Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 3, Autumn 2022, Serial No. 39

A novel lossless color secret image sharing based on homogeneous linear recursion

S. Charoghchi, S. Mashhadi*

*Assistant Professor, Iran University of Science and Technology, Tehran, Iran

(Received: 12/12/2021, Accepted: 18/01/2022)

ABSTRACT

In this paper, we propose a new color secret image sharing based on homogeneous linear recursion (HLR). Merits of the previous related schemes, such as no pixel expansion, no code book required, no public image, lossless recovery, and high resolution are maintained in the proposed scheme, simultaneously. In addition, it has smaller shadow images and less complex calculations compared to related works. Besides, there are three methods for reconstruction that make it more convenient. Also, the RGB components of the secret image are processed in one step and there is no need to repeat the process of the scheme for each color channel that makes the process faster and more convenient .

Keywords: Secret image sharing, Lossless recovery, Color image, Shadow image, Homogeneous linear recursion.

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

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۳، پاییز ۱۴۰۱، ص ۱۱۸- ۱۰۷

علمی – پژوهشی

یک طرح تسهیم راز جدید برای تصاویر رنگی بر مبنای روابط بازگشتی خطی همگن

سارا چاروقچی[۱]، سمانه مشهدی[۲*]

۱- دانشجوی دکترای ریاضی، ۲- استادیار، دانشگاه علم وصنعت ایران، تهران، ایران

(دریافت: ۱۴۰۰/۰۹/۲۱، پذیرش: ۱۴۰۰/۱۰/۲۸)

چکیده

در این مقاله یک طرح تسهیم راز جدید برای تصاویر رنگی بر مبنای روابط بازگشتی خطی همگن ارائه کرده‌ایم. این طرح مزایای موجود در کارهای مرتبط، همچون عدم انبساط پیکسل‌ها، عدم نیاز به کتاب کد، بازسازی بدون نقص و کیفیت بالای بازسازی را به‌طور همزمان دارد. علاوه بر این دارای تصاویر سایه با اندازه کوچک‌تر و پیچیدگی محاسباتی کمتر نسبت به کارهای مشابه قبلی است. همچنین در قسمت بازسازی تصویر از سه روش ماتریس واندرموند، رابطه بازگشتی و درون‌یابی چندجمله‌ای می‌توان استفاده کرد که استفاده از این طرح را آسان‌تر می‌سازد.

کلیدواژه‌ها: رابطه همگن خطی بازگشتی، تسهیم راز، تسهیم راز تصویر رنگی، کیفیت بازسازی، اندازه سایه

۱- مقدمه

پیشرفت در فناوری اطلاعات و افزایش انتقال تصاویر در بستر اینترنت و یا ذخیره‌سازی آن‌ها در دستگاه‌های دیجیتال و یا سرورهای ابری باعث افزایش نیاز به تأمین امنیت این تصاویر شده است. روش‌های مختلفی همچون رمزنگاری تصویری، تسهیم راز تصویری و نهان‌نگاری برای حل این مسئله به کار گرفته شده است [۱، ۲، ۳، ۴، ۵، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۲، ۱۳، ۱۴، ۱۵، ۱۶ و ۱۷].

