مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۴، زمستان ۱۳۹۴، ص ۹-۱

یک طرح تسهیم چندراز بصری کارآمد

عبدالرسول میرقدری[1*]، فرشته شیخ سنگ‌تجن[2]
۱- دانشیار، دانشگاه جامع امام حسین(ع)
۲- پژوهشگر، دانشگاه جامع امام حسین(ع)
(دریافت: ۹۳/۰۳/۱۳، پذیرش: ۹۴/۱۰/۲۲)

چکیده

حفاظت از اطلاعات باارزش در راستای امنیت فضای تولید و تبادل اطلاعات یکی از مسائل راهبردی پدافند سایبری می‌باشد. طرح تسهیم راز شاخه‌ای جذاب از رمزنگاری پیشرفته است که در پدافند سایبری نقشی بسیار با اهمیت دارد و برای حفاظت از اسناد و اطلاعات محرمانه در برابر خطراتی چون دستبرد و دست‌یابی‌های غیرمجاز مورد استفاده قرار می‌گیرد. در طرح تسهیم راز، سهام‌داران برای افزایش امنیت در هنگام بازیابی تصاویر راز، به‌جای سهم اصلی، سهم سایه‌ای از تصویر را ارائه می‌نمایند. به‌عبارت دیگر هر سهام‌دار با در دست‌داشتن تنها یک سهم از تصویر راز، قادر است در بسیاری از تصاویر راز با دیگران سهیم شود. برخلاف طرح‌های تسهیم راز شناخته‌شده دیگر، در این طرح تصاویر سایه که برای کنترل و شناسایی دشوار باشند، تولید نمی‌شوند. بدین ترتیب هر سهام‌دار با در دست‌داشتن تنها یک سهم از تصویر راز قادر است در بسیاری از تصاویر راز با دیگران سهیم شود. ما در این مقاله با تعریف و طراحی یک تابع مولد جدید و جایگزین‌کردن آن با تابع مولد طرح هو ژنگ فنگ و همکارش توانستیم آن را بهبود دهیم. به‌دلیل یک‌طرفه‌بودن و سخت‌بودن تابع مولد جدید، امنیت طرح بهبودیافته افزایش یافته است. همچنین، با پیاده سازی و اجرای آن، مشاهده شد که از نظر تحلیلی و سرعت محاسبات طرح تغییر یافته کارآمدتر از طرح قبلی است.

واژه‌های کلیدی: تصویر راز، تابع مولد، طرح تسهیم چندراز بصری، تصویر سایه، تابع Doubleround(x)

۱- مقدمه

رمزنگاری از زمانی پایه‌گذاری شد، که افراد برای داشتن ارتباطی امن بدون اطلاع دشمن از مطالب تبادل‌شده بین‌شان، با هم ارتباط برقرار می‌کردند. به‌طوری‌که هرچه رمزشکنی سیستم‌های رمز برای مهاجمین سخت‌تر و پیچیده‌تر بود، امنیت بهتری را برای مشترکین خود فراهم می‌ساخت. از آنجایی‌که امنیت یک سیستم رمزنگاری وابسته به کلید آن است، شاید تصور شود بهترین روش در مدیریت کلید، قراردادن آن در یک مکان امن محافظت‌شده است؛ اما این روش غیرقابل اطمینان می‌باشد، زیرا یک اتفاق بد مانند خراب‌کاری عمدی یا سهوی افراد می‌تواند باعث غیرقابل دسترسی‌شدن اطلاعات شود. روش ساده برای جلوگیری از این امر، ذخیره‌کردن نسخه‌های متعددی از کلید (راز) در مکان‌های مختلف می‌باشد، اما این کار هم از امنیت کلید می‌کاهد. در مواقعی ممکن است مشکل ساده‌تر از بروز یک اتفاق غیرمنتظره باشد.

در سال ۱۹۷۹ شامیر و بلیکلی[1] [۲ - ۱] به‌طور مجزا طرح تسهیم راز[2] را پیشنهاد کردند. طرح تسهیم راز روشی است برای تسهیم اطلاعات راز بین افراد یک گروه معین، به‌طوری‌که هیچ‌یک از افراد آن گروه، با سهمی که به آنها تخصیص داده شده است، نتوانند به اطلاعات محرمانه یکدیگر و راز دست یابند و دست‌یابی به راز فقط با استفاده از سهم‌های مجموعه‌ای مشخص از افراد امکان‌پذیر باشد. بنابراین تسهیم راز سبب افزایش قابلیت اطمینان یک سیستم رمزنگاری می‌شود. در طرح تسهیم راز تمایل داریم که، دقیقاً مشخص کنیم کدام زیرمجموعه از سهام‌داران قادر به تعیین کلید باشند و کدام یک این امکان را نداشته باشند. فرض کنید Γ مجموعه‌ای از زیرمجموعه سهام‌داران P، درنظر گرفته شوند، زیرمجموعه‌های مجاز[3] در Γ همان زیرمجموعه‌هایی از سهام‌داران فرض می‌شوند که قادر به محاسبه کلید باشند. Γ را ساختار دست‌یابی[4] گویند.

رایانامه نویسنده پاسخگو: amrghadri@ihu.ac.ir

1- Shamir and Blakley
2- Secret Sharing Scheme (sss)
3- Participance
4- Access Structure

زیرمجموعه‌هایی از سهام‌داران P که قادر به بازسازی کلید نباشند را زیرمجموعه‌های غیرمجاز[1] می‌نامند.

در سال ۱۹۸۳ کارنین و همکارانش[2] [۳] طرح تسهیم راز کامل[3] را معرفی‌کردند و برای امنیت بهتر، نوعی از طرح تسهیم چندراز براساس ماتریس را پیشنهاد دادند. در کنفرانس یوروکریپت[4] سال ۱۹۹۴ نآوور و شمیر[5] [۵ -۴] ، نوع جدیدی از طرح تسهیم را پیشنهاد کردند که رمزنگاری بصری نامیده شد. این رمزنگاری روشی بود که در آن توزیع‌کننده یک تصویر راز را طوری در n صفحه شفاف تسهیم و بین n نفر توزیع می‌کرد که زیرمجموعه‌هایی از افراد با روی هم قراردادن شفافیت‌های خود می‌توانستند تصویر راز را بازیابی نمایند.

