

طراحی الگوریتم سریع جهت رمز کردن تصاویر با استفاده از قضیه باقی مانده چینی و خم بیضوی

غلامرضا کرملی^{۱*}، عیسی کاوند^۲

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، به صورت محرمانه همواره از اهمیت بالایی برخوردار است. علم رمزنگاری نقش عمده‌ای در تبادل اطلاعات به صورت امن ایفا می‌کند. به همین منظور، الگوریتم‌های رمزنگاری متعددی طراحی و پیاده‌سازی شده است. از میان الگوریتم‌های طراحی شده، الگوریتم رمزنگاری خم بیضوی، به دلیل ویژگی‌های منحصر به فردش، 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 ارائه 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 باقی مانده 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 باقی مانده چینی.

۱- مقدمه

الگوریتم‌های رمزنگاری به دو دسته کلید متقارن و کلید نامتقارن تقسیم‌بندی می‌شوند. در سامانه رمزنگاری 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 می‌شود. سامانه رمزنگاری برپایه خم بیضوی^۱، یک سامانه رمزنگاری کلید عمومی است. این سامانه رمزنگاری توسط کوبلیتز^۲ [۲] و میلر^۳ [۳] معرفی گردید. خم‌های بیضوی در مقایسه با پروتکل^۴ RSA 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

بیان شده، از این سامانه برای رمزنگاری تصاویر استفاده شد. در این مقاله، از روش رمزنگاری الجمال [۵] برای رمزنگاری تصویر و از قضیه باقی مانده چینی^۶ 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 بر روی 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.

$$E: y^2 = x^3 + ax + b \quad (1)$$

۱-۱-۱- قانون جمع نقاط

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

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

1- Elliptic Curve
2- Koblitz
3- Miller
4- protocol
5- Rivest-Shamir-Adleman

اول باشند، یعنی $\gcd(m_i, m_j) = 1$ و b_1, b_2, \dots, b_r اعداد صحیح اختیاری باشند، در این صورت، دستگاه هم‌نهستی زیر دارای دقیقاً یک جواب در هنگ $M = m_1 \times m_2 \times \dots \times m_r$ می‌باشد.

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_r \pmod{m_r} \end{cases} \quad (11)$$

برای حل این معادلات تعریف می‌کنیم:

$$M \square m_1 m_2 \dots m_r \quad (12)$$

$$M_k \square \frac{M}{m_k} \Rightarrow \gcd(M_k, m_k) = 1 \quad (13)$$

$$x = b_1 M_1 M'_1 + b_2 M_2 M'_2 + \dots + b_r M_r M'_r \pmod{M} \quad (14)$$

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

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

۲- مروری بر کارهای 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^۱، آلفرد منز^۲ و وانستون^۳ [۷] مطالعات خود را روی محاسبات، کاربردها و پروتکل‌های رمزنگاری خم‌های بیضوی گوناگون انجام دادند. لارنس سی واشنگتن^۴ [۸] به اثبات برخی نظریه‌های مربوط به خم‌های بیضوی پرداخت. جوکو تریاهو^۵ [۹] با استفاده از نرم‌افزار متمتیکاً جنبه‌های مختلف خم بیضوی را مورد بررسی قرار داد. احمد عبدالطیف^۶ و زیامو^۷ [۱۰] برای رمزنگاری تصویر از فن خم‌های بیضوی و سامانه آشوبی استفاده کردند. آن‌ها با استفاده