در میان راهکارهای بیان شده برای تأمین امنیت تصاویر تسهیم راز تصویری از اهمیت بالایی برخوردار است زیرا به‌وسیله آن می‌توان اطلاعات را بین گروهی از افراد به اشتراک گذاشت و مانند روش‌های دیگر تمام اطلاعات در اختیار یک فرد قرار نمی گیرد و که این امر خود از امکان تخریب عمدی یا سهوی اطلاعات و ایجاد تغییر در تصاویر جلوگیری می‌کند .علاوه بر این از این طرح‌ها برای مدیریت حافظه می‌توان استفاده کرد، به‌این‌ترتیب که اطلاعات تصویر را در چندین حافظه مجزا تسهیم کرد. در واقع در طرح تسهیم راز تصویری (t,n) تصویر راز بین n شرکت‌کننده[۱] از طریق تصاویر سایه تسهیم می‌شود به‌طوری‌که هر t نفر از آن‌ها امکان بازسازی تصویر راز را دارند و هر $t-1$ نفر و یا کمتر هیچ‌گونه اطلاعاتی راجع به تصویر راز نمی توانند به دست بیاورند. طرح‌های موجود در دو دسته تسهیم راز بصری *VSS*[۲] و تسهیم راز تصویری بر مبنای چندجمله‌ای *PSIS*[۳] قرار می‌گیرند. در طرح‌های تسهیم راز بصری عملیات بازسازی تنها با قرار دادن تصاویر سایه روی هم و با استفاده از قدرت بینایی چشم انسان انجام می‌شود و نیازی به انجام محاسبات نیست. اولین طرح تسهیم راز بصری توسط نایور و شمیر[۴] در سال ۱۹۹۵ ابداع شد [۱۸]. سهولت در بازسازی تصویر راز محققین را ترغیب کرد تا طرح‌های دیگری در جهت ارتقای طرح اول ارائه کنند [۱۹، ۲۰، ۲۱، ۲۲، ۲۳ و ۲۴]. ولی این دسته از طرح‌ها ضعف‌هایی همچون انبساط پیکسل[۵]، کیفیت پایین تصاویر بازسازی شده و بازسازی نقص‌دار[۶] دارند. خوشبختانه این مشکلات در طرح‌های *PSIS* برطرف شده‌اند [۲، ۹، ۲۵، ۲۶، ۲۷، ۲۸ و ۲۹]. در سال ۲۰۰۲ تین و لین[۷] اولین طرح *PSIS* را ارائه کردند که بر اساس طرح تسهیم راز شمیر[۸] [۳۰] نوشته شده بود. محققین در مقالات متعددی با افزایش قابلیت‌هایی همچون تسهیم راز همراه با نهان‌نگاری [۱۵، ۳۱، ۳۲، ۳۳، ۳۴، ۳۵ و ۳۶]، تصاویر سایه کوچک‌تر [۲۷ و ۳۷]، طرح‌های سلسله‌مراتبی [۲، ۳۸، ۳۹، ۴۰، ۴۱ و ۴۲]، طرح‌های پیش‌رونده [۴۳، ۴۴ و ۴۵] و همچنین طرح‌های مقیاس‌پذیر [۴۲ و ۴۶] به بهبود کار آن‌ها پرداختند. تمامی کارهایی که تا کنون به آن‌ها اشاره شد برای تصاویر سیاه سفید و خاکستری طراحی شده‌اند. البته برخی از آن‌ها قابل استفاده برای تصاویر رنگی نیز می‌باشند ولی کارآمدی مطلوبی در این زمینه ندارند [۹ و ۳۷]. در واقع، باوجوداینکه تحقیقات زیادی در زمینه تسهیم راز تصاویر سیاه سفید و خاکستری انجام شده کار زیادی در زمینه تصاویر رنگی

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

[1] Participant
[2] Visual secret sharing
[3] Polynomial based secret image sharing
[4] Naor and Shamir
[5] Pixel expansion
[6] Lossy reconstruction
[7] Thien and Lin
[8] Shamir

ناشر: دانشگاه جامع امام حسین (ع)

