترکیب می‌شوند و مجموعه آن‌ها با هم به صورت یک‌جا رمز می‌گردد. بعد از رمزگشایی، پیکسل‌های ترکیبی به صورت منحصر به فرد تجزیه خواهند شد. روش ارایه‌شده در [۱۶] به گروه‌بندی پیکسل‌ها می‌پردازد. مشکلی که این طرح پیشنهادی دارد این است که وقتی پیکسل صفر در تصویر ظاهر شود دستور From Digits پاسخ درستی برنمی‌گرداند. مثلاً اگر پیکسل‌های ۰ و ۱۰ را بخواهیم با این دستور ترکیب کنیم، فرمت دستور به صورت From Digits [{0,10}, 256] خواهد بود که نتیجه این دستور، عدد ۱۰ را برمی‌گرداند. با اجرای دستور معکوس آن، یعنی Integer Digits [10 , 256] فقط عدد ۱۰ در خروجی ظاهر می‌شود، درصورتی‌که پاسخ ۰ و ۱۰ بوده است. نگارنده مقاله برای برطرف‌کردن این مشکل، به صورت رندم عدد ۱ یا ۲ را به مقادیر پیکسل‌ها اضافه کرده است. افزایش مقادیر پیکسل‌ها در نگاه اول ممکن است اهمیت چندانی نداشته باشد ولی با نگاهی دقیق‌تر متوجه خواهیم شد که این امر منجر به افزایش حافظه مورد نیاز برای پردازش تصویر خواهد شد. چرا که با اضافه‌شدن مقادیر پیکسل‌ها، اعداد ۲۵۶ یا ۲۵۷ تولید می‌شود و همان‌طورکه می‌دانید این اعدا برای ذخیره‌سازی به دو بایت حافظه نیاز دارند.

۴- طرح پیشنهادی

برای اجرای عملیات رمزنگاری ابتدا یک بلوک $m \times n = i$ از تصویر انتخاب کرده و آن‌ها را به صورت یک بردار مرتب می‌کنیم. همان‌طورکه می‌دانیم سطح روشنایی پیکسل‌ها بین ۰ تا ۲۵۵ متغیر است. با توجه به اندازه کلید رمزنگاری، i تا از پیکسل‌ها را معادل $b_1, b_2, ..., b_i$ قرار می‌دهیم و برای مقادیر مدول‌ها $m_1, m_2, ..., m_i$ اعداد اول بیش‌تر از ۲۵۵ را انتخاب می‌کنیم. مثلاً $m_1 = 257, m_2 = 263, ...$ دلیل انتخاب اعداد اول بزرگ‌تر از ۲۵۵ این است که طبق نکته ۱ تک‌تک معادلات باید دارای جواب باشند لذا با توجه به سطح روشنایی پیکسل‌ها، پیمانه‌ها باید بیش‌تر از ۲۵۵ باشد تا پس از حل معادلات، مقادیری بین ۲۵۵-۰ حاصل شوند.

مثال: فرض کنید دو پیکسل ۱۵۰ و ۲۰۴ را می‌خواهیم به روش باقی‌مانده چینی ترکیب کنیم. معادلات را به صورت زیر تشکیل می‌دهیم:

$$\begin{cases} x \equiv 150 \mod 257 \\ x \equiv 204 \mod 263 \end{cases}$$

$$M = 257 \times 263 = 67591, \quad M_1 = \frac{M}{m_1} = 263, M_2 = \frac{M}{m_2} = 257$$

$$M_1' = M_1^{-1} (\mathrm{mod}\, m_1) = 43, \quad M_2' = M_2^{-1} (\mathrm{mod}\, m_2) = 219$$

$$x = b_1 M_1 M_1' + b_2 M_2 M_2' (\mathrm{mod}\, M) = (150)(263)(43) + \\ + (204)(257)(219) \mod(67591) = 65428$$

