نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دهم، شماره ۳، پاییز ۱۳۹۸؛ ص ۳۰۶-۲۹۷

یک روش جدید رمزنگاری بصری مبتنی بر الگوریتم‌های فراابتکاری

آرا زارع[۱]، علی آقاگل‌زاده[۲]، سید جواد کاظمی‌تبار[۳*]

۱- کارشناسی ارشد، ۲- استاد، ۳- استادیار، دانشگاه صنعتی نوشیروانی بابل

(دریافت: ۹۷/۰۲/۰۳، پذیرش: ۹۷/۰۸/۳۰)

چکیده

یکی از شاخه‌های نوین رمزنگاری تصویر، رمزنگاری بصری است. رمزنگاری بصری تبدیل یک تصویر به دو یا چند تصویر نویزی شکل است به‌طوری‌که تصویرهای تولیدشده به‌تنهایی دارای اطلاعات خاصی نیستند اما اگر چاپ‌شده و برهم‌گذاشته شوند، نمایه‌ای قابل‌فهم از تصویر اصلی را تولید می‌کنند. خاصیت اصلی این روش عدم نیاز به داشتن دانشی در زمینه رمز برای بازیابی تصویر است و عملیات رمزگشایی توسط سیستم بینایی انسان انجام می‌پذیرد. در این مقاله یک روش رمزنگاری بصری بر مبنای الگوریتم اجتماع ذرات ارائه شده است. بدین ترتیب که ماتریس‌های پایه با استفاده از این الگوریتم به دست آمده و سپس از آن‌ها برای رمزنگاری استفاده می‌شود. در مقالات پیشین این نوع رمزنگاری با استفاده از الگوریتم ژنتیک مطرح شده بود. ما در این مقاله ضمن رفع ایراد الگوریتم طرح‌شده در برخی منابع مبنی بر منفی شدن کنتراست تصاویر در برخی حالات، الگوریتمی برای دستیابی به جواب بهینه از بین چندین جواب حاصل از آن الگوریتم پیشنهاد می‌کنیم. نتایج نشان می‌دهند که الگوریتم طرح‌شده ضمن کاهش میانگین تعداد عملیات لازم برای رسیدن به جواب بهینه، کنتراست را در حالت‌های مختلف افزایش می‌دهد. علاوه بر این، روش پیشنهادی می‌تواند به‌صورت جامع برای حالات مختلف رمزنگاری بصری آستانه‌ای مورد استفاده قرار گیرد.

کلیدواژه‌ها: رمزنگاری بصری، ماتریس‌های پایه، کنتراست، الگوریتم اجتماع ذرات

A Novel Metaheuristic Based Visual Cryptography

A. Zare, A. Aghagolzadeh, J. Kazemitabar*
Babol Noshirvani University of Technology
(Received: 23/04/2018; Accepted: 21/11/2018)

Abstract

Visual cryptography is one of the newest techniques is image encryption. Visual cryptography encrypts visual information and generates two or more shares which contain no information separately, but reveal the secret when superposed. The main advantage of this scheme is that the decoding process does not need any knowledge of cryptography and human visual system is able to decrypt the secret message. In this article, a new encryption method based on particle swarm optimization is provided. The basis matrices are obtained using this approach and then used for encryption. In previous work, a Genetic Algorithm based method was proposed. In our work we fix a subtle yet crucial bug in the GA based method which is generating pictures with negative contrast in some cases and propose a simpler alternative. Simulation results show that the proposed method meets all the initial conditions of visual cryptography while decreasing the number of function evaluations and can provide a contrast enhancement. Moreover, the proposed method has the advantage of being generic and can be used in various threshold based visual cryptography.

Keywords: Visual Cryptography, Basis Matrices, Contrast, Particle Swarm Optimization

*Corresponding Author E-mail: j.kazemitabar@nit.ac.ir

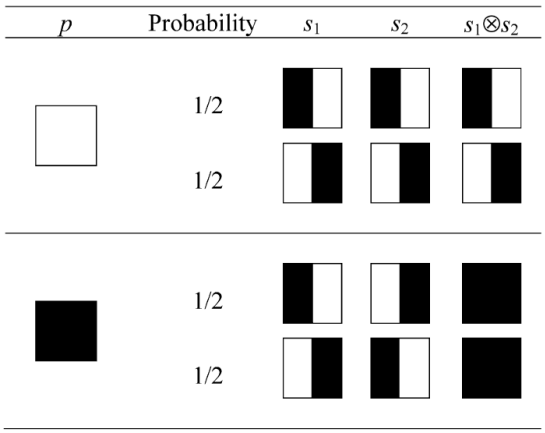
۱. مقدمه

رمزنگاری بصری در طول سال‌های اخیر پیشرفت فراوانی کرده است. در این روش، رمزگشایی کامل یک محتوای دیجیتال تنها با قدرت بینایی انسان صورت می‌گیرد؛ بدین‌صورت که پیام به دو سهم نویزی شکل رمز می‌شود، بنابراین، هرکدام از این سهم‌ها اطلاعاتی درباره پیام به شخص نمی‌دهند. درصورتی‌که این سهم‌ها بر روی صفحات شفاف چاپ شوند و به‌درستی روی هم قرار گیرند، پیام رمز آشکار می‌شود. این ویژگی این اطمینان را می‌دهد که پردازش امن، توسط کسی که هیچ‌گونه اطلاعات قبلی از رمزنگاری بصری، برنامه‌نویسی یا تجربه تحلیل رمز ندارد، صورت گیرد. رمزنگاری بصری برای اولین بار در سال ۱۹۹۴ در نشست EuroCrypt مطرح شد [۱]. در نشست یادشده، روش رمزنگاری جدیدی که توسط آن بتوان تصاویر مشکی و سفید را به اشتراک‌های متعددی تقسیم کرد، ارائه گشت. برای رمزگشایی تصویر رمز باید اشتراک‌های ایجادشده را روی صفحات شفاف چاپ کرد و بر روی هم قرار داد. از سال ۱۹۹۴ مقاله‌های زیادی در مورد گسترش انواع رمزنگاری بصری ارائه شده است و تا امروز تحقیقات برای این روش از رمزنگاری همچنان ادامه دارد. تاکنون مقاله‌های زیادی شامل مباحث وضوح تصویر، گسترش مدل‌های رمزنگاری و آستانه‌گذاری برای رمز کردن منتشر شده است [۳-۲]. از طرف دیگر، با استفاده از الگوریتم تبرید شبیه‌سازی شده، رمزنگاری بصری تصاویر انجام شده است [۴]. در مرجع مزبور علاوه بر کنتراست، تاریکی تصویر نیز به‌عنوان یک معیار تکامل انتخاب شده است. به‌علاوه سعی شده کنتراست با راحت‌تر کردن شرایط تعادل چگالی بهبود یابد. در [۵] با در نظر گرفتن تعدادی بردار ستونی به‌جای روش معمول برای رمزگذاری پیکسل‌ها استفاده شده تا از توسعه پیکسلی جلوگیری شود. در مرجع مزبور نیز از تبرید شبیه‌سازی‌شده برای حل مسئله بهینه‌سازی استفاده شده است. روشی مبتنی بر الگوریتم ژنتیک برای رمزنگاری بصری ارائه شده است [۷-۶]. به نظر می‌رسد این روش دارای ایراداتی است که در صورت برطرف شدن به بهبود کارایی خواهد انجامید. در این مقاله ضمن رفع ایراد الگوریتم طرح‌شده، الگوریتمی جهت دستیابی به جواب بهینه از بین چندین جواب حاصل از الگوریتم قبلی پیشنهاد می‌کنیم. باقی مطالب مقاله به شرح زیر است. در بخش دوم به توضیح مختصر مفاهیم رمزنگاری بصری خواهیم پرداخت. در بخش سوم روش مبتنی بر الگوریتم ژنتیک را توضیح می‌دهیم و عیب آن را معرفی می‌کنیم. سپس با رفع عیب مذکور، روشی مبتنی بر اجتماع ذرات پیشنهاد خواهیم داد. به‌علاوه خروجی دو الگوریتم را بر اساس شبیه‌سازی باهم مقایسه می‌کنیم. در بخش چهارم و پایانی این مقاله نتایج شبیه‌سازی به اختصار آورده شده و نتایج مقاله مرور می‌شود.