در این رمزنگاری سهام‌داران در یک زیرمجموعه مجاز، بدون هیچ‌گونه اطلاعی از علم رمزنگاری و بدون هیچ محاسبه پیچیده‌ای قادر خواهند بود تصویر اصلی را با انباشتن سهم‌های خود بازسازی نمایند اما زیرمجموعه‌ای از سهام‌داران که مجاز نبودند، با روی هم قراردادن شفافیت‌های خود، اطلاعاتی از راز به دست نیاورده و مجاز به دیدن تصویر راز نمی‌باشند.

در بیش‌تر طرح‌های تسهیم تصویر مانند [۷ -۶] تصاویر سایه تولید می‌شدند که کنترل، شناسایی و توزیع آن‌ها مشکل بودند و نقطه ضعف دیگر این طرح‌ها یک‌بار مصرف‌بودن[6] آن‌هاست و به‌طور معمول در این طرح‌های تسهیم راز بصری تعداد تصاویر راز محدود بود.

در سال ۲۰۰۸، هو ژنگ فنگ[7] و همکارش [۶] طرح تسهیم راز تصویری فشرده مبتنی بر طرح کارنین[8] [۳] را پیشنهاد کردند که در این طرح‌ها، تصویر راز به‌جای پیکسل منفرد به چندین بلوک مربعی غیراشتراکی تقسیم می‌شدند و هر بلوک به‌صورت یک ماتریس راز درنظر گرفته می‌شد. طرح آن‌ها می‌توانست تصویر سایه را براساس خصوصیت ضرایب ماتریس به $1/t$ تصویر راز کاهش داده و در فاز تسهیم تصویر نیازی به جایگشت نبود. این طرح‌ها، طرح چندراز مبتنی بر ماتریس بود که سهم‌های راز جدید باید هربار محاسبه و توزیع می‌شدند و سهم سهام‌داران بعد از بازیابی تصویر راز آشکار می‌شد و به این ترتیب فرآیند مذکور به طرح تقسیم راز یک‌بارمصرف تعلق داشت. با گسترش تعداد تصاویر راز، مبحثی جدید از طرح تسهیم راز برای مخفی‌کردن تصاویر چندراز مورد بررسی قرار گرفت که در آن کافی بود هر سهام‌دار سهم خود را دریافت و حفاظت نماید. باتوجه به پژوهش‌های صورت‌گرفته در طرح چندراز در آن زمان، هوژنگ‌فنگ و همکارش [۸] طرح پیشین خود را بهبود بخشیدند.

ما در این مقاله با تعریف و طراحی یک تابع مولد جدید و جایگزین‌کردن آن با تابع مولد طرح هو ژنگ فنگ و گائو هانجون[9] توانستیم طرح آنها را بهبود داده و به‌دلیل یک‌طرفه-بودن و سخت‌بودن تابع مولد جدید، مشاهده می‌شود، امنیت طرح آنها افزایش یافته است.

ساختار مقاله به این‌صورت بیان شده‌است، در بخش دوم طرح تسهیم چندراز هو ژنگ فنگ و گائو هانجون معرفی شده، در بخش سوم به تعریف توابع لازم در معرفی تابع مولد جدید پرداخته شده‌است، در بخش چهارم طرح جدید بهبودیافته ما ارائه شده است، سپس در بخش پنجم تحلیل این روش و مقایسه طرح پیشنهادی با چند طرح دیگر، صورت گرفته و نتیجه‌گیری در بخش ششم بیان شده است.

برنامه‌نویسی و شبیه‌سازی طرح در قسمت پیوست بیان شده است.

۲- معرفی طرح تسهیم چندراز هو ژنگ فنگ و گائو هانجون

طرح تسهیم تصاویر سایه‌ای چندراز، یک طرح تسهیم چندراز ویژه است که اساس آن بر تصویر سایه استوار است.

در سال ۲۰۰۹ هو ژنگ فنگ و همکارش [۸] در اصلاح طرح قبل‌شان [۶] براساس طرح تسهیم تصاویر چندراز مبتنی بر ضرب ماتریس طرحی را پیشنهاد کردند، که در آن سهام‌داران هنگام بازیابی تصاویر راز، در عوض سهم اصلی خود سهم‌های سایه را روی هم قرار می‌دادند، که با حفظ سهم اصلی هر سهام‌دار قادر بود در بسیاری از تصاویر راز با دیگران سهیم شود. در این طرح، برخلاف طرح‌های تسهیم راز شناخته‌شده، تصاویر سایه‌ای که برای کنترل و شناسایی دشوار باشند، تولید نمی‌شدند، طرح هوژنگ‌فنگ و همکارش، طرحی از تسهیم تصویر چندراز موثر و کاربردی بود و برخی اطلاعات کلی را به‌جای تولید تصاویر سایه آشکار می‌ساخت که در مراحل آن در زیر بیان شده است.

الف) مرحله آغازین

در این مرحله تابع یک‌طرفه دومتغیره $H(G,x)$ درنظر گرفته می‌شد و مقسم (D) تصویر راز را تقسیم می‌کرد سپس مجموعه‌ای از n ماتریس $\{A_1,\dots,A_n\}$ بر $GF(251)$ به‌عنوان معین‌کننده

1- Forbidden Sets
2- Karnin and et. als.
3- Perfect Secret Sharing Schem
4 - Eurocrypt
5 - Naor and Shamir
6- One Time Pad
7 -Huo Zheng Feng
8- Karnin
9 - Gao Hanjun

عمومی سهام‌داران p_i و در پی آن $n-t$، ماتریس $\{B_1,\dots,B_{n-t}\}$ بر $GF(251)$ به‌عنوان اطلاعات عمومی، درنظر می‌گرفت‌که باید هر بعد این ماتریس ها $nm \times m$ بوده و هر n از A_i رتبه کامل[1] داشته و هر t از A_i با $n-t$ از B_k نیز دارای رتبه کامل باشد به‌طوری‌که $1 \le i \le t, 1 \le k \le n-t$. و مقسم باید x_i را که $1 \le i \le n$ به‌عنوان سهم مخفی سهام‌داران p_i متناظر، انتخاب کند.