صورت نگرفته است. بخش عمده طرح‌های موجود برای تصاویر رنگی از نوع *VSS* هستند که مشکلاتی چون انبساط پیکسل که منجر به تولید تصاویر سایه با اندازه بزرگ‌تر از تصویر راز می‌شود، [۴۷، ۴۸، ۴۹ و ۵۰] و کیفیت پایین تصویر بازسازی شده [۴۷، ۴۹، ۵۰، ۵۱، ۵۲ و ۵۳] دارند. در برخی از طرح‌های *VSS* همچون طرح‌های پیش‌رونده [۵۵ و ۵۴] این ضعف‌ها برطرف شده ولی همچنان طرح [۵۴] کارآمد نیست و از طرفی [۵۵] محدود به‌شرط آستانه‌ای $(2,2)$ است. مشابه تصاویر خاکستری روش دیگر برای تسهیم راز تصاویر رنگی طرح های *PSIS* هستند اما تعداد مقالات در این زمینه بسیار محدود می‌باشد [۵۹، ۵۸، ۵۷، ۵۶ و ۴۴]. طرح [۵۶] طرحی بدون نقص با استفاده از طرح شمیر و ماتریس تصویر[1] است که اندازه تصاویر سایه آن برای یک طرح (t,n) برابر $\frac{1}{t}+\frac{1}{n}$ اندازه تصویر راز است. همچنین [۵۷] یک طرح *PSIS* نقص دار است که تصویر راز را به روش *GSBTC*[2] فشرده می‌سازد و تصاویر سایه با اندازه کوچک‌تر از تصویر راز تولید می‌کند. در [۵۸] تصویر راز به صورت یک رشته $b-$ بایتی در نظر گرفته می‌شود و محاسبات به پیمانه عدد اول p که به ترتیب $2^{8}<p<2^{8b}$ برای تصاویر خاکستری و $2^{24}<p<2^{24b}$ برای تصاویر رنگی است، انجام می‌شوند. اعداد اول بزرگ در این طرح به‌منظور افزایش کیفیت بازسازی استفاده می‌شوند اگرچه از طرف دیگربار محاسباتی را افزایش می‌دهند. همچنین با اعمال برخی عملیات امکان بازسازی بدون نقص وجود دارد ولی باعث بزرگ شدن اندازه تصاویر سایه می‌شود. اخیراً یک طرح *PSIS* بدون نقص ارائه شد که در آن از میدان $\mathbb{Z}_{۲۵۶}\times\mathbb{Z}_{۲۵۶}\times\mathbb{Z}_{۲۵۶}$ استفاده می‌شود. در این طرح $(۳و۴)$ اندازه تصاویر سایه $\frac{۱}{۲}$ اندازه تصویر راز است.

در این مقاله یک طرح *PSIS* بدون نقص بر مبنای روابط بازگشتی خطی همگن[3] (*HLR*) ارائه شده است. طرح تسهیم راز تصویری بر مبنای *HLR* برای اولین بار توسط ما در [۳۷] و با الهام از طرح [۶۰] ارائه شد. اگرچه طرح [۳۷] قابل استفاده برای تصاویر رنگی نیز می‌باشد ولی روشی کاملاً متفاوت با طرح پیشنهادشده در این مقاله دارد. به عنوان مثال تمامی مراحل [۳۷] باید برای کانال های قرمز، سبز و آبی به طور جداگانه اعمال شود که از این نظر استفاده از آن برای تصاویر رنگی بهینه نیست. در طرح [۳۷] تعداد آستانه کمتر از تعداد سهامداران و اندازه سایه‌ها بزرگ‌تر بود. در جدول یک به‌صورت خلاصه طرح‌ها مقایسه شده اند. بنا به جدول ۱ طرح ما برخی از مشکلات طرح‌های پیشین را رفع کرده است و علاوه بر این برخی ویژگی‌هایی را بهبود بخشیده است. به‌طور مثال اندازه تصاویر سایه در طرح ما از تمامی طرح‌های بدون نقص کوچک‌تر است.

همچنین به دلیل استفاده از روابط خطی طرح ما از پیچیدگی محاسباتی کمتری برخوردار است. پردازش اطلاعات یک مرحله ای کانال های رنگی ویژگی دیگر طرح ارائه شده است که باعث افزایش سرعت و سهولت در استفاده از آن می‌شود. دستاوردهای این پژوهش به شرح زیر می‌باشد:

(۱) در این مقاله یک طرح تسهیم راز بدون نقص بر مبنای *HLR* ارائه شده است که در یک مرحله عملیات تسهیم راز را انجام می‌دهد و برخلاف طرح [۳۷] نیازی به تکرار روند طرح برای هر بلوک تصویر راز ندارد و از این نظر بار محاسباتی کمتر و سرعت اجرای بالاتری دارد.