ایده اصلی این روش از رمزنگاری برای اشتراک یک پیکسل p از تصویر باینری S در دو سهم SC_1 و SC_2 در شکل (۱) نشان داده شده است. برای تولید این دو سهم، اگر پیکسل p سفید باشد یکی از دو سطر اول جدول و اگر پیکسل p مشکی باشد یکی از دو سطر دوم انتخاب می‌شود. احتمال انتخاب سطر اول یا دوم مستقل از مقدار p و برابر با یکدیگر است. درنتیجه SC_1 و SC_2 هیچ‌گونه اطلاعاتی از پیکسل p در تصویر اصلی نمی‌دهند.

هنگامی‌که این دو سهم روی هم قرار گیرند (این امر معادل با اعمال عملگر منطقی OR است)، اگر پیکسل p در تصویر اصلی مشکی باشد، پیکسل معادل با آن در تصویر حاصل SC معادل با یک بلوک دوپیکسلی شامل دو پیکسل مشکی است و اگر p سفید باشد به‌صورت یک بلوک دوپیکسلی با یک پیکسل سفید و یک پیکسل مشکی دیده خواهد شد. درنتیجه بازیابی پیکسل مشکی با ضریب یک و پیکسل سفید با ضریب نیم صورت می‌گیرد. در این روش ۵۰٪ از شفافیت تصویر اصلی از دست خواهد رفت ولی تصویر اصلی قابل‌شناسایی می‌ماند.

به‌عنوان‌مثال، ستون S_1 در شکل (۱) یک پیکسل نیست بلکه بلوک پیکسلی توسعه‌یافته است. تعداد پیکسل‌ها در هر بلوک توسعه‌یافته، توسعه پیکسلی نامیده می‌شود که در طرح اولیه برابر با دو در نظر گرفته شده است.



شکل ۱. طرح اولیه برای رمزنگاری یک پیکسل به دو سهم [۱]

در روش کلی ارائه‌شده طی یکی از گزارش‌ها [۱]، یک تصویر به n سهم شکسته می‌شود و تنها در شرایطی تصویر اصلی قابل بازیابی است که حداقل به تعداد k ($k \le n$) از n اشتراک رمز

وجود داشته باشند (طرح تسهیم رمز آستانه‌ای (k,n)) و حتی با در اختیار داشتن k-1 اشتراک از صفحات رمز هیچ‌گونه اطلاعاتی از تصویر اصلی نمایش داده نشود. هرکدام از اشتراک‌های رمز، روی صفحات شفاف به‌صورت توزیعی از پیکسل‌ها چاپ می‌شوند و زمانی که تمام اشتراک‌ها روی هم قرار گیرند، تصویر اصلی ظاهر خواهد شد. در یک دیدگاه ساده، این روش معادل با روش OTP[1] در رمزنگاری است؛ که یکی از اشتراک‌های رمز به‌عنوان کلید[2] تعریف می‌شود و اشتراک دیگر نقش متن رمز[3] را بازی خواهد کرد، بنابراین، امنیت لازم را دارا است. (در رمزنگاری ثابت می‌شود که روش OTP واجد معیارهای امنیت با عنوان محرمانگی کامل است که توسط شانون تعریف و اثبات شد.)

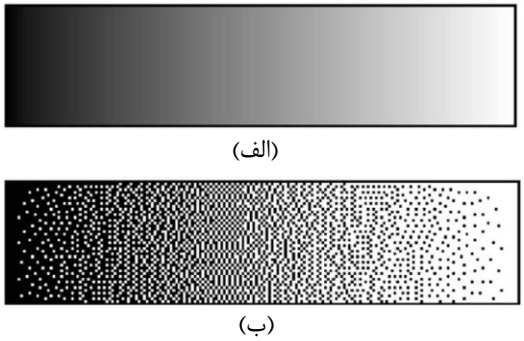
در واقع در این روش، هر پیکسل اصلی در n سهم کد می‌شود که هر سهم شامل m پیکسل مشکی و سفید است که به آن‌ها زیرپیکسل[4] می‌گویند. در این حالت از دو ماتریس بولین پایه n*m استفاده می‌شود: یک ماتریس پایه برای پیکسل‌های سفید(B_0) و یک ماتریس پایه برای پیکسل‌های سیاه(B_1). حال فرض کنید C_0 مجموعه‌ای شامل تمام جایگشت‌های ستونی ماتریس B_0 و C_1 مجموعه‌ای شامل تمام جایگشت‌های ستونی ماتریس B_1 باشد. برای کدگذاری یک پیکسل سفید ($p = 0$) یکی از ماتریس‌های موجود در C_0 و برای کدگذاری یک پیکسل سیاه ($p = 1$) یکی از ماتریس‌های موجود در C_1 به‌صورت کاملاً تصادفی انتخاب می‌شوند. سپس از هر سطر از ماتریس انتخاب‌شده برای تعیین رنگ m پیکسل برای n سهم استفاده می‌گردد.

معیارهای سنجش: معیارهای مختلفی برای تعیین عملکرد روش‌های ارائه‌شده در این زمینه وجود دارد که از جمله مهم‌ترین آن‌ها می‌توان به نرخ توسعه پیکسل، کنتراست و امنیت اشاره نمود. شایسته است پیش از توصیف بیشتر موضوع، ابتدا به معرفی این سه عامل مهم در سنجش عملکرد روش رمزنگاری بصری بپردازیم.

نرخ توسعه پیکسل: نرخ توسعه پیکسل بیانگر تعداد زیرپیکسل هایی است که هر یک از پیکسل های تصویر اصلی در هر سهم به آن میزان رمز می‌شوند. در روش‌های اولیه رمزنگاری بصری هر پیکسل به m ($m \geq 1$) زیرپیکسل شکسته می‌شود. بنابراین، اندازه سهم‌های ایجادشده m برابر تصویر اصلی خواهد بود. با توجه به وجود محدودیت در پهنای باند و فضای ذخیره‌سازی، نرخ توسعه پیکسل معیار بسیار مهمی برای تعیین عملکرد یک روش است [۸].

- **کنتراست:** کنتراست تا حدی اختلاف بین پیکسل‌های سیاه و سفید تصویر رمزگشایی‌شده را نشان می‌دهد و به‌نوعی بیانگر وضوح تصویر ازنظر سیستم بینایی انسان است. بنابراین، از عوامل مهم و قابل‌توجه در این زمینه است.