ب) مرحله تسهیم تصویر راز

در این فاز، S تصویر راز با اندازه $r \times r$ درنظر گرفته می‌شود که مقسم، چنین عمل می‌کند.

۱. تصویر راز S در چند بلوک غیراشتراکی S_j با اندازه $nm \times m$ تسهیم می‌شود و سپس تصویر مولد G متناظر با اندازه مشابه S، را انتخاب می‌کند (G) در چند بلوک غیراشتراکی G_i با اندازه $nm \times nm$، $1 \le j \le \lceil r/nm \rceil^2$ تسهیم می‌شود.

۲. در این قسمت تابع مولد $H(G_j, x_i)$ محاسبه می‌شود و مقادیر $H(G_j, x_i)$ در ماتریس v_{ji} همانند سهام‌داران شبه‌سایه با اندازه $nm \times m$ که $1 \le i \le n$ و $1 \le j \le \lceil r/nm \rceil^2$ باشد، تغییر می‌یابد.

۳. $U_j \times A_i = v_{ji} (\mathrm{mod}\ 251)$ به‌صورت روابط زیر درنظر گرفته می‌شود:

$$U_j \times [A_1, A_2, \dots, A_n] = [v_{j1}, v_{j2}, \dots, v_{jn}] (\mathrm{mod}\ 251) \quad (۱)$$

$$U_j = [v_{j1}, v_{j2}, \dots, v_{jn}] \times [A_1, A_2, \dots, A_n]^{-1} (\mathrm{mod}\ 251) \quad (۲)$$

سپس $U_j \times B_k$ محاسبه می‌شود $U_j \times B_k$، j امین بلوک از $U \times B_k$ بوده که $1 \le j \le \lceil r/nm \rceil^2$، $1 \le k \le n-t$.

۴. رابطه $S'_j = S_j \oplus U_j$ محاسبه می‌شود، که در آن S'_j، j ($1 \le j \le \lceil r/nm \rceil^2$) امین بلوک از تصاویر عمومی S' است.

۵. در رابطه $U \times B_k$ ، S' به‌عنوان تصویر عمومی و G که $1 \le k \le n-t$ به‌عنوان تصویر مولد، معرفی می‌شوند.

ج) فاز بازیابی تصویر راز

۱. با تولید تصویر G هر t سهام‌دار $(p_1, p_2, \dots, p_t)$ با ارائه تصویر سایه خود قادر است G_j را به‌دست آورده و $H(G_j, x_i)$ را محاسبه نماید و آن‌ها را در ماتریسی به‌فرم v_{ji}، که $1 \le i \le n$ و $1 \le j \le \lceil r/nm \rceil^2$ قرار دهد.

۲. با اطلاعات عمومی $U \times B_k$ سهام‌داران قادرند $U_j \times B_k$ را براساس معادله زیر به‌دست آورده:

$$U_j \times [A_1, \dots, A_t, B_1, \dots, B_t] = [v_{j1}, , \dots, v_{jt}, U_j \times B_1, \dots U_j \times B_{n-t}] (\mathrm{mod}\ 251) \quad (۳)$$

U_j به‌صورت زیر محاسبه نمایند.

$$U_j = [v_{j1}, , \dots, v_{jt}, U_j \times B_1, \dots U_j \times B_{n-t}] \times [A_1, \dots, A_t, B_1, \dots, B_t]^{-1} (\mathrm{mod}\ 251) \quad (۴-۱)$$

$$= [U_j \times A_1, \dots U_j \times A_j, U_j \times B_1, \dots U_j \times B_{n-t}] \times [A_1, \dots, A_t, B_1, \dots, B_{n-t}]^{-1} (\mathrm{mod}\ 251) = U_j$$

$1 \le j \le \lceil r/nm \rceil^2$ است.

۳. سپس سهام‌داران با همکاری یکدیگر S' را به S'_j تبدیل کرده و $S_j = S'_j \oplus U_j$ را محاسبه می‌نمایند و درنهایت S_j ها که $1 \le j \le \lceil r/nm \rceil^2$ برای ایجاد تصویر راز روی هم انباشته[2] می‌شوند.

د) تسهیم تصویر دیگر

هنگام تسهیم تصویر راز دیگر، لازم است مقسم، تصویر مولدی متفاوت از G را انتخاب نماید و فاز تسهیم تصویر راز را در زیر بخش (ب) تکرار کند. به‌طور مشابه سهام‌داران با همکاری یکدیگر قادرند تصویر راز را با تکرار مرحله بازیابی تصویر راز در زیر بخش (ج) به‌دست آورد.

مشاهده کردیم که هوژنگ‌فنگ و همکارش [۸] در اصلاح طرح خود، طرح چندرازی را معرفی کردند که می‌توانست به طور مستقل و بدون توزیع دوباره، سهم شوند و هر سهام‌دار به‌منظور بازسازی راز، سهم سایه‌ای را به‌جای سهم اصلی خود، دریافت و ارائه می‌کرد. مشاهده شد که بازسازی راز تحدیدی بر ابزارهای باقی‌مانده در بازیابی رازهای دیگر، که هنوز بازسازی نشده بودند، نبود.

۳- تابع مولد جدید

ما با تغییر و معرفی تابع مولد جدیدی در طرح هوژنگ‌فنگ و همکارش و اجرای این تابع در رمزنگاری مذکور دیدیم که بار دیگر برخی اطلاعات کلی در تولید تصاویر سایه‌ای به‌کار رفته است و نیز سهم‌های مخفی سهام‌داران هنگام بازیابی تصویر راز آشکار نمی‌شوند.

توابع لازم در معرفی تابع جدید به‌شرح ذیل می‌باشد [۹].