(۲) طرح ارائه شده برخلاف اغلب طرح‌های قبلی نیازی به پیش پردازش برای تأمین امنیت ندارد و امنیت آن تنها بر مبنای تسهیم راز است.

(۳) اندازه تصاویر سایه تولید شده $\frac{1}{n}$ تصویر راز است که این امر موجب افزایش بهینگی در انتقال و نگهداری تصاویر سایه تولید شده می‌شود.

(۴) استفاده از میدان عدد اول ۲۵۷، امکان بازسازی بدون نقص را فراهم کرده و سرعت محاسبات را افزایش داده است.

ترتیب مطالب مقاله به این شرح است، در بخش دوم مقدمات ریاضی موردنیاز بیان شده و مفاهیم مربوط به *HLR* به طور دقیق شرح داده شده است. طرح ارائه شده در بخش سوم توضیح داده شده است. نتایج مربوط به آزمایش طرح و مقایسه آن با طرح های مشابه به ترتیب در بخش های چهارم و پنجم قرار دارند. همچنین نتیجه‌گیری در بخش ششم انجام شده است.

۲- پیش‌نیازها

در این بخش مقدمات موردنیاز برای مطالعه مقاله را شرح داده شده است. ایده اصلی طرح ما بر مبنای روابط بازگشتی خطی همگن است. به این منظور ابتدا به بیان تعاریف و قضایای این مفهوم ریاضی می‌پردازیم. برای مطالعه عمیق‌تر مطالب به [۳۷ و ۶۱] مراجعه کنید.

۲-۱- روابط بازگشتی خطی همگن

در این تحقیق از روابط بازگشتی خطی همگن برای تسهیم راز تصویری استفاده شده است. به همین منظور ابتدا تعاریف و قضایای موردنیاز با این مفهوم بیان شده است. فرض کنید $n\geq 0$ یک عدد صحیح و $a_1,a_2,...,a_n$ و $c_1,c_2,...,c_n$ اعداد حقیقی باشند. یک رابطه بازگشتی خطی همگن *HLR* از درجه n توسط دستگاه معادلات زیر تعریف می‌شود [۶۰]:

$$\begin{cases} u_1=c_1, u_2=c_2,...,u_n=c_n \\ u_{n+i}+a_1u_{n+i-1}+a_2u_{n+i-2}+...+a_nu_i=0 \quad (i\geq 1) \end{cases} \qquad (1)$$

[1] Projection matrix
[2] Gradual search algorithm for a single bitmap BTC
[3] Homogeneous linear recursion

جدول (۱). مقایسه‌ی طرح SIS رنگی با طرح‌های مشابه قبلی

طرح	[۴۴]	[۴۵]	[۵۵]	[۵۶]	[۵۷]	[۵۸]	[۵۹]	طرح ما
تصویر	رنگی	رنگی	رنگی	رنگی	رنگی	رنگی	رنگی	رنگی
روش هسته ای	بولین	بصری	بصری	چندجمله ای	چندجمله ای	چندجمله ای	چندجمله ای	HLR
بدون نقص	بله	خیر	خیر	بله	خیر	خیر/بله	بله	بله
ابعاد سایه	۱	۱	۱	$\frac{1}{t}+\frac{1}{n}$	$\frac{1}{2t}$	$\frac{1}{t-1}$ ، $\frac{t-1}{b}+\frac{1}{t-1}$	$\frac{1}{t-1}$	$\frac{1}{n}$
فشرده سازی	خیر	خیر	خیر	خیر	بله	خیر	خیر	خیر
پیش پردازش	خیر	خیر	خیر	خیر	بله	بله	خیر	خیر
یک مرحله ای	خیر	خیر	خیر	خیر	خیر	خیر	بله	بله
مقدار عمومی	خیر	خیر	خیر	خیر	خیر	خیر	خیر	خیر
آستانه	(۲,n)	(t,n)	(۲,۲)	(t,n)	(t,n)	(t,n)	(t,n)	(n,n)
انبساط پیکسل	خیر	خیر	بله	خیر	خیر	خیر	خیر	خیر
پیشرونده	بله	بله	بله	خیر	خیر	خیر	خیر	خیر