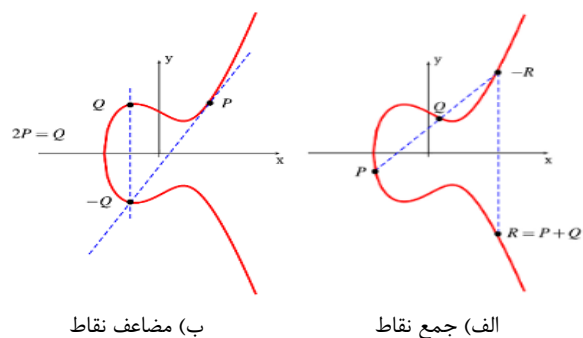
محدود p تعریف شده است، باشند. آن‌گاه این دو نقطه با استفاده از روابط زیر با هم جمع خواهند شد:

$$P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3) \quad (2)$$

$$x_3 = (\lambda^2 - x_1 - x_2) \pmod{p} \quad (3)$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{p} \quad (4)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad (5)$$



شکل (۱): تعبیر هندسی جمع و مضاعف نقاط

۲-۱-۱- قانون مضاعف نقاط

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

$$P(x_1, y_1) + P(x_1, y_1) = R(x_3, y_3) \quad (6)$$

$$x_3 = (\lambda^2 - 2x_1) \pmod{p} \quad (7)$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{p} \quad (8)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p} \quad (9)$$

۳-۱-۱- قانون مضاعف نقاط

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

$$kP = P + P + \dots + P \quad (k \text{ times}) \quad (10)$$

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

۲-۱- قضیه باقی‌مانده چینی [۶]

اگر اعداد صحیح مثبت m_1, m_2, \dots, m_r دو به دو نسبت به هم

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

۳- طرح مسئله

همان طور که می دانیم یکی از روش های رمزنگاری تصویر، انجام عملیات رمز بر روی تک تک پیکسل هاست. اگر بتوان به نحوی داده های ورودی را کاهش داد. عملیات رمزنگاری با سرعت بیش تری انجام خواهد پذیرفت. برای این منظور روش گروه بندی پیکسل ها را پیشنهاد می دهیم. در این روش، چند پیکسل توسط یک الگوریتم با هم ترکیب می شوند و مجموعه آن ها با هم به صورت یک جرم می گردد. بعد از رمزگشایی، پیکسل های ترکیبی به صورت منحصر به فرد تجزیه خواهند شد. روش ارایه شده در [۱۶] به گروه بندی پیکسل ها می پردازد. مشکلی که این طرح پیشنهادی دارد این است که وقتی پیکسل صفر در تصویر ظاهر شود دستور From Digits پاسخ درستی بر نمی گرداند. مثلاً اگر پیکسل های ۰ و ۱۰ را بخواهیم با این دستور ترکیب کنیم، فرمت دستور به صورت $\text{From Digits } \{0,10\}, 256$ خواهد بود که نتیجه این دستور، عدد ۱۰ را برمی گرداند. با اجرای دستور معکوس آن، یعنی $\text{Integer Digits } [10, 256]$ فقط عدد ۱۰ در خروجی ظاهر می شود، در صورتی که پاسخ ۰ و ۱۰ بوده است. نگارنده مقاله برای برطرف کردن این مشکل، به صورت رندم عدد ۱ یا ۲ را به مقادیر پیکسل ها اضافه کرده است. افزایش مقادیر پیکسل ها در نگاه اول ممکن است اهمیت چندانی نداشته باشد ولی با نگاهی دقیق تر متوجه خواهیم شد که این امر منجر به افزایش حافظه مورد نیاز برای پردازش تصویر خواهد شد. چرا که با اضافه شدن مقادیر پیکسل ها، اعداد ۲۵۶ یا ۲۵۷ تولید می شود و همان طور که می دانید این اعداد برای ذخیره سازی 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 آن ها را به صورت یک بردار مرتب می کنیم. همان طور که می دانیم سطح روشنایی پیکسل ها بین ۰ تا ۲۵۵ متغیر است. با توجه به اندازه کلید رمزنگاری، i تا از پیکسل ها را معادل b_1, b_2, \dots, b_i قرار می دهیم و برای مقادیر مدول ها m_1, m_2, \dots, m_i اعداد اول بیش تر از ۲۵۵ را انتخاب می کنیم. مثلاً $m_1 = 257, m_2 = 263, \dots$. دلیل انتخاب اعداد اول بزرگ تر از ۲۵۵ این است که طبق نکته ۱ تک تک معادلات باید دارای جواب باشند لذا با توجه به سطح روشنایی پیکسل ها، پیمانها باید بیش تر از ۲۵۵ باشد تا پس از حل معادلات، مقادیری بین ۰-۲۵۵ حاصل شوند.