1- Full Rank

2 - Combine

الف- تابع Rowround

اگر $y=(y_0,y_1,y_2,y_3,\dots,y_{15})$ حلقه سطری

$(y)=(z_0,z_1,z_2,z_3,\dots,z_{15})$ باشد که

$$(z_0,z_1,z_2,z_3)=quarterround(y_0,y_1,y_2,y_3)$$
$$(z_5,z_6,z_7,z_4)=quarterround(y_5,y_6,y_7,y_4)$$
$$(z_{10},z_{11},z_8,z_9)=quarterround(y_{10},y_{11},y_8,y_9)$$
$$(z_{15},z_{12},z_{13},z_{14})=quarterround(y_{15},y_{12},y_{13},y_{14})$$

لذا می‌توان ورودی $(y_0,y_1,y_2,y_3,\dots,y_{15})$ را به‌عنوان ماتریس مربعی مشاهده کرد.

$$\begin{bmatrix} y_0 & y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 & y_7 \\ y_8 & y_9 & y_{10} & y_{11} \\ y_{12} & y_{13} & y_{14} & y_{15} \end{bmatrix}$$

در تابع دوران سطری، سطرهای ماتریس به‌طور موازی با جایگشت هر سطر داخل quarterround مرتب می‌شوند. در سطر اول تابع دوران سطری، در y_1 ، پس از آن y_2 و y_3 و سپس y_0 مرتب می‌گردد، در سطر دوم، تابع دوران سطری تابع y_6 ، بعد y_7 و y_4 و سپس y_5 را مرتب می‌نماید، در سطر سوم، تابع دوران سطری به ترتیب y_{11} ، سپس y_8 و y_9 و سپس y_{10} قرار می‌گیرد و در سطرچهارم نیز به ترتیب تابع دوران سطری y_{12} ، سپس y_{13} و y_{14}، سپس y_{15} قرار می‌گیرد.

ب- تابع Columnround

اگر $x=(x_0,x_1,x_2,x_3,\dots,x_{15})$ دوران ستونی $(x)=(y_0,y_1,y_2,y_3,\dots,y_{15})$ باشد لذا می‌توان ورودی $(x_0,x_1,x_2,x_3,\dots,x_{15})$ را به‌عنوان ماتریس مربعی ذیل مشاهده کرد.

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

تابع دوران ستونی، ستون‌های ماتریس را به‌طور موازی با حایگشت هر سطر داخل *quarterround* مرتب می‌کند. به‌طوری‌که در ستون اول به‌ترتیب، تابع دوران ستونی، y_4، y_8، سپس y_{12} و پس از آن y_0 قرار می‌گیرد، در ستون دوم نیز به‌ترتیب، تابع دوران ستونی y_9، سپس y_{13}، y_1 و پس از آن y_5قرار می‌گیرد، در ستون سوم، تابع دوران ستونی y_{14} ، سپس y_2 ، y_6 و سپس y_{10} مرتب می‌شود و در ستون چهارم تابع دوران ستونی y_3، سپس y_7 ، y_{11}، پس از آن y_{15} مرتب می‌گردد.

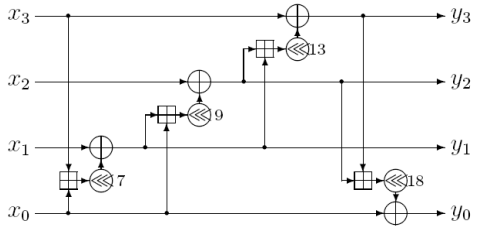
ورودی تابع $H_1(\mathrm{x})$ ۱۶ بیتی باشد آن‌گاه خروجی آن هم کلمه ۱۶ بیتی می‌باشد.

تابع رمزنگاری $H(G,x_i)$ یک زنجیر بلند شامل سه عملیات ساده بر کلمات ۳۲ بیتی است که در شکل (۱) نشان داده شده است.

جمع ۳۲ بیتی: $(a+b)mod\ 32$، a ، b هرکدام ۳۲ بیتی هستند.

Xor، ۳۲ بیتی: $a\ XOR\ b$، a ، b هرکدام ۳۲ بیتی می‌باشند.

چرخش با فاصله ثابت ۳۲ بیتی: $a <<< b$، کلمه ۳۲ بیتی a ، b بیت به‌سمت چپ شیفت دوری می‌یابد. B ثابت است. عملیات بالا توسط هر مداری به‌سادگی قابل ساخت و پیاده‌سازی است.



شکل (۱). تابع بین x و y در هسته تابع $H(G,x_i)$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = quarterround \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$\rightarrow \begin{cases} y_1 = x_1 \oplus \big((x_0 + x_3) \lll 7\big) \\ y_2 = x_2 \oplus \big((y_1 + x_0) \lll 9\big) \\ y_3 = x_3 \oplus \big((y_2 + y_1) \lll 13\big) \\ y_0 = x_0 \oplus \big((y_3 + y_2) \lll 18\big) \end{cases}$$

$$\begin{bmatrix} \mathrm{x}_0 & \mathrm{x}_1 & \mathrm{x}_2 & \mathrm{x}_3 \\ \mathrm{x}_4 & \mathrm{x}_5 & \mathrm{x}_6 & \mathrm{x}_7 \\ \mathrm{x}_8 & \mathrm{x}_9 & \mathrm{x}_{10} & \mathrm{x}_{11} \\ \mathrm{x}_{12} & \mathrm{x}_{13} & \mathrm{x}_{14} & \mathrm{x}_{15} \end{bmatrix}$$

$$\rightarrow \begin{cases} (\mathrm{y}_0,\mathrm{y}_1,\mathrm{y}_2,\mathrm{y}_3) = \mathrm{quarterround}(\mathrm{x}_0,\mathrm{x}_1,\mathrm{x}_2,\mathrm{x}_3) \\ (\mathrm{y}_5,\mathrm{y}_6,\mathrm{y}_7,\mathrm{y}_4) = \mathrm{quarterround}(\mathrm{x}_5,\mathrm{x}_6,\mathrm{x}_7,\mathrm{x}_4) \\ (\mathrm{y}_{10},\mathrm{y}_{11},\mathrm{y}_8,\mathrm{y}_9) = \mathrm{quarterround}(\mathrm{x}_{10},\mathrm{x}_{11},\mathrm{x}_8,\mathrm{x}_9) \\ (\mathrm{y}_{15},\mathrm{y}_{12},\mathrm{y}_{13},\mathrm{y}_{14}) = \mathrm{quarterround}(\mathrm{x}_{15},\mathrm{x}_{12},\mathrm{x}_{13},\mathrm{x}_{14}) \end{cases}$$