تعریف ۲-۱- معادله مشخصه رابطه بازگشتی خطی همگن از درجه n به شکل زیر است [۶۰]:

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + ... + a_n = 0 \qquad (۲)$$

قضیه ۲-۱- فرض کنید u_i یک دنباله HLR و α یک ریشه معادله مشخصه آن با درجه تکرار n در این صورت معادله بدیهی آن به‌صورت زیر محاسبه می‌شود [۶۰]:

$$u_i = p(i)\alpha^i = (A_0 + A_1 i + ... + A_{n-1} i^{n-1})\alpha^i \ (i \geq 1) \qquad (۳)$$

نکته ۲-۱. فرض کنید α به‌عنوان یک ریشه معادله مشخصه و $\{u_1, u_2, ..., u_n\}$، n جمله دلخواه از HLR داده شده است در این صورت معادله بدیهی دنباله از روش‌های زیر قابل‌محاسبه است [۶۰]:

(۱) بنا به قضیه ۲-۱ معادله صریح دنباله به هر دو روش زیر قابل‌محاسبه است:

$$\begin{bmatrix} ۱ & ۱ & ۱ & \dots & ۱ \\ ۱ & ۲ & ۲^۲ & \dots & ۲^{n-۱} \\ \vdots & & & & \\ ۱ & n & n^۲ & \dots & n^{n-۱} \end{bmatrix} \begin{bmatrix} A_۰ \\ A_۱ \\ \vdots \\ A_{n-۱} \end{bmatrix} = \begin{bmatrix} u_۱/\alpha \\ u_۲/\alpha^۲ \\ \vdots \\ u_n/\alpha^n \end{bmatrix} \qquad (۴)$$

$$\begin{bmatrix} ۱ & ۱ & ۱ & \dots & ۱ \\ ۱ & ۲ & ۲^۲ & \dots & ۲^{n-۱} \\ \vdots & & & & \\ ۱ & n & n^۲ & \dots & n^{n-۱} \end{bmatrix} \begin{bmatrix} A_۰ \\ A_۱ \\ \vdots \\ A_{n-۱} \end{bmatrix} = \begin{bmatrix} u_۱/\alpha \\ u_۲/\alpha^۲ \\ \vdots \\ u_n/\alpha^n \end{bmatrix}$$

(الف) حل دستگاه واندرموند [1]: بنا به تساوی قضیه ۲-۱ ضرایب $A_0, A_1, ..., A_{n-1}$ با حل دستگاه زیر قابل‌محاسبه هستند:

(ب) استفاده از درون‌یابی چندجمله‌ای [2]: بنا به تساوی قضیه ۲-۱ با داشتن n نقطه $(j, \frac{u_j}{\alpha^j})$، $j \in \{1,2,...,n\}$ و با استفاده از درون‌یابی می‌توان معادله صریح دنباله را به‌صورت زیر محاسبه کرد:

$$p(i) = \sum_{j=1}^{n} \frac{u_j}{\alpha^j} \prod_{k=1, k\neq j}^{n} \frac{i-k}{j-k} \qquad (۵)$$

(۲) بنا به رابطه بازگشتی HLR و با داشتن هر n جمله متوالی و رابطه ذیل:

$$u_{n+i} + a_1 u_{n+i-1} + a_2 u_{n+i-2} + ... + a_n u_i = 0 \ \ (i \geq 1) \qquad (۶)$$

می‌توان تمام جملات دنباله را محاسبه کرد.

۳- طرح ارائه شده

در این بخش مراحل طرح به‌طور کامل شرح داده شده است.