از نقاط خم های بیضوی و سامانه آشوبی یک رشته کلید شبه تصادفی پیشنهاد دادند که از آن برای رمزنگاری تصویر استفاده می شد. هانگ لیو^۱ و یانگ بینگ^۲ [۱۱] پیشنهادی برای رمزگشایی تصویر رمز شده با استفاده از سامانه ترکیبی آشوبی و خم های بیضوی ارائه کردند. آن ها دریافتند که با استفاده از متن آشکار و انتخاب یک تصویر که تمام پیکسل های آن صفر باشد، می تواند تصویر رمز شده را تولید کنند. ماریا^۳ و مانیس وارن^۴ [۱۲] الگوریتمی برای رمزنگاری تصویر با استفاده از خم های بیضوی ارائه کردند. آن ها از یک زوج مولد خطی همبسته برای تولید کلید خصوصی و یک عدد تصادفی k استفاده کردند. برای به دست آوردن تصویر رمز شده برای هر پیکسل ضرب نقطه ای انجام می گرفت و با استفاده از مولد بر روی خم بیضوی قرار می گرفت. در این روش یک جدول تطابق برای رمزگشایی مورد نیاز است. علی سلیمانی، جان نوردین و زولکاریان [۱۳] یک تکنیک رمزنگاری با استفاده از خم های بیضوی روی میدان محدود ارائه دادند. آن ها 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 رمز شده دوباره از جدول تطابق استفاده می شد و نقاط به اعداد ۲۵۵-۰ تبدیل می شدند. بهیان، اخوان، اخشانی و شمس الدین [۱۴] از مختصات ژاکوبین خم بیضوی برای رمزنگاری استفاده کردند. آن ها با استفاده از کلید رمزنگاری و انجام اعمالی بر روی ماتریس تصویر آن را به یک ماتریس یک بعدی تبدیل کردند. به این ترتیب، با استفاده از معادلات خم های بیضوی رمزنگاری انجام می شد. احمد عبدالطیف و زیامونو [۱۵] با استفاده از الگوریتم الجمال در رمزنگاری خم های بیضوی و برپایه تصاویر هم شکل، یک تصویر مجرمانه را به اشتراک گذاشتند. آن ها پارامترهایی برای خم بیضوی در نظر گرفتند که در مقابل حمله پولارد^۵ و هم چنین فولینگ هلمن^۶ مقاوم بود. لویی، موافی و ولید الجوبی^۷ [۱۶] از دو خم بیضوی و هم چنین ضرایب DCT تصویر، برای رمزنگاری استفاده کردند. دولندرو و منگ لم^۸ [۱۷] با گروه بندی پیکسل ها و به دست آوردن یک عدد بزرگ، تعداد عملیات رمزنگاری را کاهش دادند. آن ها با استفاده از دستوری در نرم افزار متمتیکا^۹ این گروه بندی را انجام دادند.

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

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 هم‌نهستی را حل و مقدار x را به دست می‌آوریم. مقدار x به دست آمده همان پیام است که می‌خواهیم رمز کنیم.

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

۵- با استفاده از الگوریتم الجمال، عملیات رمزنگاری را بر روی نقطه به دست آمده انجام داده و نقاط جدیدی به دست می‌آوریم.

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

۷- اعداد به دست آمده را در هنگ اعداد اول بزرگ‌تر از ۲۵۵ به ترتیب محاسبه می‌کنیم. باقی‌مانده‌های به دست آمده همان پیکسل‌های تصویر رمز شده هستند.