در نهایت، به‌جای دو پیکسل ۱۵۰ و ۲۰۴ عدد حاصل از ترکیب آن‌ها یعنی ۶۵۴۲۸ رمز می‌شود. به این ترتیب به جای، دوبار اجرای الگوریتم رمزنگاری برای تک‌تک پیکسل‌های ذکرشده، توانستیم با یک بار اجرا، هر دو پیکسل را رمز کنیم. در سمت گیرنده، بعد از رمزگشایی پیام ارسالی، عدد ۶۵۴۲۸ ظاهر خواهد شد. حال برای به‌دست‌آوردن پیکسل‌های معادل با توجه به عدد به‌دست‌آمده، کافی است این عدد را به‌ترتیب در هنگ اعداد اول ۲۵۷ و ۲۶۳ محاسبه کنیم. مشاهده می‌شود که باقی‌مانده همان مقادیر پیکسل‌ها هستند.

$$65428 (\mathrm{mod}\, 257) = 150$$
$$65428 (\mathrm{mod}\, 263) = 204$$

جدول (۱): بیشترین پیکسل‌های انتخابی

تعداد پیکسل انتخابی	پارامترهای خم برحسب بیت
۷	۶۴
۱۵	۱۲۸
۳۰	۲۵۶
۵۸	۵۱۲

این‌که بتوان چند پیکسل را با هم به صورت یک گروه درنظر گرفت و به یک‌باره رمز کرد، به پارامترهای خم بیضوی انتخابی وابسته است. هرچقدر این پارامترها بزرگ‌تر باشند، تعداد بیش‌تری پیکسل را می‌توان به صورت یک گروه درنظر گرفت. جدول (۱) تعداد پیکسل‌هایی که می‌توان به صورت یک گروه انتخاب کرد را به ازای پارامترهایی با طول مختلف نشان می‌دهد.

۴-۱- رمزنگاری تصویر

ابتدا گیرنده و فرستنده روی یک خم بیضوی E و یک نقطه مولد G توافق می‌کنند. سپس عملیات رمزنگاری به ترتیب زیر انجام می‌شود:

۱- ابتدا یک بلوک $m \times n = i$ از تصویر انتخاب می‌شود و سپس این بلوک از پیکسل‌ها به فرم برداری مرتب می‌گردند.

۲- با توجه به قضیه باقی‌مانده چینی، i معادله تشکیل داده که بخش معلوم این معادلات همان مقادیر پیکسل‌ها هستند.

۳- با استفاده از رابطه (۱۴)، این دسته معادلات هم‌نهشتی را حل و مقدار x را به‌دست می‌آوریم. مقدار x به‌دست آمده همان پیام است که می‌خواهیم رمز کنیم.

۴- مقدار x به‌دست‌آمده را با استفاده از جدول تطابق به نقطه‌ای روی خم بیضوی منتقل می‌کنیم.

۵- با استفاده از الگوریتم الجمال، عملیات رمزنگاری را برروی نقطه به‌دست‌آمده انجام داده و نقاط جدیدی به‌دست می‌آوریم.

۶- با استفاده از جدول تطابق نقاط رمزشده روی خم بیضوی را به اعداد معادل آن‌ها تبدیل می‌کنیم. این مقدار در شکل (۲) با حرف Y نشان داده شده است.

۷- اعداد به‌دست‌آمده را در هنگ اعداد اول بزرگ‌تر از ۲۵۵ به‌ترتیب محاسبه می‌کنیم. باقی‌مانده‌های به‌دست‌آمده همان پیکسل‌های تصویر رمزشده هستند.

۴-۲- رمزگشایی تصویر

پس از این‌که تصویر رمزشده توسط گیرنده دریافت شد، گیرنده با استفاده از کلید خصوصی خود عملیات رمزگشایی را به‌ترتیب زیر انجام می‌دهد:

۱- ابتدا گیرنده با گروه‌بندی پیکسل‌ها مقدار Y' را محاسبه می‌کند. با توجه به شکل (۲)، این مقدار حاصل گروه‌بندی پیکسل‌های تصویر رمزشده است. سپس با استفاده از جدول تطابق، نقاط معادل آن‌ها را روی خم بیضوی مشخص می‌کند.