برای کاهش تلفات در کنتراست، طرح‌های جدیدی با استفاده از نیم‌تن‌سازی دیجیتالی برای تصاویر خاکستری و رنگی ارائه شد که همان‌طور که در شکل (۲) قابل مشاهده است در این روش‌ها تصاویر با تن‌های پیوسته به‌صورت تصاویر باینری در نظر گرفته می‌شوند. در واقع تغییر اندازه نقاط و فاصله بین آن‌ها سبب ایجاد خطای دیداری می‌شود که منجر به دیده شدن تصویر به‌صورت تن‌های پیوسته می‌گردد. ازآنجایی‌که نیم‌تن‌سازی دیجیتالی یک فرآیند حاوی تلفات است، بازیابی کامل تصویر رمز ممکن نخواهد بود [۹-۱۰].



(الف)

(ب)

شکل ۲. تبدیل تصویر با تن پیوسته به تصویر باینری [۵] (الف) تصویر با تن پیوسته، (ب) تصویر نیم‌تن

با توجه به این نکته که برهم گذاشتن دو سهم را معادل با اعمال عملگر OR بر روی پیکسل‌ها در نظر می‌گیرند، پیکسل سفید را با مقدار صفر و پیکسل مشکی را با مقدار یک نشان می‌دهند. از طرفی میزان انتقال نور برای یک پیکسل سفید برابر با یک و برای پیکسل سیاه برابر با صفر است که به‌صورت زیر نمایش داده می‌شود:

$$T(S) = \begin{cases} 1, S = 0 \\ 0, S = 1 \end{cases} \quad (۱)$$

انتقال نور برای یک تصویر به‌صورت میانگین تعریف می‌شود. بدین ترتیب که اگر تصویر باینری S اندازه‌ای برابر با M×N

[1] One Time Pad
[2] Pad
[3] Ciphertext
[4] Subpixel

داشته باشد، خواهیم داشت:

$$T(S) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} T(S(i,j))}{M \times N} \quad (۲)$$

درنهایت کنتراست تصویر بازیابی‌شده به‌صورت زیر تعریف می‌شود:

$$\alpha = \frac{T(B[A(0)]) - T(B[A(1)])}{1 + T(B[A(1)]} \quad (۳)$$

A و B به ترتیب بیانگر تصویر اصلی رمز و تصویر بازیابی‌شده حاصل از برهم‌گذاری بیش از k سهم هستند. اگر کنتراست تصویر حاصل از برهم‌گذاری بیشتر از k سهم، مقداری بزرگ‌تر از صفر داشته باشد یا به عبارتی $T(B[A(0)]) > T(B[A(1)])$، تصویر بازیابی‌شده به‌صورت بصری قابل‌شناسایی خواهد بود.

امنیت: سهم‌های ایجادشده باید به نوعی باشند که هیچ‌گونه اطلاعاتی از تصویر اصلی را به نمایش نگذارند. در رمزنگاری (k, n)-VCS[1] سهم‌ها باید به‌گونه‌ای ایجاد شوند که تنها با در دست داشتن k تعداد و یا بیشتر از آن‌ها بتوان تصویر اصلی را بازیابی کرد و با داشتن تعدادی کمتر از k سهم، نباید هیچ‌گونه اثری از تصویر اصلی را در خود داشته باشد.

در واقع اگر میزان کنتراست حاصل از برهم‌گذاری کمتر از k سهم برابر با صفر باشد یا به‌عبارت‌دیگر $T(B[A(0)]) = T(B[A(1)])$، شرط امنیت رعایت می‌شود و تصویر حاصل نویزی شکل خواهد بود. در اینجا B بیانگر تصویر بازیابی‌شده حاصل از برهم‌گذاری کمتر از k سهم است.

برای افزایش امنیت در این روش، استفاده از سهم‌های معنی‌دار نیز بسیار مفید خواهد بود [۱]. با استفاده از سهم‌های بامعنی می‌توان وجود اطلاعات مخفی را پنهان کرد و درنتیجه نسبت به سهم‌های نویزی شکل، کمتر توجه هکرها را جلب می‌کنند. سهم‌های ایجادشده در حین بامعنی بودن، نباید اثری از تصویر اصلی را در اختیار بگذارند [۱۴-۱۳].

۳. تحلیل نقاط ضعف الگوریتم‌های قبلاً گزارش‌شده

هر یک از روش‌های ارائه‌شده برای رمزنگاری بصری مزایا و معایبی دارند. فارغ از معایب خاص روش‌ها، هر یک از آن‌ها برای حالت خاصی از رمزنگاری آستانه‌ای طراحی شده‌اند. هدف اصلی گزارش‌های قبلی [۷-۶]، ارائه روشی ساده برای پیاده‌سازی تمامی حالت‌های مختلف رمزنگاری بصری آستانه‌ای است. الگوریتم مطرح‌شده بر مبنای الگوریتم ژنتیک است که شامل اشکالاتی نیز هست. در ادامه به تشریح این روش، بهبود آن و جایگزینی آن با الگوریتمی ساده‌تری می‌پردازیم.

ازآنجایی‌که روشی جامع برای تمامی حالات رمزنگاری (k, n) وجود ندارد، لزوم طراحی الگوریتمی ساده که قابل‌اجرا برای مقادیر مختلف k و n باشد از جمله چالش‌های این شیوه از رمزنگاری به شمار می‌آید. بدین ترتیب، طرحی مبتنی بر الگوریتم ژنتیک برای رمزنگاری بصری آستانه‌ای ارائه شده که برای حالت (Γ_{Qual}, Γ_{Forb}) نیز قابل‌اجرا است [۷-۶].

هدف طرح پیشنهادی تولید ماتریس‌های پایه برای نگاشت پیکسل‌های سفید و پیکسل‌های مشکی برای تولید سهم‌های نویزی شکل با رعایت شروط امنیت و کنتراست است. برای تشریح این روش در ابتدا نیاز به بیان نحوه تعریف کروموزوم‌ها است. تمامی درایه‌های ماتریس‌های پایه ژن‌های یک کروموزوم را تشکیل می‌دهند، در واقع سطرهای این ماتریس‌ها کنار هم قرار می‌گیرند و حاصل قرار گرفتن این درایه‌ها در کنار هم یک بردار خواهد شد که کروموزوم را تشکیل می‌دهد. فرض کنید دو ماتریس پایه برای حالت (۲، ۲) به‌صورت زیر باشند:

$$S_0 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, S_1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

در این صورت برای تشکیل کروموزوم موردنظر، هر ماتریس با قرار گرفتن ردیف‌هایش در کنار هم به یک بردار تبدیل شده، سپس در کنار بردار حاصل از ماتریس دیگر قرار می‌گیرد. کروموزوم حاصل به‌صورت زیر خواهد بود:

$$C_i = \{1,0,0,1,0,1,1,0,0,1,1,0,0,1,1,0\}$$

در واقع در الگوریتم ژنتیک عکس این عملیات صورت می‌گیرد و تنها برای درک بهتر موضوع نحوه تشکیل کروموزوم به این صورت مطرح شد؛ در الگوریتم ژنتیک درایه‌های بردار C_i به‌صورت تصادفی تشکیل می‌شوند و پس از بهینه‌سازی، نتیجه حاصل که یک کروموزوم برداری است با تخصیص درایه‌ها، به‌صورت مشخص به هر ماتریس، به ماتریس‌های پایه تبدیل خواهد شد. با فرض داشتن n شریک و میزان m توسعه پیکسل، دو ماتریس n×m برای پیکسل‌های سفید و مشکی خواهیم داشت، بنابراین، اندازه بردار کروموزوم برابر با ۲×n×m خواهد بود. همان‌طور که در مثال بالا قابل مشاهده است طول بردار کروموزوم برابر با ۱۶ است که درنهایت به دو ماتریس ۴×۲ تبدیل می‌شود.