۳-۱- آماده‌سازی

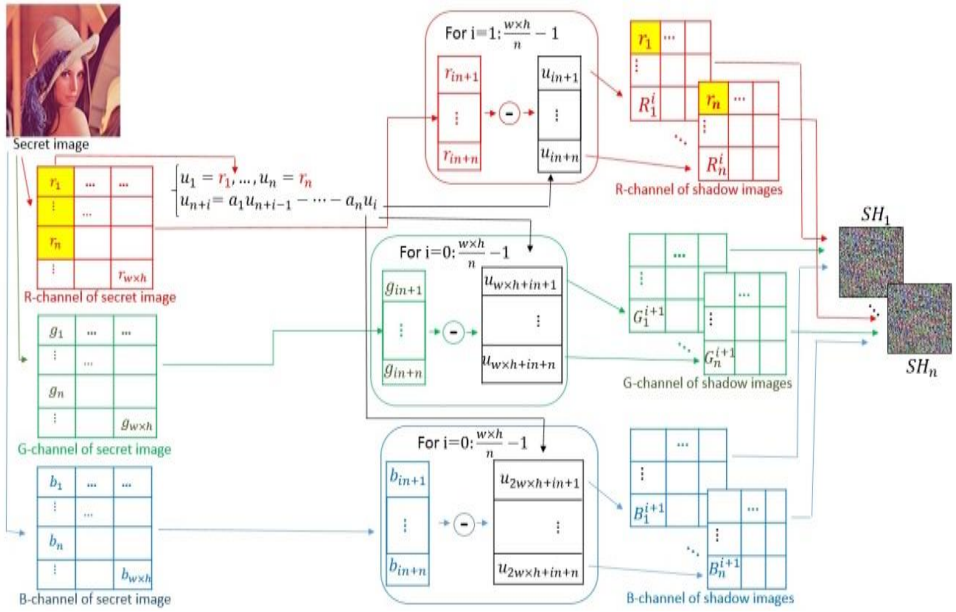
فرض کنید S یک تصویر راز رنگی RGB با ابعاد $W \times H$ باشد. پیکسل j-ام S، S_j قرار داده می‌شود. همچنین r_j ، g_j و b_j به ترتیب مؤلفه‌های قرمز، سبز و آبی S در نظر گرفته می‌شود. واسطه ابتدا یک ریشه صحیح مثبت α را به‌عنوان ریشه چندجمله‌ای مشخصه انتخاب و چندجمله‌ای را می‌سازد. سپس رابطه بازگشتی زیر را تعریف می‌کند:

$$(x-\alpha)^n = x^n + a_1 x^{n-1} + a_2 x^{n-2} + ... + a_n = 0 \qquad (۷)$$

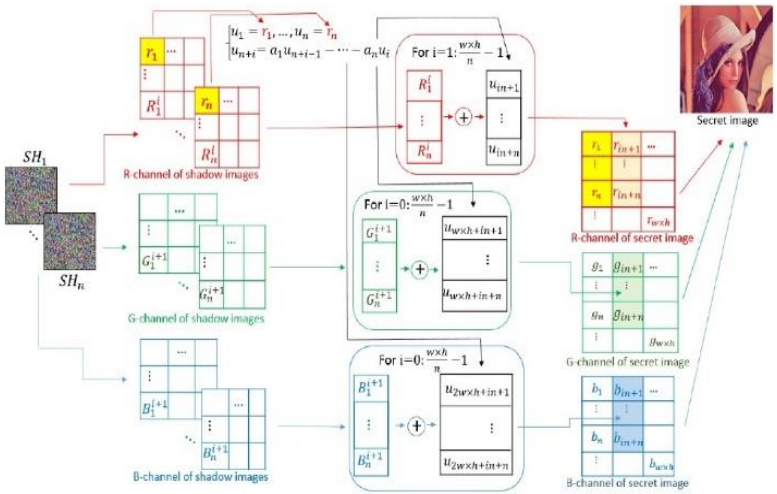
$$\begin{cases} u_1 = r_1, u_2 = r_2, ..., u_n = r_n \\ u_{n+i} + a_1 u_{n+i-1} + a_2 u_{n+i-2} + ... + a_n u_i = 0 \ \ (i \geq 1) \end{cases} \qquad (۸)$$