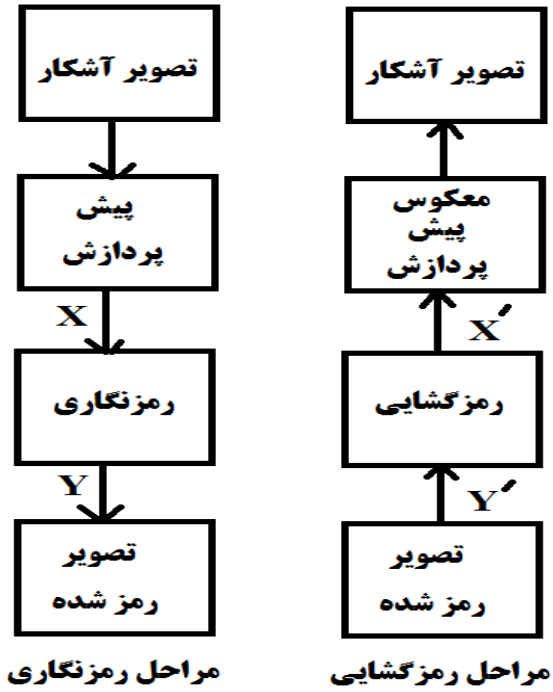
۲- در مرحله بعد، با استفاده از کلید خصوصی خود پیام رمزشده را آشکار کرده و مجموعه‌ای از نقاط مربوط به خم بیضوی مورد توافق را به‌دست می‌آورد.

۳- با استفاده مجدد از جدول تطابق، این نقاط را به اعداد معادل آن‌ها تبدیل می‌کند تا مقدار X' به‌دست آید.

۴- گیرنده، باقی‌مانده X' را با توجه به اندازه بلوک انتخابی، به‌ترتیب بر اعداد اول بزرگ‌تر از ۲۵۵ محاسبه می‌کند.

۵- باقی‌مانده‌های محاسبه‌شده مقادیر پیکسل‌های تصویر آشکار هستند که به فرم برداری می‌باشند. با اجرای عملیات معکوس، این بردارهای محاسبه‌شده را به فرم بلوکی $m\times n$ تبدیل می‌کنیم.

۶- در انتها با قراردادن بلوک‌های $m\times n$ کنار هم تصویر اصلی ساخته می‌شود.

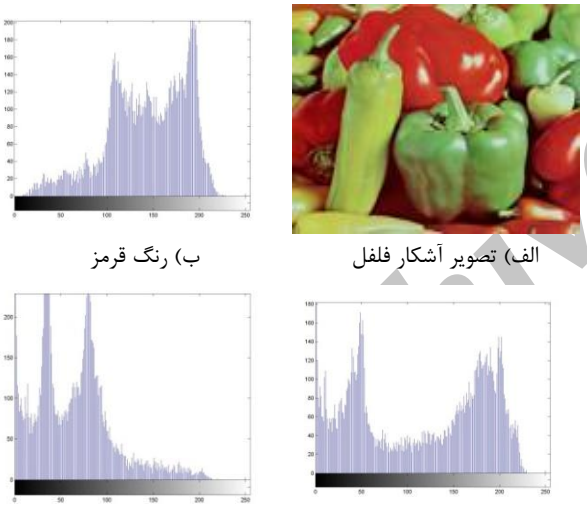


شکل (۲): فلوچارت رمزنگاری و رمزگشایی

۵- شبیه‌سازی و بررسی نتایج رمزنگاری و رمزگشایی تصویر

در این شبه سازی از نرم افزار متلب[1] R2013b(8.2.0.701) استفاده شده است. فرض کنید که آلیس گیرنده پیام باشد، آنگاه باب با استفاده از کلید عمومی آلیس، تصویر را با استفاده از رابطه $pc=[(m+k\times pua),(k\times G)]$ رمز می کند که در آن m پیام و k یک عدد رندم است. (در این شبیه سازی اعداد رندم بین ۱:۴۰۰۰ انتخاب شده اند)، pua کلید عمومی آلیس و G نقطه مولد است. برای رمز گشایی ، آلیس با استفاده از کلید خصوصی خود، $m=[(m+k\times pua)-(pra\times k\times G)]$ را محاسبه می کند که در این عبارت pra کلید خصوصی آلیس است. برای شبیه سازی پارامتر ها به صورت زیر انتخاب شده اند.