تولید ماتریس‌های پایه بهینه با رعایت شروط امنیت و کنتراست است [۷-۶]. بنابراین، تابع هدف بر مبنای وزن همینگ که هر دو شرط به آن وابسته است، تعریف شده است. به‌این‌ترتیب که کروموزوم C_i به دو ماتریس S_0 و S_1 تفکیک

[1] Visual Cryptography Scheme

گردیده و عملگر OR برای هر عضو X که زیرمجموعه‌های مجموعه شریک‌های P را تشکیل می‌دهند، اعمال می‌گردد. نمایش حاصل از اعمال عملگر OR به‌صورت S_0^x و S_1^x در نظر گرفته شده است. در این گزارش‌ها کنتراست (β) به‌صورت حاصل تفاضل وزن همینگ برای ماتریس پایه پیکسل مشکی و پیکسل سفید تعریف می‌شود:

$$\beta = H(S_1^X) - H(S_0^X) \quad (۴)$$

طبق تعریف در این نوع از رمزنگاری، میزان کنتراست برای $|X| < k$ باید برابر با صفر و در سایر حالت‌ها باید عددی مثبت و غیر صفر باشد. در واقع حاصل برهم‌گذاری X سهم برای $|X| < k$، که معادل با اعمال عملگر OR بر X سطر از هر ماتریس است، باید بردارهای مشابهی با تعداد یک‌های برابر تولید کند که میزان تفاضل وزن همینگ برابر با صفر شود و شرط امنیت برقرار گردد. از طرفی حاصل برهم‌گذاری X سهم برای $|X| \geq k$، باید بردارهایی را تولید کند که وزن همینگ بردار تولیدشده از ماتریس S_1، از وزن همینگ بردار تولیدشده از ماتریس S_0 بیشتر شده، شرط کنتراست رعایت شود و تصویر قابل‌تشخیص باشد.

تابع هدف به نحوی تعریف شده است که میزان برازندگی برای حالت‌های قابل‌قبول بالا رفته و در غیر این صورت کاهش یابد؛ به‌عبارت‌دیگر φ_0 به‌عنوان برازندگی اولیه به هر کروموزوم اختصاص می‌یابد و مقدار φ به‌عنوان تابع برازندگی، با توجه به مقدار β، با کاهش یا افزایش مقدار ثابت δ حاصل می‌گردد. الگوریتم به‌کاررفته در مقاله در ادامه آورده شده است.

```
Algorithm 1: Objective Function
Initialise φ0
φ = φ0
For each stack, s, of size 1 to k, do,
  If s < k, then,
    If β != 0, then φ := φ – δ
  Else,
     If β != 0, then,
      If general access structure and X1 != 1, then,
        φ = φ – δ
      Else, φ = φ + δ
      End If
    Else If β = 0, then φ = φ – δ
    End If
  End If
End For
```

در ابتدا مقدار برازندگی برابر با مقدار φ_0 قرار می‌گیرد که در این مرجع مقدار φ_0 به‌صورت دلخواه برابر با ۱۰۰ انتخاب شد. مسئله به‌صورت بهینه‌سازی حداکثری تعریف شده است بنابراین، مقادیر φهای بزرگ‌تر حاوی ماتریس‌های بهتری هستند. پس از مقداردهی اولیه به تابع برازندگی، بر روی نتیجه حاصل از برهم‌گذاری s سهم (حاصل اعمال OR بر s ردیف از ردیف‌های هر ماتریس) عملیات زیر انجام می‌شود:

برای $s < k$، اگر مقدار کنتراست حاصل غیر صفر باشد یعنی شرط امنیت رعایت نشده و به میزان δ از تابع برازندگی کم می‌شود. برای $s \geq k$، درصورتی‌که مقدار کنتراست مخالف با صفر باشد، الگوریتم بررسی می‌کند که اگر رمزنگاری بصری با ساختار دسترسی عمومی است سهم اول در این برهم‌گذاری شرکت دارد یا خیر. X_1 در این الگوریتم نشان‌دهنده سهم اول است.

حضور سهم اول برای بازیابی تصویر در حالت ساختار دسترسی عمومی ضروری در نظر گرفته شده است [۶-۷]. در صورت عدم حضور سهم اول از مقدار برازندگی کاسته و در صورت حضور بر مقدار آن افزوده می‌شود. درنهایت نیز اگر $s \geq k$ و مقدار کنتراست برابر با صفر باشد یعنی تصویر بازیابی‌شده حاصل از s سهم، نویزی شکل بوده و شرط کنتراست برقرار نیست بنابراین، به میزان δ از مقدار تابع برازندگی کم می‌شود و در اینجا الگوریتم پایان می‌یابد. مقدار δ همانند پارامترهای الگوریتم ژنتیک بهینه‌سازی می‌شود. در بخش بعد، نحوه بهینه‌سازی این پارامترها شرح داده خواهد شد.

برای اثبات درستی این روش، حالات مختلف رمزنگاری بصری آستانه‌ای شامل حالات (۲، ۲)، (۳، ۲)، (۳، ۳) و (۴، k) برای $k < ۴$ را بررسی شده است [۶]. در رمزنگاری (۲، ۲) با توسعه پیکسلی برابر با ۴، ماتریس‌های پایه نهایی به‌صورت زیر به دست آمد:

$$S_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}, S_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

تصاویر رمز حاصل از این ماتریس‌ها و نتیجه بازیابی تصویر در شکل (۳) آمده است. برای درک بهتر نتیجه در معادله ۳-۱ به‌جای x برای هر سهم شماره سهم و برای سهم‌هایی که عملگر OR بر آن‌ها اعمال شده است شماره آن‌ها را قرار می‌دهیم:

$$\begin{cases} H(S_0^1) = 2 \\ H(S_0^2) = 2 \\ H(S_1^1) = 2 \\ H(S_1^2) = 2 \end{cases} \rightarrow \begin{cases} \beta_1 = H(S_1^1) - H(S_0^1) = 0 \\ \beta_2 = H(S_1^2) - H(S_0^2) = 0 \end{cases}$$

همان‌طور که در عبارات بالا پیداست شرط امنیت به‌صورت کامل رعایت شده است. برای نمایش شرط کنتراست داریم:

$$\begin{cases} H(S_0^{1,2}) = 2 \\ H(S_1^{1,2}) = 4 \end{cases} \rightarrow \beta_{1,2} = H(S_1^{1,2}) - H(S_0^{1,2}) = 2$$