[1] Vandermonde system

[2] Polynomial interpolation



شکل (۱). مرحله تسهیم تصویر راز



شکل (۲): مرحله‌ی بازسازی تصویر راز

۳-۲- تسهیم

در این مرحله واسطه مؤلفه‌های رنگ قرمز، سبز و آبی تصاویر سایه را به صورت جداگانه تولید می‌کند. برای ایجاد کانال رنگ قرمز تصویر سایه $SH_j\ (1\le j\le n)$ به شیوه زیر عمل می‌کند:

$$\begin{cases} r_j & 1st\ pixel \\ R_j^i = r_{in+j} - u_{in+j} & (i+1)-th\ pixel \end{cases} \qquad (۹)$$

حال برای ایجاد کانال رنگ سبز پیکسل $i+1$-ام تصویر سایه $SH_j\ (1\le j\le n)$ و $1\le i\le \frac{W\times H}{n}$ عبارت زیر را محاسبه می‌کند:

$$G_j^{i+1} := g_{in+j} - u_{w\times h+in+j} \qquad (۱۰)$$

برای ایجاد کانال رنگ آبی پیکسل $i+1$-ام تصویر سایه $SH_j\ (1\le j\le n)$ و $1\le i\le \frac{W\times H}{n}$ عبارت زیر را محاسبه می‌کند:

$$B_j^{i+1} := b_{in+j} - u_{2w\times h+in+j} \qquad (۱۱)$$

۳-۳ بازسازی

فرض کنید سهام‌داران می‌خواهند تصویر راز S را بازسازی کنند. به این منظور آن‌ها ابتدا با مؤلفه قرمز اولین پیکسل تصویر راز، رابطه HLR ذیل را تشکیل می‌دهند:

$$u_i = (A_0 + A_1 i + \dots + A_{n-1} i^{n-1})\alpha^i \qquad (۱۲)$$

بر اساس نکته ۲-۱ می‌توانند تمام جملات دنباله را به سه روش زیر محاسبه کنند:

- استفاده از رابطه بازگشتی:

$$u_{n+i} = -a_1 u_{n+i-1} - a_2 u_{n+i-2} - \ldots - a_n u_i \qquad (۱۳)$$

• استفاده از فرمول صریح دنباله *HLR*، به‌طور مثال

$$u_i = (A_0 + A_1 i + \ldots + A_{n-1} i^{n-1})\alpha^i \qquad (۱۴)$$

که ضرایب A_i در آن را توسط حل دستگاه واندرموند ذیل محاسبه می‌کنند:

$$\begin{bmatrix} ۱ & ۱ & ۱ & \ldots & ۱ \\ ۱ & ۲ & ۲^۲ & \ldots & ۲^{n-۱} \\ \vdots & & & & \\ ۱ & n & n^۲ & \ldots & n^{n-۱} \end{bmatrix} \begin{bmatrix} A_۰ \\ A_۱ \\ \vdots \\ A_{n-۱} \end{bmatrix} = \begin{bmatrix} \frac{u_۱}{\alpha} \\ \frac{u_۲}{\alpha^۲} \\ \vdots \\ \frac{u_n}{\alpha^n} \end{bmatrix} \qquad (۱۵)$$

• استفاده از رابطه صریح برای $u_i = p(i)\alpha^i$ که در آن $p(i)$ توسط درون‌یابی محاسبه می‌شود:

$$p(i) = \sum_{j=1}^{n} \frac{u_j}{\alpha^j} \prod_{k=1, k\neq j}^{n} \frac{i-k}{j-k} \qquad (۱۶)$$

سپس $r_1, r_2, \ldots, r_n$ را به‌عنوان مؤلفه‌های قرمز n پیکسل اول و در ادامه مقادیر $r_{in+j} = R_j^i + u_{in+j},\ 1 \le j \le n$ را به‌عنوان مؤلفه قرمز اعضای $(i+1)$- امین بخش n پیکسلی تصویر راز S در نظر می‌گیرند. همچنین برای بازسازی کانال رنگ سبز $g_{in+j} = G_j^{i+1} + u_{w\times h+in+j},\ 1 \le j \le n$ را به‌عنوان مؤلفه رنگ سبز i- امین بخش n پیکسلی تصویر راز S در نظر می‌گیرند. در نهایت برای بازسازی کانال آبی مقادیر $b_{in+j} = B_j^{i+1} + u_{2w\times h+in+j},\ 1 \le j \le n$ را به‌عنوان مؤلفه رنگ سبز i- امین بخش n پیکسلی تصویر راز S در نظر می‌گیرند. برای ایجاد شفافیت بیشتر برای خوانندگان، در شکل‌های ۱ و ۲ به‌ترتیب مراحل تسهیم و بازسازی به‌طور کامل نشان داده شده است.