منحنی بیضوی $E: y^2=x^3+2477x+199$ روی میدان اولیه $F_p=69997$ و نقطه مولد $G=(502,27795)$است. کلید خصوصی آلیس $pra=7$ و کلید خصوصی باب $prb=20$ در نظر گرفته شده است. در نتیجه کلید عمومی آلیس برابر با $pua=pra\times G=(35644,62140)$ و کلید عمومی باب برابر با $pub=prb\times G=(12816,68291)$ خواهد بود.



الف) تصویر آشکار فلفل — ب) رنگ قرمز

ج)رنگ سبز — د)رنگ آبی

شکل (۳): تصویر آشکار فلفل و هیستوگرام رنگ‌های آن

شکل(۳) یک تصویر رنگی آشکار و هیستوگرام کانال‌های رنگی آن‌را نشان می‌دهد. محور افقی نشان‌دهنده سطوح خاکستری تصویر است که از ۰-۲۵۵ شماره‌گذاری شده است و محور عمودی، تعداد تکرار هر سطح خاکستری را نشان می‌دهد. با استفاده از نمودار هیستوگرام تصویر، می‌توان دریافت که هر پیکسل با سطح روشنایی خاص چندبار در تصویر ظاهر شده است. هیستوگرام تصویر، اطلاعاتی ازقبیل میزان روشنایی تصویر، وضوح تصویر و رنج دینامیکی آن به ما می‌دهد که می‌تواند در

1- MatLab

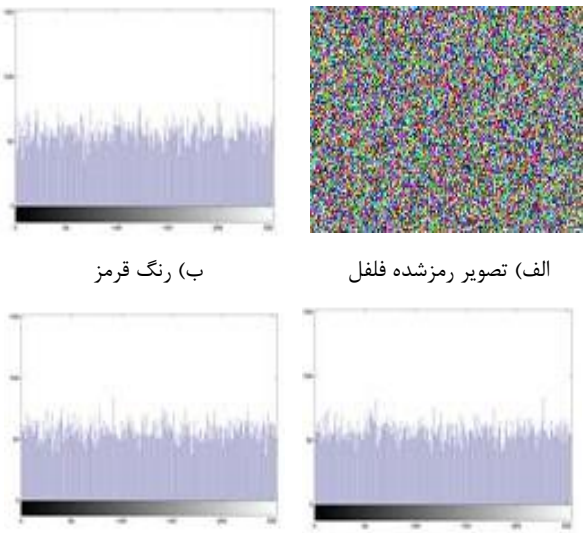
تحلیل یک تصویر رمزشده مورد استفاده قرار گیرد. یک الگوریتم رمزنگاری خوب می‌بایست هیستوگرام تصویر را به‌گونه‌ای تغییر دهد که هیچ‌گونه اطلاعاتی از آن قابل درک نباشد.

۶- آنالیز و بررسی امنیت

در این بخش به بررسی مشخصه های امنیتی تصاویر رمز شده و مقایسه آن ها با تصاویر آشکار می پردازیم. از مهمترین این مشخصه ها شامل هیستوگرام تصویر، همبستگی بین پیکسل ها و آنتروپی یک تصویر می باشند. عملیات رمزنگاری، تغییرات اساسی در شکل و مقدار این مشخصه ها ایجاد می کند که باعث بالا رفتن امنیت اطلاعات رمزنگاری شده می گردد. برای یک تصویر رمز شده ضریب همبستگی بین پیکسل ها به شدت کاهش می یابد و آنتروپی آن به بیشترین مقدار خود خواهد رسید.

۶-۱- هیستوگرام تصویر

نمودار هیستوگرام یک تصویر نشان‌دهنده میزان تکرار یک پیکسل با سطح روشنایی مشخص است. در یک تصویر رمزشده می‌بایست پیکسل‌ها با سطوح روشنایی تقریباً به یک میزان تکرارشده باشند. با توجه به شکل (۴) مشاهده می‌شود که نمودار هیستوگرام تصویر رمزشده، همه سطوح روشنایی را شامل می‌شود و میزان رخداد آن‌ها نیز تقریباً برابر است.