درنتیجه شرط کنتراست نیز برقرار است. کنتراست هر یک از سهم‌ها (α_1 و α_2) و درنهایت کنتراست تصویر بازیابی‌شده ($\alpha_{1,2}$) طبق معادله ۳ برابر است با:

$$\alpha_1 = \alpha_2 = \frac{T(B[A(0)]) - T(B[A(1)])}{1 + T(B[A(1)]} = \frac{\frac{2}{4} - \frac{2}{4}}{1 + \frac{2}{4}} = 0$$

$$\alpha_{1,2} = \frac{T(B[A(0)]) - T(B[A(1)])}{1 + T(B[A(1)]} = \frac{\frac{2}{4} - \frac{0}{4}}{1 + \frac{0}{4}} = \frac{1}{2}$$

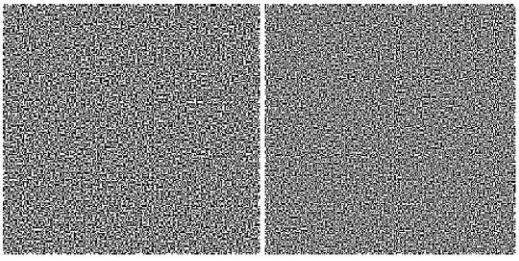
طبق [۹] کنتراست بهینه برای رمزنگاری (n, n) به‌صورت $\alpha = \frac{1}{2}^{n-1}$ است. بنابراین، برای n = ۲، کنتراست بهینه برابر با ۰/۵ خواهد بود که بهینگی این حالت از رمزنگاری را تائید می‌کند.

برای مقادیر $n \geq ۳$ از توسعه پیکسلی برابر با ۸ استفاده کردند. ماتریس‌های پایه برای مدل (۳، ۲) به‌صورت زیر هستند:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

(الف)



(ب)

شکل ۳. استفاده از الگوریتم ژنتیک جهت اجرای رمزنگاری بصری [۹] (الف) سهم اول و دوم، (ب) نتیجه بازیابی تصویر رمز

وزن همینگ هر یک از سهم‌ها و درنتیجه شرط امنیت به‌صورت زیر است:

$$\begin{cases} H(S_0^1) = 4 \\ H(S_0^2) = 4 \\ H(S_0^3) = 4 \\ H(S_1^1) = 4 \\ H(S_1^2) = 4 \\ H(S_1^3) = 4 \end{cases} \rightarrow \begin{cases} \beta_1 = H(S_1^1) - H(S_0^1) = 0 \\ \beta_2 = H(S_1^2) - H(S_0^2) = 0 \\ \beta_3 = H(S_1^3) - H(S_0^3) = 0 \end{cases}$$

همان‌طور که در محاسبات قابل مشاهده است شرط امنیت به‌صورت کامل رعایت شد. برای نمایش شرط کنتراست داریم:

$$\begin{cases} H(S_0^{1,2})=8 \\ H(S_0^{1,3})=8 \\ H(S_0^{2,3})=4 \\ H(S_0^{1,2,3})=8 \\ H(S_1^{1,2})=5 \\ H(S_1^{1,3})=7 \\ H(S_1^{2,3})=8 \\ H(S_1^{1,2,3})=8 \end{cases} \rightarrow \begin{cases} \beta_{1,2} = H(S_1^{1,2}) - H(S_0^{1,2}) = -3 \\ \beta_{1,3} = H(S_1^{1,3}) - H(S_0^{1,3}) = -1 \\ \beta_{2,3} = H(S_1^{2,3}) - H(S_0^{2,3}) = 4 \\ \beta_{1,2,3} = H(S_1^{1,2,3}) - H(S_0^{1,2,3}) = 0 \end{cases}$$

نتایج نشان می‌دهند شرط کنتراست برقرار نیست. حتی اگر فرض شود که ماتریس‌های S_1 و S_0 جابه‌جا نوشته شده‌اند که توجیه اعداد منفی باشد، تفاضل وزن همینگ در حالتی که سه سهم بر روی یکدیگر قرار می‌گیرند برابر با صفر است؛ بدین معنی که تصویر نهایی قابل‌تشخیص نخواهد بود. اما در مقاله ذکرشده که مقدار کنتراست تصویر نهایی طبق معیار بیان‌شده در مقاله [۱۱] برابر با مقدار بهینه است. ماتریس‌های پایه حاصل از این الگوریتم برای حالت (۳، ۳) در مقاله به‌صورت زیر ذکر شده‌اند:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

این ماتریس‌ها دقیقاً ماتریس‌های پایه‌ای هستند که برای حالت قبل ذکر شده‌اند که در این حالت نیز، با فرض جابه‌جایی ماتریس‌ها، شرط امنیت برقرار نیست زیرا تفاضل وزن همینگ حاصل از برهم‌گذاری دو سهم بر روی یکدیگر مقداری غیر صفر دارد و شرط کنتراست نیز برقرار نیست زیرا حاصل برهم‌گذاری هر سه سهم بر رو یکدیگر تفاضلی برابر با صفر دارد و درنتیجه تصویر حاصل نویزی شکل خواهد بود. برای حالت (۴، ۴) ماتریس‌های زیر ارائه شده‌اند:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S_1=\begin{bmatrix}0&1&1&1&0&1&0&0\\0&1&0&0&0&1&1&1\\1&1&0&1&0&0&1&0\\0&0&0&1&1&1&1&0\end{bmatrix}$$

وزن همینگ هر یک از سهم‌ها و درنتیجه شرط امنیت و نویزی شکل بودن هر سهم برای این حالت در ادامه محاسبه شده است.

$$\begin{cases}H(S_0^1)=4\\H(S_0^2)=4\\H(S_0^3)=4\\H(S_0^4)=4\\H(S_1^1)=4\\H(S_1^2)=4\\H(S_1^3)=4\\H(S_1^4)=4\end{cases}\rightarrow\begin{cases}\beta_1=H(S_1^1)-H(S_0^1)=0\\\beta_2=H(S_1^2)-H(S_0^2)=0\\\beta_3=H(S_1^3)-H(S_0^3)=0\\\beta_4=H(S_1^4)-H(S_0^4)=0\end{cases}$$

در این حالت برای برقراری امنیت باید نتایج حاصل از برهم‌گذاری هر دو و هر سه سهم نیز تفاضلی برابر با صفر داشته باشند. نتایج برهم‌گذاری دو سهم به‌صورت زیر است:

$$\begin{cases}H(S_0^{1,2})=6\\H(S_0^{1,3})=6\\H(S_0^{1,4})=6\\H(S_0^{2,3})=6\\H(S_0^{2,4})=6\\H(S_0^{3,4})=6\\H(S_1^{1,2})=6\\H(S_1^{1,3})=6\\H(S_1^{1,4})=6\\H(S_1^{2,3})=6\\H(S_1^{2,4})=6\\H(S_1^{3,4})=6\end{cases}\rightarrow\begin{cases}\beta_{1,2}=H(S_1^{1,2})-H(S_0^{1,2})=0\\\beta_{1,3}=H(S_1^{1,3})-H(S_0^{1,3})=0\\\beta_{1,4}=H(S_1^{1,4})-H(S_0^{1,4})=0\\\beta_{2,3}=H(S_1^{2,3})-H(S_0^{2,3})=0\\\beta_{2,4}=H(S_1^{2,4})-H(S_0^{2,4})=0\\\beta_{3,4}=H(S_1^{3,4})-H(S_0^{3,4})=0\end{cases}$$