۴-۲- رمزگشایی تصویر

پس از این که تصویر رمز شده توسط گیرنده دریافت شد، گیرنده با استفاده از کلید خصوصی خود عملیات رمزگشایی را به ترتیب 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 رمز شده است. سپس با استفاده از جدول تطابق، نقاط معادل آن‌ها را روی خم بیضوی مشخص می‌کند.

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

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

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

$$M_1' = M_1^{-1} \pmod{m_1} = 43, \quad M_2' = M_2^{-1} \pmod{m_2} = 219$$

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

در نهایت، به جای دو پیکسل ۱۵۰ و ۲۰۴ عدد حاصل از ترکیب آن‌ها یعنی ۶۵۴۲۸ رمز می‌شود. به این ترتیب به جای، دوبار اجرای الگوریتم رمزنگاری برای تک تک پیکسل‌های ذکر شده، 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 به دست آوردن پیکسل‌های معادل با توجه به عدد به دست آمده، کافی است این عدد را به ترتیب در هنگ اعداد اول ۲۵۷ و ۲۶۳ محاسبه کنیم. مشاهده می‌شود که باقی‌مانده همان مقادیر پیکسل‌ها هستند.

$$65428 \pmod{257} = 150$$

$$65428 \pmod{263} = 204$$

جدول (۱): بیشترین پیکسل‌های انتخابی

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

این که بتوان چند پیکسل را با هم به صورت یک گروه در نظر گرفت و به یک‌باره رمز کرد، به پارامترهای خم بیضوی انتخابی وابسته است. هر چقدر این پارامترها بزرگ‌تر باشند، تعداد بیش‌تری پیکسل را می‌توان به صورت یک گروه در نظر گرفت. جدول (۱) تعداد پیکسل‌هایی که می‌توان به صورت یک گروه انتخاب کرد

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

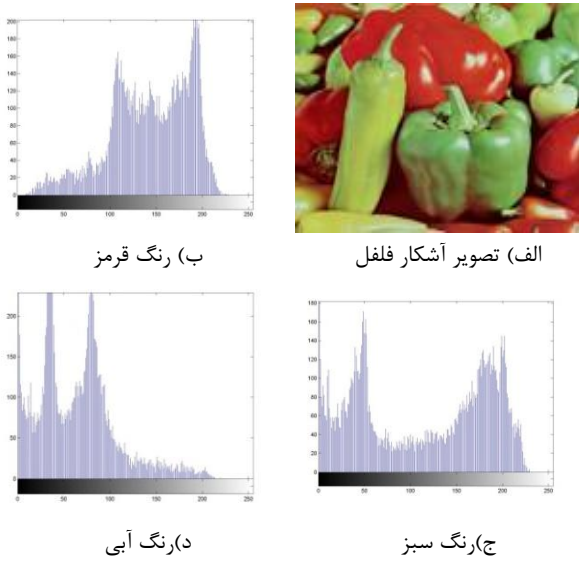
۳- با استفاده مجدد از جدول تطابق، این نقاط را به اعداد معادل آن‌ها تبدیل می‌کند تا مقدار X' به دست آید.

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

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

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

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.



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

شکل (۳) یک تصویر رنگی آشکار و هیستوگرام کانال‌های رنگی آن را نشان می‌دهد. محور افقی نشان‌دهنده سطوح خاکستری تصویر است که از ۰ تا 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 از قبیل میزان روشنایی تصویر، وضوح تصویر و رنج دینامیکی آن به ما می‌دهد که می‌تواند در