الف) تصویر رمزشده فلفل ب) رنگ قرمز

ج) رنگ سبز د) رنگ آبی

شکل (۴): تصویر رمزشده فلفل و هیستوگرام رنگ‌های آن

الف) تصویر رمزشده ب) کلید صحیح ج) کلید اشتباه

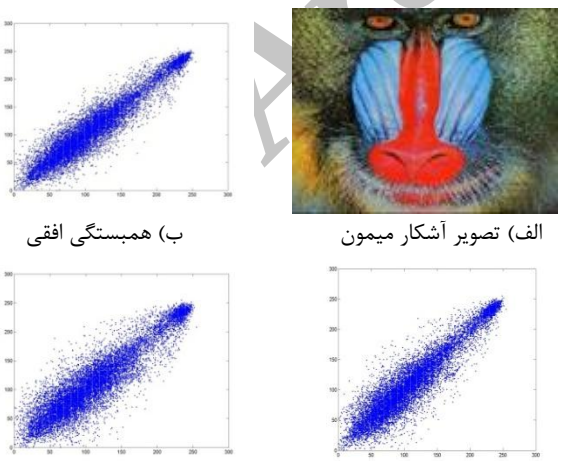
شکل (۵): نتیجه رمزگشایی تصویر اسب با کلید صحیح و اشتباه

۶-۲- حساسیت به کلید

امنیت یک الگوریتم رمزنگاری می‌بایست وابسته به کلید باشد. لذا استفاده از کلید اشتباه نباید نتیجه‌ای دربرداشته باشد. در شکل (۵) یک تصویر رمزشده، یک بار با استفاده از کلید صحیح و یک بار با کلید $pra-1$ رمزگشایی شده است. همان‌طورکه مشاهده می‌شود، رمزگشایی با کلید اشتباه هیچ نتیجه‌ای دربرندارد.

۶-۳- بررسی همبستگی

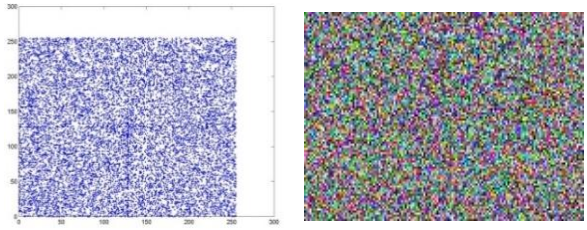
در یک تصویر آشکار، میزان همبستگی بین پیکسل‌ها بسیار زیاد است. در تصویر رمزشده این میزان همبستگی، باید بسیار ناچیز باشد. در شکل‌های (۷-۶) نمودار میزان همبستگی رنگ قرمز تصویر اصلی و تصویر رمزشده در سه راستای افقی، عمودی و قطری نشان داده شده است. همان‌طورکه مشاهده می‌شود در تصویر آشکار نمودار میزان همبستگی، حول محور y=x متمرکز شده است که نشان‌دهنده میزان همبستگی بالای پیکسل‌های تصویر آشکار است. درحالی‌که در تصویر رمزشده، این نقاط در کل صفحه پراکنده شده اند.



الف) تصویر آشکار میمون ب) همبستگی افقی

ج) همبستگی عمودی د) همبستگی قطری

شکل (۶): نمودار همبستگی پیکسل های تصویر آشکار



الف) تصویر رمز شده میمون ب) همبستگی افقی

ج) همبستگی عمودی د) همبستگی قطری

شکل (۷): نمودار همبستگی پیکسل‌های تصویر رمزشده

۶-۴- آنتروپی تصویر

مقدار آنتروپی با رابطه $entropy = -\sum p_i \log_2 p_i$ محاسبه می‌شود که در آن p_i احتمال حضور پیکسل با سطح روشنایی i است. با توجه به این رابطه می‌توان نتیجه گرفت که اگر همه سطوح روشنایی با احتمال یکسان در تصویر ظاهر شوند آن‌گاه احتمال هر سطح روشنایی برابر با $1/256$ خواهد بود. لذا در حالت ایده‌آل آنتروپی تصویر رمزشده، برابر با ۸ خواهد بود. این مقدار برای تصویر رمزشده می‌بایست به عدد ۸ نزدیک باشد. آنتروپی سه تصویر رمزشده مربوط به اسب، میمون و فلفل در جدول (۴) آورده شده است. این مقادیر محاسبه‌شده، به عدد ۸ بسیار نزدیک است که نشان‌دهنده آنتروپی بالای تصویر رمزشده است.