برای این حالت نیز امنیت برقرار است. در حالت نهایی نتیجه برهم‌گذاری سه سهم به‌صورت زیر است:

$$\begin{cases}H(S_0^{1,2,3})=7\\H(S_0^{1,3,4})=7\\H(S_0^{1,2,4})=7\\H(S_0^{2,3,4})=7\\H(S_1^{1,2,3})=7\\H(S_1^{1,3,4})=7\\H(S_1^{1,2,4})=7\\H(S_1^{2,3,4})=7\end{cases}\rightarrow\begin{cases}\beta_{1,2,3}=H(S_1^{1,2,3})-H(S_0^{1,2,3})=0\\\beta_{1,3,4}=H(S_1^{1,3,4})-H(S_0^{1,3,4})=0\\\beta_{1,2,4}=H(S_1^{1,2,4})-H(S_0^{1,2,4})=0\\\beta_{2,3,4}=H(S_1^{2,3,4})-H(S_0^{2,3,4})=0\end{cases}$$

نتایج بالا نشان می‌دهند که این ماتریس‌های پایه شرط امنیت را رعایت می‌کنند. برای تحلیل و بررسی شرط کنتراست داریم:

$$\begin{cases}H(S_0^{1,2,3,4})=7\\H(S_1^{1,2,3,4})=8\end{cases}\rightarrow\beta_{1,2,3,4}=H(S_1^{1,2,3,4})-H(S_0^{1,2,3,4})=1$$

محاسبات نشان‌دهنده برقراری شرط کنتراست است. کنتراست تصویر بازیابی‌شده ($\alpha_{1,2,3,4}$) طبق معادله (۱-۳) برابر است با:

$$\alpha_{1,2,3,4}=\frac{T(B[A(0)])-T(B[A(1)])}{1+T(B[A(1)]}=\frac{\frac{1}{8}-\frac{0}{8}}{1+\frac{0}{8}}=\frac{1}{8}$$

کنتراست ۱/۸ طبق مقالات اشاره‌شده در صفحات قبل، بهینه است. نویسندگان [۶] ذکر کرده‌اند که برای حالت (k، ۴) و $k<4$ نیز الگوریتم به پاسخ بهینه دست یافت.

۴. طرح پیشنهادی

تابع هدف ساده‌ای برای رمزنگاری بصری آستانه‌ای قبلاً ارائه شده [۶] و مقادیر بهینه پارامترهای الگوریتم ژنتیک به‌صورت تجربی با هزینه محاسباتی کم به دست آمده است. در ابتدا به رفع اشکال موجود در این الگوریتم می‌پردازیم و در ادامه الگوریتمی برای دستیابی به کنتراست بهتر ارائه می‌دهیم. برای برطرف نمودن اشکال گفته‌شده در قسمت قبل، برای مقادیر $s \geq k$ در الگوریتم باید شرط $\beta!=0$ به‌صورت $\beta > 0$ اصلاح شود (در الگوریتم اصلاح‌شده و در ادامه بهبود داده‌شده در این مقاله، وجود سهم اول را الزامی در نظر نگرفتیم):

```
If s ≥ k
    If β > 0
      φ = φ + δ;
    Else
      φ = φ – δ;
    End
End
```

در این حالت حاصل تفاضل وزن همینگ جهت بازیابی تصاویر برای حالات $s \geq k$ منفی نشده و شرط کنتراست به‌درستی مطرح می‌شود. در الگوریتم ارائه‌شده توسط این مقاله میزان بالا یا پایین بودن کنتراست تأثیری ندارد. در واقع شرط کنتراست به‌گونه‌ای مطرح شده است که تنها غیر صفر بودن آن برای رسیدن به برازندگی مطلوب کافی است. بنابراین، الگوریتم لزوماً به جواب بهینه نخواهد رسید و دارای اشکال است. در ادامه برای اصلاح الگوریتم و در نظر گرفتن تأثیر مقدار کنتراست، کد زیر به الگوریتم اضافه شد:

```
For r < k
  If β = 0
    For r ≥ k
      φ = φ + sum (β);
    End
  End
End
```

در الگوریتم ارائه‌شده پس از اطمینان حاصل کردن از برقراری شرط امنیت، مقدار برازندگی محاسبه‌شده از قسمت قبل الگوریتم، با مقدار کنتراست‌های حاصل از برهم‌گذاری مقادیر بیشتر از k جمع می‌گردد. درنتیجه کروموزومی که شرط امنیت و

کنتراست را دارا باشد و درعین‌حال بیش‌ترین میزان کنتراست را پس از بازیابی تصاویر بدهد، به‌عنوان بهترین جواب ممکن از میان چندین حالت انتخاب خواهد شد.

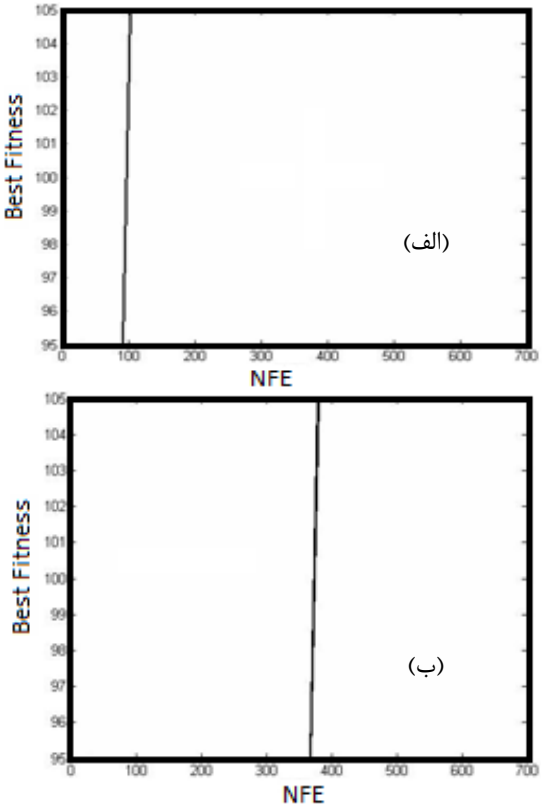
۵. تحلیل ویژگی‌ها و نقاط قوت طرح پیشنهادی

شکل (۷) اجرای الگوریتم در دو دفع مختلف برای حالت (۲، ۲) را نشان می‌دهد که برازندگی یکسانی حاصل شد اما ماتریس‌ها و درنتیجه کنتراست متفاوت است. ماتریس‌های پایه مطرح‌شده در این مرجع و کنتراست تصویر بازیابی‌شده به‌صورت زیر هستند:

$$S_0=\begin{bmatrix}1&0&1&0\\1&0&1&0\end{bmatrix}, S_1=\begin{bmatrix}0&0&1&1\\1&1&0&0\end{bmatrix}, \alpha_{1,2}=\frac{1}{2}$$

درصورتی‌که همان‌طور که در شکل (۴-الف) مشاهده می‌شود ماتریس‌های زیر نیز برازندگی یکسانی با ماتریس‌های بالا خواهند داشت:

$$S_0'=\begin{bmatrix}1&1&1&0\\1&1&1&0\end{bmatrix}, S_1'=\begin{bmatrix}0&1&1&1\\1&1&1&0\end{bmatrix}$$



شکل ۴. نمودار حاصل از اجرای الگوریتم پیشین در دو دفعه مختلف (الف) ماتریس‌های پایه S' با کنتراست نهایی ۱، (ب) ماتریس‌های پایه S با کنتراست نهایی ۲