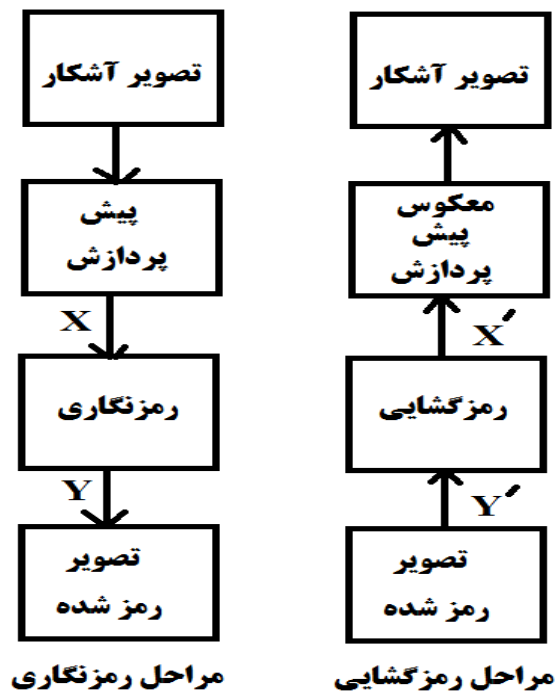
۲- در مرحله بعد، با استفاده از کلید خصوصی خود پیام رمز شده را آشکار کرده و مجموعه‌ای از نقاط مربوط به خم بیضوی مورد توافق را به دست می‌آورد.

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

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

۵- باقی مانده‌های محاسبه شده مقادیر پیکسل‌های تصویر آشکار هستند که به فرم برداری می‌باشند. با اجرای عملیات معکوس، این بردارهای محاسبه شده 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^۱ (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



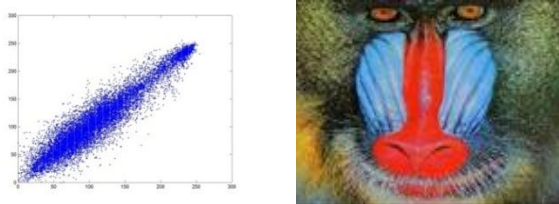
الف) تصویر رمز شده
ب) کلید صحیح
ج) کلید اشتباه
شکل (۵): نتیجه رمزگشایی تصویر اسب با کلید صحیح و اشتباه

۶-۲- حساسیت به کلید

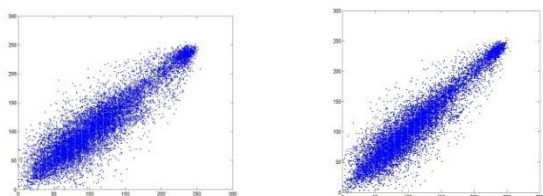
امنیت یک الگوریتم رمزنگاری می‌بایست وابسته به کلید باشد. لذا استفاده از کلید اشتباه نباید نتیجه‌ای دربرداشته باشد. در شکل (۵) یک تصویر رمز شده، یک بار با استفاده از کلید صحیح و یک بار با کلید $pra-1$ رمزگشایی شده است. همان‌طور که مشاهده می‌شود، رمزگشایی با کلید اشتباه هیچ نتیجه‌ای دربر ندارد.

۶-۳- بررسی همبستگی

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

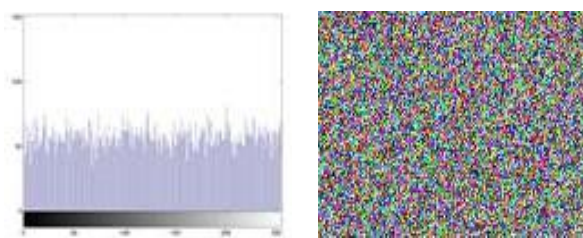
تحلیل یک تصویر رمز شده مورد استفاده قرار گیرد. یک الگوریتم رمزنگاری خوب می‌بایست هیستوگرام تصویر را به گونه‌ای تغییر دهد که هیچ گونه اطلاعاتی از آن قابل درک نباشد.