۶-۵- حمله از طریق متن شناخته شده

در شکل (۸) یک تصویر کاملاً سیاه برای رمزنگاری انتخاب شده است. نتایج دو بار اجرای الگوریتم رمزنگاری در شکل (۸- ب) و (۸- ج) نشان داده شده است. با توجه به این‌که نمی‌توان اختلاف میان این دو تصویر را مشاهده کرد، لذا برای نشان‌دادن این اختلاف اندازه حاصل تفریق این دو شکل رمزشده، در شکل (۸- د) نمایش داده شده است. همان‌طورکه از شکل پیداست اختلاف زیادی بین این دو تصویر وجود دارد. بنابراین نمی‌توان با استفاده از آن کلید رمزنگاری را پیدا کرد.

جدول (۲): ضرایب همبستگی تصویر آشکار میمون

اجزای تصویر	افقی	عمودی	قطری
قرمز	۰/۹۵۲۳۵۸	۰/۹۴۳۹۷۷	۰/۹۲۰۹۱۶
سبز	۰/۸۸۷۹۵۳	۰/۸۸۴۳۰۹	۰/۸۳۲۳۶۹
آبی	۰/۹۲۹۰۲۶	۰/۹۳۱۶۴۲	۰/۸۹۰۳۲۶

جدول (۳): ضرایب همبستگی تصویر رمزشده میمون

اجزای تصویر	افقی	عمودی	قطری
قرمز	-۰/۰۰۲۲۵۴	-۰/۰۰۵۸۲۰	-۰/۰۰۴۶۳۳
سبز	۰/۰۱۲۸۹۶	-۰/۰۰۱۰۵۷	۰/۰۱۰۱۸۴
آبی	-۰/۰۰۵۹۹۵	-۰/۰۰۲۳۰۱	۰/۰۰۸۸۴۴

۶-۶- ضریب همبستگی

برای بررسی میزان همبستگی پیکسل‌های یک تصویر، پارامتری به‌نام ضریب همبستگی تعریف می‌شود. این پارامتر با استفاده از رابطه (۱۵) قابل محاسبه است. با توجه به میزان همبستگی دو متغیر، ضریب همبستگی مقداری بین {۱ تا ۱- } دارد.

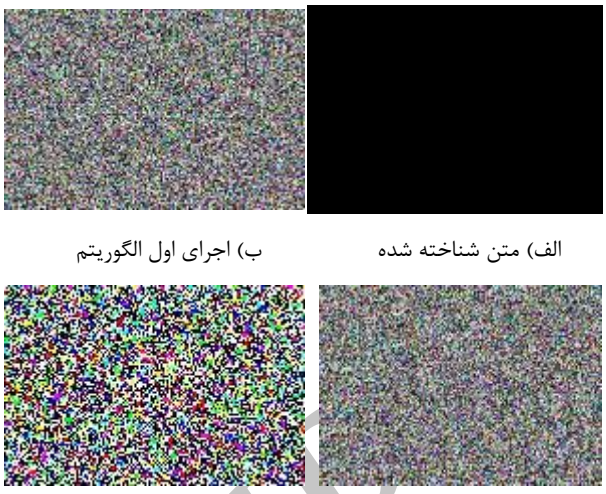
$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\left(\sum_{i=1}^{N}(x_i - E(x))^2\right)^{1/2} * \left(\sum_{i=1}^{N}(y_i - E(y))^2\right)^{1/2}} \quad (۱۵)$$

هرچقدر میزان همبستگی دو متغیر نسبت به هم کم‌تر باشد، ضریب همبستگی آن دو متغیر به سمت صفر میل می‌کند [۹]. با مقایسه جدول‌های (۳ و ۲) مشاهده می‌شود که الگوریتم پیشنهاد شده، ضریب همبستگی بین پیکسل‌های تصویر رمزشده را به شدت کاهش داده و تا حد صفر پایین آورده است. درحالی‌که در تصویر آشکار ضریب همبستگی[1] بین پیکسل‌ها، بسیار زیاد بوده و به عدد ۱ نزدیک است.