$$\begin{bmatrix} \mathrm{x}_0 & \mathrm{x}_1 & \mathrm{x}_2 & \mathrm{x}_3 \\ \mathrm{x}_4 & \mathrm{x}_5 & \mathrm{x}_6 & \mathrm{x}_7 \\ \mathrm{x}_8 & \mathrm{x}_9 & \mathrm{x}_{10} & \mathrm{x}_{11} \\ \mathrm{x}_{12} & \mathrm{x}_{13} & \mathrm{x}_{14} & \mathrm{x}_{15} \end{bmatrix}$$

$$\rightarrow \begin{cases} (\mathrm{y}_0,\mathrm{y}_4,\mathrm{y}_8,\mathrm{y}_{12}) = \mathrm{quarterround}(\mathrm{x}_0,\mathrm{x}_4,\mathrm{x}_8,\mathrm{x}_{12}) \\ (\mathrm{y}_5,\mathrm{y}_9,\mathrm{y}_{13},\mathrm{y}_1) = \mathrm{quarterround}(\mathrm{x}_5,\mathrm{x}_9,\mathrm{x}_{13},\mathrm{x}_1) \\ (\mathrm{y}_{10},\mathrm{y}_{14},\mathrm{y}_2,\mathrm{y}_6) = \mathrm{quarterround}(\mathrm{x}_{10},\mathrm{x}_{14},\mathrm{x}_2,\mathrm{x}_6) \\ (\mathrm{y}_{15},\mathrm{y}_3,\mathrm{y}_7,\mathrm{y}_{11}) = \mathrm{quarterround}(\mathrm{x}_{15},\mathrm{x}_3,\mathrm{x}_7,\mathrm{x}_{11}) \end{cases}$$

۴- ارائه طرح جدید بهبودیافته

با تغییر در تابع مولد و نحوه ساخت سهم‌های تصویر سایه در طرح هو ژنگ فنگ و گائو هانجون مشاهده می‌شود که اجرای تابع $\mathbf{H(G_j,x_i)}$ جدید در طرح جدید با حفظ کارآمدی

طرح، سرعت آن افزایش یافته است.

الف) مرحله آغازین

ابتدا تابع یک‌طرفه دو متغیره نوع خاصی از توابع درهم‌ساز H(G,X) را در نظر گرفتیم. سپس مقسم D، باید تعدادی از تصاویر راز را تقسیم نماید. مقسم مجموعه‌ای از n ماتریس $\{A_1, \dots, A_n\}$ در $GF(251)$ را به‌عنوان معین‌کننده عمومی سهام‌داران p_i تشکیل می‌دهد، سپس $n-t$، ماتریس $\{B_1, \dots, B_{n-t}\}$ در$GF(251)$ را به‌عنوان اطلاعات عمومی، در نظر می‌گیرد، بعد هر ماتریس $nm \times m$ می‌باشد. هر n از A_i مرتبه کامل دارد، هر t از A_i و هر $n-t$ ازB_k نیز دارای رتبه کامل است که $1 \le k \le n-t$,$1 \le i \le t$. D پس از آن، x_i را که $1 \le i \le n$، به‌عنوان سهم مخفی سهام‌داران p_i متناظر، انتخاب می‌کند.

ب) مرحله تسهیم تصویر راز

S تصویر راز با اندازه $r \times r$ بوده که D، آن را به‌صورت ذیل تسهیم می‌نماید.

۱- تصویر راز S در چند بلوک غیراشتراکی S_j با اندازه $nm \times m$ تسهیم می‌شود و سپس تصویر مولد متناظر که اندازه مشابه با S دارد، با استفاده از تابع $H(G,X) = [G + H_1(G)].x_i$ که درآن: $H_1(G) = \text{Doubleround}(G) = \text{rowround}(\text{columnround}(G))$، محاسبه می‌شود.

۲- با محاسبه $H(G_j, x_i)$ و تبدیل به ماتریس، v_{ji}، سهام‌دار P_i سهم شبه‌سایه با اندازه $nm \times m$ با $1 \le i \le n$ و $1 \le j \le \lceil r/nm \rceil^2$، که در آن:

$$U_j \times A_i = v_{ij} (\text{mod } 251)$$

به‌صورت روابط زیر برقرار است.

$$U_j \times [A_1, A_2, \dots, A_n] = [v_{j1}, v_{j2}, \dots, v_{jn}] (\text{mod } 251)$$
$$U_j = [v_{j1}, v_{j2}, \dots, v_{jn}] \times [A_1, A_2, \dots, A_n]^{-1} (\text{mod } 251)$$

و $U_j \times B_k$ محاسبه می‌شود ($U_j \times B_k$، j امین بلوک از $U \times B_k$ است که $1 \le k \le n-t$ ، $1 \le j \le \lceil r/nm \rceil^2$).

۳- $S'_j = S_j \oplus U_j$ محاسبه می‌گردد، که در آن S'_j، j امین بلوک از تصاویر عمومیS' است که $1 \le j \le \lceil r/nm \rceil^2$ روابط $U \times B_k$، تصویر عمومیS' و تصویر مولد G که $1 \le k \le n-t$ است، درنظر گرفته می‌شوند.

ج) فاز بازیابی تصویر راز

۱- با تولید تصویر G هر t سهام‌دار، $(p_1, p_2, \dots, p_t)$ می‌توانند G_j را به‌دست آورده و سپس تابع مولد $H(G_j, x_i)$ را محاسبه نمایند و آن‌ها را در ماتریس به‌فرم v_{ji}، که $1 \le i \le n$ و $1 \le j \le \lceil r/nm \rceil^2$ قرار دهند.