۶- آنالیز و بررسی امنیت

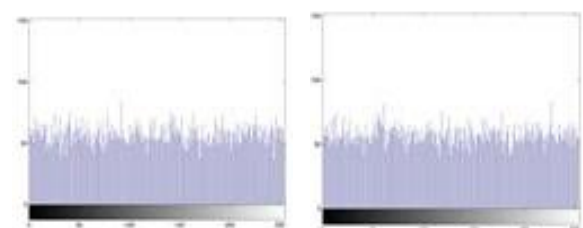
در این بخش به بررسی مشخصه‌های امنیتی تصاویر رمز شده و مقایسه آن‌ها با تصاویر آشکار می‌پردازیم. از مهمترین این مشخصه‌ها شامل هیستوگرام تصویر، همبستگی بین پیکسل‌ها و آنتروپی یک تصویر می‌باشند. عملیات رمزنگاری، تغییرات اساسی در شکل و مقدار این مشخصه‌ها ایجاد می‌کند که باعث بالا رفتن امنیت اطلاعات رمزنگاری شده می‌گردد. برای یک تصویر رمز شده ضریب همبستگی بین پیکسل‌ها به شدت کاهش می‌یابد 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 رمز شده می‌بایست پیکسل‌ها با سطوح روشنایی تقریباً به یک میزان تکرار شده باشند. با توجه به شکل (۴) مشاهده می‌شود که نمودار هیستوگرام تصویر رمز شده، همه سطوح روشنایی را شامل می‌شود و میزان رخداد آن‌ها نیز تقریباً برابر است.



الف) تصویر رمز شده فلفل
ب) رنگ قرمز



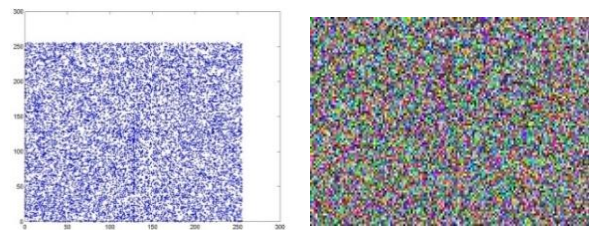
ج) رنگ سبز
د) رنگ آبی
شکل (۴): تصویر رمز شده فلفل و هیستوگرام رنگ‌های آن

جدول (۲): ضرایب همبستگی تصویر آشکار میمون

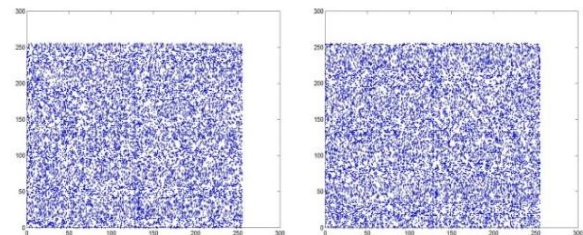
قطری	عمودی	افقی	اجزای تصویر
۰/۹۲۰۹۱۶	۰/۹۴۳۹۷۷	۰/۹۵۲۳۵۸	قرمز
۰/۸۳۲۳۶۹	۰/۸۸۴۳۰۹	۰/۸۸۷۹۵۳	سبز
۰/۸۹۰۳۲۶	۰/۹۳۱۶۴۲	۰/۹۲۹۰۲۶	آبی

جدول (۳): ضرایب همبستگی تصویر رمز شده میمون

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



الف) تصویر رمز شده میمون (ب) همبستگی افقی



ج) همبستگی عمودی (د) همبستگی قطری
شکل (۷): نمودار همبستگی پیکسل‌های تصویر رمز شده

۶-۶- ضریب همبستگی

برای بررسی میزان همبستگی پیکسل‌های یک تصویر، پارامتری به نام 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 $\{-1, 1\}$ دارد.

$$r_{xy} = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\left(\sum_{i=1}^N (x_i - E(x))^2\right)^{1/2} * \left(\sum_{i=1}^N (y_i - E(y))^2\right)^{1/2}} \quad (15)$$

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 رمز شده را به شدت کاهش داده و تا حد صفر پایین آورده است. درحالی که در تصویر آشکار ضریب همبستگی^۱ بین پیکسل‌ها، بسیار زیاد بوده و به عدد ۱ نزدیک است.