جدول (۴): آنتروپی تصاویر رمزشده

تصویر	سایز تصویر	آنتروپی
اسب	۱۰۰×۱۵۰	۷/۹۹۴۵
میمون	۱۰۰×۱۵۰	۷/۹۹۲۰
فلفل	۱۰۰×۱۵۰	۷/۹۹۳۷

1- Correlation Coefficient



الف) متن شناخته شده ب) اجرای اول الگوریتم

ج) اجرای دوم الگوریتم د) اختلاف تصاویر (ب)و(ج)

شکل (۸): دوبار اجرای الگوریتم بر روی یک متن شناخته‌شده

۷- بررسی سرعت رمزنگاری طرح پیشنهادی

زمانی‌که رمزنگاری بر روی تک‌تک پیکسل ها انجام می‌گیرد [۱۳]، به تعداد پیکسل‌های تصویر، الگوریتم رمزنگاری می‌بایست اجرا گردد. طرح پیشنهادشده در این مقاله، با درنظر گرفتن یک مجموعه پیکسل به‌عنوان یک گروه و رمزنگاری یک‌باره آن‌ها، تعداد دفعات رمزنگاری را کاهش داده و همین امر باعث افزایش سرعت عملیات رمزنگاری می‌گردد. مقایسه سرعت انجام عملیات رمزنگاری طرح پیشنهادی ما با روش ارائه‌شده در [۱۳] در جدول (۵) نشان داده شده است. در این مقایسه یک تصویر با ابعاد ۱۵۰×۱۰۰ انتخاب شده و خم بیضوی با پارامتر های ۵۱۲ بیتی درنظر گرفته شده است. با توجه به جدول (۱)، با انتخاب پارامترهای ۵۱۲ بیتی می‌توان ماکزیمم تا ۵۸ پیکسل را به صورت یک گروه درنظر گرفت.

جدول (۵): مقایسه سرعت

تعداد دفعات اجرای الگوریتم	ابعاد تصویر	
۱۵۰۰۰	۱۵۰×۱۰۰	روش فعلی
۲۵۹	۱۵۰×۱۰۰	روش پیشنهادی

با درنظرگرفتن مقادیر جدول (۵) می‌توان نتیجه گرفت که سرعت عملیات رمزنگاری ۱۵۰۰۰/۲۵۹=۵۷/۹۱ برابر افزایش پیدا کرده است.

۸- نتیجه‌گیری

در این مقاله، به شبیه‌سازی الگوریتم رمزنگاری خم بیضوی بر روی تصاویر رنگی پرداخته شد. جهت بهبود سرعت اجرای عملیات رمزنگاری با گروه‌بندی پیکسل‌ها، تعداد دفعات اجرای الگوریتم رمزنگاری را کاهش دادیم. بررسی سرعت اجرای الگوریتم نشان داد که طرح پیشنهادی می‌تواند سرعت عملیات رمزنگاری را تا ۵۷/۹ برابر روش‌های فعلی افزایش دهد. این روش پیشنهادی تضمین می‌کند که عملیات رمزنگاری و رمزگشایی بدون ازدست‌دادن حتی یک بیت اطلاعات انجام گیرد. هم‌چنین نحوه گروه‌بندی پیکسل‌ها به‌طور کامل تشریح گردید و مشاهده شد که با انتخاب یک خم بیضوی با پارامترهای ۵۱۲ بیتی، می‌توان ۵۸ پیکسل را به صورت یک گروه در نظر گرفت. بررسی نتایج اجرای الگوریتم نشان داد که تصاویر رمزنگاری‌شده دارای بیش‌ترین آنتروپی هستند. هم‌چنین ضریب همبستگی بین پیکسل‌ها به شدت کاهش یافته است. از طرفی، نشان دادیم که اجرای چندباره الگوریتم رمزنگاری منجر به تولید تصاویر رمزشده کاملاً متفاوت خواهد شد که این امر در مقابل "حمله با استفاده از متن شناخته شده" بسیار مقاوم است.