۲- از اطلاعات عمومی $U \times B_k$ سهام‌داران می‌توانند $U_j \times B_k$ را به‌دست آورند و U_j را به‌صورت زیر محاسبه می‌نمایند.

$$U_j \times [A_1, \dots, A_t, B_1, \dots, B_t] = [v_{j1}, , \dots, v_{jt}, U_j \times B_1, \dots U_j \times B_{n-t}] (\text{mod } 251)$$

$$T_1 = (v_{j1}, , \dots, v_{jt}, U_j \times B_1, \dots U_j \times B_{n-t}) \quad (۴)$$
$$T_2 = (A_1, \dots, A_t, B_1, \dots, B_{n-t})$$

پارامترهایی که در اختیار سهام‌داران قرار می‌گیرند.

$$U_j = (T_1 \times T_2^{-1}) (\text{mod } 251)$$
$$U_j = [v_{j1}, , \dots, v_{jt}, U_j \times B_1, \dots U_j \times B_{n-t}] \times [A_1, \dots, A_t, B_1, \dots, B_{n-t}]^{-1} (\text{mod } 251)$$
$$= [U_j \times A_1, \dots U_j \times A_{n-t}, U_j \times B_1, \dots U_j \times B_{n-t}] \times [A_1, \dots, A_t, B_1, \dots, B_{n-t}]^{-1} (\text{mod } 251)$$

$1 \le j \le \lceil r/nm \rceil^2$ است.

$$U_j \times B_l = v_t \qquad l = 1,2, \dots, n-t$$

۱- سهام‌داران تصویر عمومی S' را به S'_jها تقسیم کرده و $S_j = S'_j \oplus U_j$ را محاسبه می‌نمایند و سپس با انباشتن S_jها تصویر راز آشکار می‌شود. که در آن $1 \le j \le \lceil r/nm \rceil^2$ است.

د)تسهیم تصویر دیگر

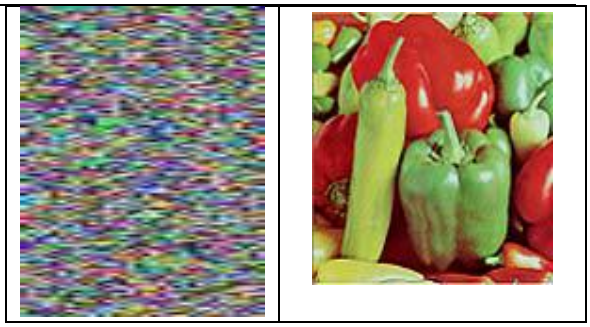
هنگام تسهیم تصویر دیگر، مقسم تنها نیار دارد، تصویر مولدی متفاوت از G را انتخاب نموده و فاز تسهیم تصویر راز را در زیربخش (ب) تکرار کند. به‌طور مشابه سهام‌داران با همکاری یک‌دیگر قادرند تصویر را با تکرار مرحله بازیابی تصویر راز در زیربخش (ج) به‌دست آورد.

مثال

در این مثال تصویر فلفل‌ها به‌عنوان تصویر راز در شکل (۲) در نظر گرفته شده است.

اگر A_i (i=1, 2, 3, 4) ماتریس معین‌کننده عمومی‌سهام‌داران باشند:

$$A_1 = \begin{bmatrix} 1 \\ 2 \\ 5 \\ 12 \end{bmatrix}, \ A_2 = \begin{bmatrix} 2 \\ 3 \\ 8 \\ 12 \end{bmatrix}, \ A_3 = \begin{bmatrix} 3 \\ 4 \\ 9 \\ 18 \end{bmatrix}, \ A_4 = \begin{bmatrix} 7 \\ 9 \\ 22 \\ 5 \end{bmatrix}$$



(الف) (ب)

شکل (۲) الف) تصویر راز با اندازه ۱۲۸×۱۲۸

ب) تصویر راز عمومی S' با اندازه ۱۲۸×۱۲۸

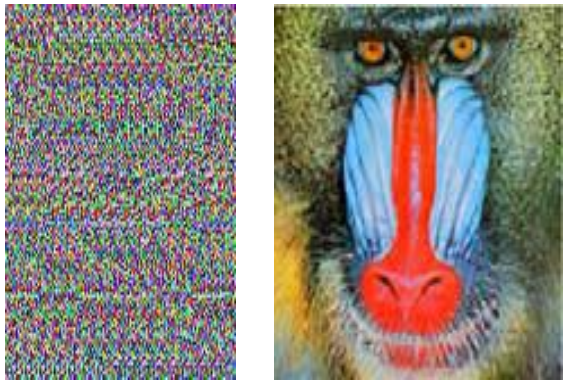
B_k $(k = 1,2)$ ماتریس معرف اطلاعات عمومی باشند:

$$B_1 = \begin{bmatrix} 6 \\ 7 \\ 21 \\ 11 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 8 \\ 11 \\ 20 \\ 17 \end{bmatrix}$$

اگر $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$ تصویر راز سهام‌داران x_i $(i = 1,2,3,4)$ باشند و با فرض این‌که ماتریس تصویر راز S و ماتریس تصویر مولد G به‌صورت زیر باشند:

$$G = \begin{bmatrix} 11 & 21 & 111 & 1 \\ 12 & 22 & 112 & 111 \\ 15 & 25 & 221 & 175 \\ 16 & 26 & 222 & 201 \end{bmatrix} \quad S = \begin{bmatrix} 255 & 248 & 210 & 175 \\ 255 & 235 & 170 & 172 \\ 255 & 212 & 178 & 183 \\ 255 & 196 & 176 & 171 \end{bmatrix}.$$

تصویر مولد G و راز S در شکل (۳) مشاهده می‌شود.



(الف) (ب)

شکل (۳) الف) تصویر عمومی G با اندازه ۱۲۸×۱۲۸

ب) اطلاعات عمومی $U \times B_1$ و $U \times B_2$ با اندازه ۱۳۲ × ۱۲۸

با استفاده از رابطه زیر

$$U_j \times [A_1, \dots, A_t, B_1, \dots, B_t] = [v_{j1}, , \dots, v_{jt}, U_j \times B_1, \dots U_j \times B_{n-t}] (\text{mod } 251)$$

مقادیر $U \times B_1$ و $U \times B_2$ محاسبه می‌شوند.

با توجه به روابط شرح داده شده در بخش ۳ و به دلیل جایگشت‌های سطری و ستونی پی‌درپی، کلیه محاسبات با استفاده از نرم‌افزار MATLAB محاسبه و سپس اجرا گردیده است (پیوست ۱).