وزن همینگ سهم‌ها در این حالت محاسبه شده و در نتیجه آن شرط امنیت برای ماتریس‌های جدید در ادامه بررسی می‌شود.

$$\begin{cases}H(S'^1_0)=3\\H(S'^2_0)=3\\H(S'^1_1)=3\\H(S'^2_1)=3\end{cases}\rightarrow\begin{cases}\beta'_1=H(S'^1_1)-H(S'^1_0)=0\\\beta'_2=H(S'^2_1)-H(S'^2_0)=0\end{cases}$$

همان‌طور که محاسبات نشان می‌دهند شرط امنیت رعایت شد. برای نمایش شرط کنتراست داریم:

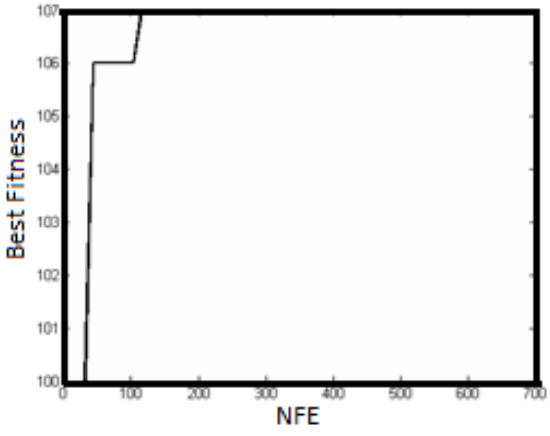
$$\begin{cases}H(S'^{1,2}_0)=3\\H(S'^{1,2}_1)=4\end{cases}\rightarrow\beta'_{1,2}=H(S'^{1,2}_1)-H(S'^{1,2}_0)=1$$

بنابراین، شرط کنتراست نیز برقرار است. مقدار کنتراست تصویر بازیابی‌شده $(\alpha'_{1,2})$ برابر است با:

$$\alpha'_{1,2}=\frac{T(B[A(0)])-T(B[A(1)])}{1+T(B[A(1)]}=\frac{\frac{1}{4}-\frac{0}{4}}{1+\frac{0}{4}}=\frac{1}{4}<\alpha_{1,2}=\frac{1}{2}$$

همان‌طور که محاسبات نشان می‌دهد کنتراست در این حالت برابر با ۰/۲۵ است که نصف حالت قبل است. بنابراین، با چندین بار اجرای الگوریتم، امکان ارائه کنتراست‌های بدتری وجود دارد. شکل (۵)، نمودار حاصل از اجرای الگوریتم پیشنهادی با در نظر گرفتن اهمیت مقدار کنتراست را برای حالت (۲، ۲) نشان می‌دهد. همان‌طور که مشاهده می‌شود میزان برازندگی در این نمودار متفاوت با حالت قبل است.

برای درک بهتر تفاوت الگوریتم مطرح‌شده و الگوریتم اصلاح‌شده قبلی، شکل (۶) نتیجه حاصل از استفاده از دو ماتریس‌های پایه ذکرشده در بالا (S و S') برای حالت (۲، ۲) را نشان می‌دهد. در واقع در الگوریتم قبلی هرکدام از این دو نتیجه قابل‌قبول بود ولی مشاهدات نشان می‌دهد کیفیت تصویر ۳-۹(ز) از تصویر ۳-۹(د) بهتر است.



شکل ۵. نمودار حاصل از اجرای الگوریتم پیشنهادی در حالت (۲، ۲)

با توجه به نتایج حاصل از محاسبات در بخش قبل، در سایر حالت‌ها نیز به نظر می‌رسد شرایط امنیت و کنتراست به‌خوبی رعایت نشده‌اند. ماتریس‌های پایه برای حالت (۳، ۲) با استفاده از

الگوریتم اصلاح‌شده و بهبودیافته به‌صورت زیر هستند:

$$S_0=\begin{bmatrix}1&0&1&0&1&0&1&0\\1&0&1&1&1&0&1&0\\1&1&1&0&1&0&1&0\end{bmatrix}$$

$$S_1=\begin{bmatrix}1&1&0&0&0&1&1&0\\0&1&1&1&1&0&1&0\\1&0&1&1&0&1&0&1\end{bmatrix}$$

وزن همینگ هر یک از سهم‌ها و درنتیجه شرط امنیت به‌صورت زیر است:

$$\begin{cases}H(S_0^1)=4\\H(S_0^2)=5\\H(S_0^3)=5\\H(S_1^1)=4\\H(S_1^2)=5\\H(S_1^3)=5\end{cases}\rightarrow\begin{cases}\beta_1=H(S_1^1)-H(S_0^1)=0\\\beta_2=H(S_1^2)-H(S_0^2)=0\\\beta_3=H(S_1^3)-H(S_0^3)=0\end{cases}$$

محاسبات نشان‌دهنده ارضای شرط امنیت هستند. برای نمایش شرط کنتراست داریم:

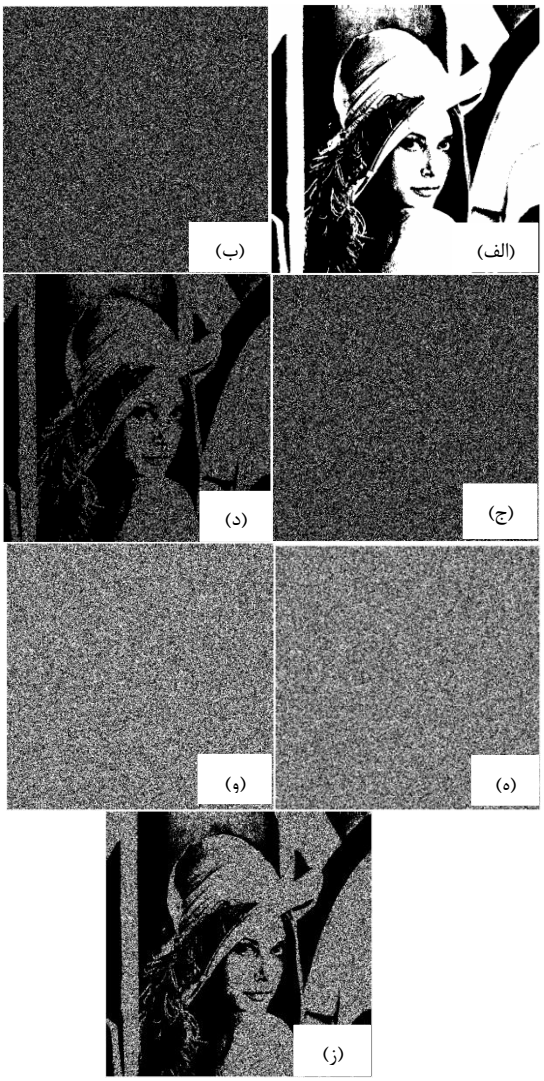
$$\begin{cases}H(S_0^{1,2})=5\\H(S_0^{1,3})=5\\H(S_0^{2,3})=6\\H(S_0^{1,2,3})=6\\H(S_1^{1,2})=7\\H(S_1^{1,3})=7\\H(S_1^{2,3})=8\\H(S_1^{1,2,3})=8\end{cases}\rightarrow\begin{cases}\beta_{1,2}=H(S_1^{1,2})-H(S_0^{1,2})=2\\\beta_{1,3}=H(S_1^{1,3})-H(S_0^{1,3})=2\\\beta_{2,3}=H(S_1^{2,3})-H(S_0^{2,3})=2\\\beta_{1,2,3}=H(S_1^{1,2,3})-H(S_0^{1,2,3})=2\end{cases}$$