۹- مراجع

[1] A. lotfi and M. Doustari, "A new protocol for mobile payments using cipher-signed based on elliptic curve," Journal of Electronic and Cyber Defense, vol. 3, no.1, pp. 53-61, 2013. (In Persian)

[2] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203-209, 1987.

[3] V. S. Miller, "Use of Elliptic Curve in Cryptography," Advances in cryptology CRYPTO 1985, NewYork: Springer-Verlag, pp. 417-429, 1985.

[4] A. kumar, Tyagi, M. Rana, N. ggarwal, P. Bhadana, and M. Rachna, "A Comparative Study of Public Key Cryptosystem based on ECC and RSA," International Journal on Computer Science and Engineering (IJOARCS), 2011.

[5] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory (IEEE T INFORM THEORY), vol. 31, Issue. 4, pp. 469-472, 1985.

[6] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1997.

[7] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography," Springer, 2004.

[8] C. W. Lawrence, "Elliptic Curves Number Theory and Cryptography," Taylor & rancis Group, Second Edition, 2008.

[9] J. Teeriaho, "Cyclic Group Cryptography with Elliptic Curves," Brasov., May 2011.

[10] A. Ahmed, A. El-Latif, and X. Niu, "A Hybrid Chaotic System and Cyclic Elliptic Curve for Image Encryption," AEU-International Journal of Electronics and Communications, Elsevier, issue 2, vol. 67, pp. 136–143, 2013.

[11] H. Liu and Y. Liu, "Cryptanalyzing an Image Encryption Scheme based on Hybrid Chaotic System and Cyclic Elliptic Curve," Optics and Laser Technology (Opt. Laser Technol.), Elsevier, vol. 56, pp.15–19, 2014.

[12] S. M. Celestin Vigila and K. Muneeswaran, "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications," International Journal of Network Security, vol. 14, no. 4, pp. 236–242, July 2012.

[13] A. Soleymani, M. J. Nordin, and M. A. Zulkarnain, "A Novel Public Key Encryption based on Elliptic Curves Over Prime Group Field," Journal of Image and Graphics, vol. 1, pp. 43–49, 2013.

[14] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin, "Image Encryption based on the Jacobian Elliptic Maps," The Journal of System and Software(J SYST SOFTWARE), Elsevier, vol. 86, pp. 2429–2438, 2013.

[15] L. Li, A. Abd El-Latif, and X. Niu, "Elliptic Curve ElGamal Based Homomorphic Image Encryption Scheme for Sharing Secret Images," Signal Processing (SIGNAL PROCESS), Elsevier, vol. 92, pp. 1069–1078, 2012.

[16] L. Tawalbeh, M. Mowafi, and W. Aljoby, "Use of Elliptic Curve Cryptography for Multimedia Encryption," IET Information Security, vol. 7, issue 2, pp. 67–74, 2012.

[17] L. Dolendro Singh and K. Manglem Singh, "Image Encryption using Elliptic Curve Cryptography," Procedia Computer Science, Elsevier, vol. 54, pp. 472 – 481, 2015.

Journal Of Electronical & Cyber Defence
Vol. 5, No. 3, 2017, Serial No. 19

Designing Fast Algorithm to Encrypt Images Using The Chinese Remainder Theorem and Elliptic Curve

Gh. R. Karamali*, E. Kavand

*Aeronautical University Of Science And Technology

(Received: 15/11/2016, Accepted: 13/02/2017)

ABSTRACT

Sending and receiving information confidentially has always been very important. The cryptography Plays a major role in exchanging information securely. For this purpose, several encryption algorithms are designed and implemented. Among the designed algorithms, the old RSA and Diffie-Hellman algorithms have been superseded by the elliptic curve encryption algorithm, due to its unique features. The proposed method has higher speed for image encryption and decryption in comparison with the current method. For this purpose, the grouping of pixels by remainder Chinese theorem has been employed. The proposed method is applicable on other data such as text, sound and video.

Keywords: Image Processing, Image Encryption, Image Decryption, Elliptic Curve Encryption, Chinese Reminder Theo

* Corresponding Author Email: g_karamali@iust.ac.ir