۵- تحلیل و مقایسه این طرح با چند طرح دیگر

طرح تسهیم راز بصری بهبودیافته در این مقاله را با چند طرح دیگر که مبتنی بر ماتریس بولی (دودویی) هستند مورد مقایسه قرار می‌دهیم. نتایج مقایسه در جدول (۱) در زیر آمده و مشاهده می‌شود که در این طرح‌ها بسط پیکسل ناچیز و پیچیدگی در محاسبات، طرح وانگ و همکارانش $1/n \times 1$، طرح مارتین دل‌ری و آویلا[1] [۱۰] $8N^2$، طرح چن و وو[2] $n/(n+1) \times 1$ [۱۱] و در طرح وانگ و چنگ[3] [۱۲] به‌دلیل داشتن محاسبات ساده جایگشتی پیچیدگی آن $O(\frac{(n+1)!}{(n-1)!})$ است. طرح بهبودیافته به‌دلیل استفاده از توابع سالسا دارای پیچیدگی تقریبی 2^{255} [۱۳] می‌باشد. پیچیدگی طرح هوزنگ‌فنگ و همکارش به‌دلیل نامشخص‌بودن تابع مولدش به‌طور کامل قابل محاسبه نمی‌باشد.

۵-۱- تحلیل طرح بهبودیافته

در این مقاله با بررسی طرح هوژنگ‌فنگ و همکارش و معرفی یک تابع مولد جدید از جایگشت‌ها، که از مسایل سخت ریاضی می‌باشد، توانستیم در سرعت طرح قبل بهبود ایجاد نماییم. از آنجایی‌که از نظر محاسبه تابع مولد طرح هوژتگ‌فنگ و همکارش تابع چکیده‌ساز کلی و نامشخص بود لذا، طرح جدید بهبودیافته در مقایسه با طرح اولیه از نظر امنیت، کارایی و بنا بر احاطه بر مفاهیم محاسباتی برتری آن مشهود است. در انتها طرح بهبودیافته را با چند طرح دیگر از منظر شکل تصویر، لزوم کتاب کد، بسط پیکسل، کیفیت بازیابی تصویر، قابلیت بازبینی و مرتبه پیچیدگی مقایسه نموده که نتایج آن در جدول (۱) آمده است.

اجرای طرح اصلاحی با برنامه‌نویسی در محیط متلب توسط رایانه از نوع 520M-2.4Hz-Core i5 صورت گرفته است. حافظه Ram کم‌تر از $1/100$ گیگابایت، ۱۰ مگابایت، Cpuusag ۱۳٪ در بازه زمانی اجرای محاسبات حافظه را درگیر کرده است. زمان کل انجام محاسبات طرح اصلاحی ۰/۱۸۶ ثانیه می‌باشد. مشاهده می‌شود که سرعت زمان اجرای طرح

1 - Martin Delrey and Avila
2 - Chang and Wu
3 - Wang and Chang

اصلاح‌شده مناسب و مطلوب است.

جدول (۱). مقایسه طرح جدید با چند طرح تسهیم راز دیگر

طرح‌ها / ویژگی	وانگ و همکاران	مارتین دل ری و همکارش	زی هویی وانگ و همکارانش	چن و وو	هو ژنگ فنگ و همکارش	طرح جدید [۱۵]
شکل تصویر	سطح خاکستری دودویی	تصویر راز بصری دودویی	سطح خاکستری دودویی	سطح خاکستری دودویی	تصویر راز بصری دودویی	تصویر راز بصری دودویی
لزوم کتاب کد	خیر	خیر	خیر	خیر	خیر	خیر
بسط پیکسل	خیر	خیر	خیر	خیر	خیر	خیر
کیفیت بازیابی تصویر	بی کم و کاست	بی‌کم و کاست	بی کم و کاست	بی کم و کاست	بی‌کم و کاست	بی‌کم و کاست
قابلیت بازبینی	ندارد	ندارد	دارد	ندارد	ندارد	ندارد
مرتبه پیچیدگی	$1/n \times 1$	$8N^2$	$O(\frac{(n+1)!}{(n-1)!})$	$n/(n+1) \times 1$		2^{255}
منابع	[۱۴]	[۱۰]	[۱۲]	[۱۱]	[۸]	[۱۳]

۶- نتیجه‌گیری

در طرح هوژنگ‌فنگ و همکارش دیدیم که هنگام تسهیم تصاویر راز گوناگون، برای هر تصویر راز، تنها نیاز است مقسم (D)، تصویر مولد جدیدی را انتخاب نموده و مراحل تسهیم تصویر راز را تکرار نماید. در الگوی این طرح سهام‌داران تنها نیاز دارند به‌جای آشکارکردن سهم راز خود یعنی (x)، در تصویر شبه‌سایه ائتلاف نمایند بدین‌ترتیب سهم راز هر سهام‌دار چندین‌بار قابل استفاده است. ما برای بهبود طرح هوژنگ‌فنگ و همکارش تابع مولد را به‌کار بردیم که تابعی چکیده‌ساز یک‌طرفه دومتغیره مبتنی بر مسأله سخت ریاضی بوده و بر اساس دوران سطری، ستونی و جایگشت و تابع Doubleround(x) استوار است. مشهود است که از نظر تحلیلی و سرعت محاسبات طرح بهبودیافته ما نسبت به طرح اولیه کارآمدتر و دارای امنیت بالا با پیچیدگی مطلوب می‌باشد.

۷- مراجع

[1] A. Shamir, "How to Share a Secret," Journal of Communication, ACM, vol. 24, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding Cryptographic Keys[C]," Proc. of AFIPS 1979 National Computer Conference, pp. 313-317, 1979.

[3] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On Sharing Secret Systems[J]," IEEE Transactions on Information Theory, vol. 29, no. 1, pp. 35-41, 1983.

[4] M. Naor and A. Shamir, "Visual Cryptography[C]," Advances in Cryptology-Eurocrypt, vol. 94, pp. 1-12, 1994.

[5] M. Naor and A. Shamir, "Visual Cryptography II: Improving the Contras Via the Cover Base[C]," Lecture Notes in Computer Science, Springer Berlin vol. 1189, pp. 197-202, 1997.

[6] H. Zheng Feng and G. Hanjun, "A Compressible Threshold Image Sharing Scheme Based on Matrix Multiplication[J]," Geomatics and Information Science of Wuhan University, vol. 33, no. 10, pp. 1003-1006, 2008.

[7] Ch. Chin-Chen, L. Chia-Chen, L. Chia-Hsuan, and Ch. Yi-Hui, "A Novel Secret Image Sharing Scheme in Color Images Using Small Shadow Images [J]," Information Sciences, vol. 178, pp. 2433–2447, 2008.