همان‌طور که از نتایج پیداست شرط کنتراست برقرار است. کنتراست تصاویر بازیابی‌شده به‌صورت زیر هستند:

$$\alpha_{1,2}=\alpha_{1,3}=\frac{\frac{3}{8}-\frac{1}{8}}{1+\frac{1}{8}}=\frac{2}{9},\alpha_{2,3}=\alpha_{1,2,3}=\frac{\frac{2}{8}-\frac{0}{8}}{1+\frac{0}{8}}=\frac{2}{8}$$

جدول ۱. مقایسه نتایج

	نتایج اجرای الگوریتم قبلی [۶-۷]	نتایج اصلاح‌شده با الگوریتم ژنتیک	نتایج طرح پیشنهادی
کنتراست حاصل از برهم‌گذاری دو سهم در حالت (۲، ۲) با m=۴	۰/۵ یا ۰/۲۵	۰/۵ یا ۰/۲۵ ($\overline{NFE}$=219)	۰/۵ ($\overline{NFE}$=180)
میانگین کنتراست حاصل از برهم‌گذاری دو سهم در حالت (۲، ۳) با m=۸	منفی	-	۰/۲۳ ($\overline{NFE}$=210)
کنتراست حاصل از برهم‌گذاری سه سهم در حالت (۲، ۳) با m=۸	منفی	-	۰/۲۵ ($\overline{NFE}$=210)
کنتراست حاصل از برهم‌گذاری سه سهم در حالت (۳، ۳) با m=۸	منفی	-	۰/۱۲۵ ($\overline{NFE}$=221)
میانگین کنتراست حاصل از برهم‌گذاری دو سهم در حالت (۲، ۳) با m=۴	-	۰/۲ یا ۰/۳ ($\overline{NFE}$=301)	۰/۳ ($\overline{NFE}$=268)
کنتراست حاصل از برهم‌گذاری سه سهم در حالت (۲، ۳) با m=۴	-	۰/۲۵ یا ۰/۵ ($\overline{NFE}$=301)	۰/۵ ($\overline{NFE}$=268)
کنتراست حاصل از برهم‌گذاری سه سهم در حالت (۳، ۳) با m=۴	-	۰/۲۵ ($\overline{NFE}$=342)	۰/۲۵ ($\overline{NFE}$=289)



شکل ۶. مقایسه دو جواب قابل‌قبول در الگوریتم پیشین برای حالت (۲، ۲) (الف) تصویر محرمانه، (ب) سهم اول با استفاده از ماتریس‌های پایه S’، (ج) سهم دوم با استفاده از ماتریس‌های پایه S’، (د) تصویر بازیابی‌شده با استفاده از ماتریس‌های پایه S’، (ه) سهم اول با استفاده از ماتریس‌های پایه S، (و) سهم دوم با استفاده از ماتریس‌های پایه S، (ز) تصویر بازیابی‌شده با استفاده از ماتریس‌های پایه S

۶. نتیجه‌گیری

در این مقاله ضمن بیان مبانی پایه رمزنگاری بصری و تشریح الگوریتم‌های فراابتکاری، الگوریتمی بر مبنای الگوریتم اجتماع ذرات ارائه شد که ضمن برقراری شروط پایه، بهترین کنتراست را تا حد امکان بیابد. ازآنجایی‌که الگوریتم اجتماع ذرات، ساده‌تر بوده و برای رسیدن به جواب بهینه نیاز به عملیات محاسباتی کمتری ($\overline{NFE}$[1]) از نسبت به الگوریتم ژنتیک دارد، مسئله سادگی

[1] Number of Function Evaluations

و درعین‌حال جامع بودن روش تا حدی بهبود یافت. NFE بیانگر تعداد دفعاتی است که تابع برازندگی محاسبه می‌شود تا الگوریتم به جواب بهینه دست یابد. با توجه به این نکته که به ازای هر بار اجرا این مقدار متفاوت خواهد بود، این پارامتر به‌صورت میانگین بیان می‌گردد. در این مقاله ضمن رفع ایراد الگوریتم برخی گزارش‌ها مبنی بر منفی شدن کنتراست تصاویر در برخی حالات، الگوریتمی برای دستیابی به جواب بهینه از بین چندین جواب حاصل از آن الگوریتم ارائه شد. الگوریتم طرح‌شده ضمن کاهش میانگین تعداد عملیات لازم برای رسیدن به جواب بهینه، کنتراست را در حالت‌های مختلف افزایش می‌دهد.

۷. مرجع‌ها

[1] Naor, M.; Shamir, A. "Visual Cryptography"; Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1994.

[2] Thomas, S. A.; Gharge, S. "Review on Various Visual Cryptography Schemes"; Int. Conf. Current Trends in Computer, Electrical, Electronics and Communication, Mysore, 2017, 1164-1167.

[3] Jia, X.; Wang, D.; Nie, D.; Zhang, C. "Collaborative Visual Cryptography Schemes"; IEEE Trans. Circuits and Systems for Video Technology 2018, 28, 1056-1070.

[4] Chiu, P. L.; Lee, K. H. "A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes"; IEEE Trans. Information Forensics and Security 2011, 6, 992 - 1001.

[5] Lee, K. H.; Chiu, P. L. "Image Size Invariant Visual Cryptography for General Access Structures Subject to Display Quality Constraints"; IEEE Trans. Image Proc. 2013, 22, 3830-41.

[6] Buckley, N.; Nagar, A.; Arumugam, S. "Evolution of Visual Cryptography Basis Matrices with Binary Chromosomes"; IEEE 8th EUROSIM Congress on Modelling and Simulation 2013.

[7] Arumugam, S.; Lakshmanan, R.; Nagar, A. K. "On (k, n)*-Visual Cryptography Scheme Designs"; Codes and Cryptography 2014, 71, 153-162.

[8] Revenkar, P. S.; Anjum, A.; Gandhare, W. "Survey of Visual Cryptography Schemes"; Int. J. Security and Its Applications 2010, 4, 49-56.

[9] Ramya, J.; Parvathavarthini, B. "An Extensive Review on Visual Cryptography Schemes"; IEEE Int. Conf. Control, Instrumentation, Communication and Computational Technologies, 2014.

[10] Hou, Y. C. "Visual Cryptography for Color Images"; Pattern Recognition 2003, 36, 1619-1629.

[11] Ateniese, G.; Blundo, C.; De Santis, A.; Stinsonc, D. R. "Constructions and Bounds for Visual Cryptography"; Int. Colloquium on Automata, Languages, and Programming. 1996, 416-428.

[12] Hofmeister, T.; Krause, M.; Simon, S. M. "Contrast-Optimal k Out of n Secret Sharing Schemes in Visual Cryptography"; Theoretical Computer Sci. 2000, 240, 471-485.

[13] Ateniese, G.; Blundo, C.; De Santis, A.; Stinsonc, D. R. "Extended Capabilities for Visual Cryptography"; Theoretical Computer Sci. 2001, 250, 143-161.

[14] Mirghaderi, A.; Jolfaei, A. "A Novel Chaotic Image Encryption Scheme Using Chaotic Maps"; Adv. Defence Sci. Technol. 2011, 2, 111-124.