جدول (۴): آنتروپی تصاویر رمز شده

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

۴-۶- 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 رمز شده، برابر با ۸ خواهد بود. این مقدار برای تصویر رمز شده می‌بایست به عدد ۸ نزدیک باشد. آنتروپی سه تصویر رمز شده مربوط به اسب، میمون و فلفل در جدول (۴) آورده شده است. این مقادیر محاسبه شده، به عدد ۸ بسیار نزدیک است که نشان‌دهنده آنتروپی بالای تصویر رمز شده است.

۵-۶- حمله از طریق متن شناخته شده

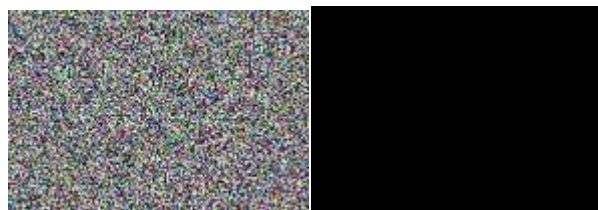
در شکل (۸) یک تصویر کاملاً سیاه برای رمزنگاری انتخاب شده است. نتایج دو بار اجرای الگوریتم رمزنگاری در شکل (۸-ب) و (۸-ج) نشان داده شده است. با توجه به این که نمی‌توان اختلاف میان این دو تصویر را مشاهده کرد، لذا برای نشان دادن این اختلاف اندازه حاصل تفریق این دو شکل رمز شده، در شکل (۸-د) نمایش داده شده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

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 $57/9$ 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 رمزنده کاملاً متفاوت خواهد شد که این امر در مقابل "حمله با استفاده از متن شناخته شده" بسیار مقاوم است.

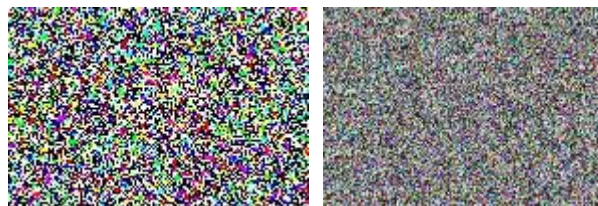
۹- مراجع

- [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. Teeriahoo, "Cyclic Group Cryptography with Elliptic Curves," Brasov., May 2011.



(ب) اجرای اول الگوریتم

(الف) متن شناخته شده



(د) اختلاف تصاویر (ب) و (ج)

(ج) اجرای دوم الگوریتم

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

۷- بررسی سرعت رمزنگاری طرح پیشنهادی

زمانی که رمزنگاری بر روی تک‌تک پیکسل‌ها انجام می‌گیرد [۱۳]، به تعداد پیکسل‌های تصویر، الگوریتم رمزنگاری می‌بایست اجرا گردد. طرح پیشنهادی در این مقاله، با در نظر 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 100×150 انتخاب شده و خم بیضوی با پارامترهای ۵۱۲ بیتی در نظر گرفته شده است. با توجه به جدول (۱)، با انتخاب پارامترهای ۵۱۲ بیتی می‌توان ماکزیمم تا ۵۸ پیکسل را به صورت یک گروه در نظر گرفت.

جدول (۵): مقایسه سرعت

تعداد دفعات اجرای الگوریتم	ابعاد تصویر	روش فعلی
۱۵۰۰۰	100×150	روش فعلی
۲۵۹	100×150	روش پیشنهادی

با در نظر گرفتن مقادیر جدول (۵) می‌توان نتیجه گرفت که سرعت عملیات رمزنگاری $15000/259 = 57/91$ برابر افزایش پیدا کرده است.

- [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.

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 Remainder Theo