[8] H. Zheng Feng and G. Hanjun, "Multi Secret Image Sharing Based on Matrix Multiplication," IEEE International Conference on Networks Security, vol. 1, pp. 184-187, 2009.

[9] D. J. Bernstein, "Salsa 20 Specification," Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, 2007.

[10] A. Martin, D. Rey, and D. Avila, "A Matrix-Based Secret Sharing Scheme for Images," Lecture Notes in Computer Science, vol. 5197, PP. 235-242, 2008.

[11] T.-H. Chen, C-S Wu, and W. Chang, "Efficient Multi-Secret Image Sharing Based on Boolean Operations," Department of Computer Science and Information Engineering, National Chiayi University, 300 University Rd., Chia-Yi City, Taiwan 600, 2011.

[12] Z. H. Wang, Ch. Ch. Chang, H. Ngoc Tu, and M. Ch. Li, "Sharing a Secret Image in Binary Images with Verification," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 1, 2011.

[13] J. Daniel, "Bernstein The Salsa20 Family of Stream Ciphers," Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, IL 60607–7045.

[14] D. Wang, L. Zhang, N. Ma, and X. Li, "Two Secret Sharing Schemes Based on Boolean Operations," vol. 40, no. 10, pp. 2776–2785, 2007.

[15] F. Sheikh Sangtajan and M. Hadyan Dehkordi, "Analysis of several Visual Secret Sharing Schemes and Improvement One of Them," Ph.D. Thesis, Imam Hussein University, Sep. 2013.

پیوست

```
clc
close all
clear all

S                          =
uint8([255 248 210 172; 255 235 170
172;255 212 178 183; 255 196 176
171])
G                          = uint8([11
21 11 1; 12 22 112 111;15 25 221
175; 16 26 222 201])  %

y0                         = G(1,:)
y1                         = G(2,:)
y2                         = G(3,:)
y3                         = G(4,:)

z1                         =
bitxor(y1, (y0+y2))- uint8(7)
z2                         =
bitxor(y2, (z1+y0))- uint8(9)
z3                         =
bitxor(y3, (z2+z1))- uint8(13)
z0                         =
bitxor(y0, (z2+z3))- uint8(18)
%
Z                          = [z0; z1 ;
z2 ; z3 ]
%
y0                         = Z(:,1)
y1                         = Z(:,2)
y2                         = Z(:,3)
y3                         = Z(:,4)
%
z1                         =
bitxor(y1, (y0+y2))- uint8(7)
z2                         =
bitxor(y2, (z1+y0))- uint8(9)
z3                         =
bitxor(y3, (z2+z1))- uint8(13)
z0                         =
bitxor(y0, (z2+z3))- uint8(18)
% %
double_round_G             = [z0 z1 z2
z3]
% %
x                          =
uint8(eye(4))
% %
H_G_x1                     =
double(G+double_round_G)*double(x)
H_G_x                      =
mod(H_G_x1,251) %
% %


A1                         = [ 1 2 5
12]'
A2                         = [ 2 3 8
15]'
A3                         = [ 3 4 9
18]'
A4                         = [ 7 9 22
5]'
A                          = [A1 A2 A3
A4]
A_inv                      = inv(A)

B1                         = [6 7 21
11]'
B2                         = [8 11 20
17]'
%
v1                         =
H_G_x(:,1)  %% barai bazyabi
estefadeh mishavad
v2                         =
H_G_x(:,2)
v3                         =
H_G_x(:,3)
v4                         =
H_G_x(:,4)
%
U                          = [ v1  v2
v3  v4]* A_inv
U                          =
uint8(ceil(mod(U,251)))
```

```
% % double_round_G          = [z0
z1 z2 z3]
% %
% % y0                      =
double_round_G(1,:)
% % y1                      =
double_round_G(2,:)
% % y2                      =
double_round_G(3,:)
% % y3                      =
double_round_G(4,:)
% % double_column_G         = [y0;
y1 ; y2 ; y3 ]
% % H_G_x1                  =
double(G+double_column_G)*double(x)
% % H_G_x                   =
mod(H_G_x1,251)
% %
% % v1                      =
H_G_x(:,1)
% % v2                      =
H_G_x(:,2)
%
```

```
U_rnsh                    =
uint8(mod(U,251))     %% barai
bazyabi estefadeh mishavad

S1                        =
bitxor(S, U)      %

U_B1                      =
mod(double(U)*B1,251)  %
U_B2                      =
mod(double(U)*B2,251)  %

%% secret
G                         = uint8([11
21 11 1; 12 22 112 111;15 25 221
175; 16 26 222 201])  %
% % y0                          =
G(:,1)
% % y1                          =
G(:,2)
% % y2                          =
G(:,3)
% % y3                          =
G(:,4)
% %
% % z1                          =
bitxor(y1, (y0+y2))- uint8(7)
% % z2                          =
bitxor(y2, (z1+y0))- uint8(9)
% % z3                          =
bitxor(y3, (z2+z1))- uint8(13)
% % z0                          =
bitxor(y0, (z2+z3))- uint8(18)
```

An Efficient Visual Multi-Secret Sharing Scheme

A. R. Mirghadri*, F. Sheikh Sangtajan

*Imam Hossein University

(Received: 03/06/2014, Accepted: 12/01/2016)

ABSTRACT

Protecting valuable data along the Cyber Security is the one of the strategic issues of cyber defense. The secret sharing scheme is an attractive branch of advanced cryptography that has extremely important role in cyber defense and for the preservation of documents and confidential information against threats such as robbery and unauthorized accesses.In the secret sharing schemes, for increasing security shareholders present a shadow image instead of the genuine share while they are recovering secret images. Thus each share-holder is able to share several images with others by having only one portion of image.

In this paper, we define and design a new generating function that by replacing with the Hou Zheng Feng and et.al's generating function, can improved it. Since the new generating function is one-way and hard problem, hence increased the security of improved scheme. Also, with implementation and performing the new scheme again, our revised scheme will be more efficient respect to previous scheme according to the analysis and speed of computations.

Keywords: Secret image, Generating Function, Visual Multiple-Secret Sharing Scheme, Shadow Image, Doubleround(x) Function.

* Corresponding Author Email: amrghadri@ihu.ac.ir