۳-۴- مثال

در این بخش طرح تسهیم راز رنگی ارائه شده توسط یک مثال به‌طور کامل شرح داده شده است. فرض کنید $n=4$ و $\alpha=1$، طرح (4,4) روی تصویر راز با ابعاد 128×128 اجرا می‌شود. فرض کنید $s_1, \ldots, s_8$ هشت پیکسل اول تصویر راز s باشند. واسطه ابتدا کانال‌های رنگی هر پیکسل s_j را به ترتیب به‌صورت r_j ، g_j و b_j جداسازی می‌کند. فرض کنید:

$$r_1 = 224, r_2 = 219, r_3 = 220, r_4 = 239$$
$$r_5 = 225, r_6 = 225, r_7 = 229, r_8 = 223$$
$$g_1 = 134, g_2 = 132, g_3 = 126, g_4 = 122$$
$$b_1 = 115, b_2 = 117, b_3 = 111, b_4 = 104$$

سپس واسطه $r_1 = 224, r_2 = 219, r_3 = 220, r_4 = 239$ را به‌عنوان چهار جمله اول رابطه بازگشتی خطی قرار می‌دهد و سپس چندجمله‌ای مشخصه $(x-1)^4 = 0$ را محاسبه می‌کند:

و دنباله *HLR* را به‌صورت زیر تعریف می‌کند:

$$\begin{cases} u_1 = 224, u_2 = 219, u_3 = 220, u_4 = 229 \\ u_{4+i} + 253u_{3+i} + 6u_{2+i} + 253u_{1+i} + u_i = 0\ (i \ge 1) \end{cases}$$

حال با استفاده از جملات *HLR* مؤلفه‌های *RGB* پیکسل‌های تصاویر سایه را تولید می‌کند. با توجه به تساوی ۹ واسطه $R_1^1, R_2^1, R_3^1, R_4^1$ به‌عنوان مؤلفه کانال قرمز دومین پیکسل از تصاویر سایه $SH_1, SH_2, \ldots, SH_n$ قرار می‌دهد.

$$u_5 = -(253\times239 + 6\times220 + 253\times219 + 224) = 31 \bmod 257$$
$$u_6 = -(253\times31 + 6\times239 + 253\times220 + 219) = 122 \bmod 257$$
$$u_7 = -(253\times122 + 6\times31 + 253\times239 + 220) = 10 \bmod 257$$
$$u_8 = -(253\times10 + 6\times122 + 253\times31 + 239) = 221 \bmod 257$$
$$R_1^1 = r_5 - u_5 = 225 - 31 = 194 \bmod 257$$
$$R_2^1 = r_6 - u_6 = 225 - 122 = 103 \bmod 257$$
$$R_3^1 = r_7 - u_7 = 229 - 10 = 219 \bmod 257$$
$$R_4^1 = r_8 - u_8 = 223 - 221 = 2 \bmod 257$$

پیکسل های بعدی کانال قرمز تصاویر سایه با توجه تساوی ۹ به روش مشابه محاسبه می شوند. حال با استفاده از جملات $u_{16385} = 6, u_{16386} = 162, u_{16387} = 70, u_{16388} = 265$ واسطه پیکسل اول کانال سبز تصاویر سایه $SH_1, SH_2, \ldots, SH_n$ را با توجه به تساوی ۱۰ تولید می‌کند:

$$G_1^1 = g_1 - u_{16385} = 134 - 6 = 128 \bmod 257$$
$$G_2^1 = g_2 - u_{16386} = 132 - 162 = 227 \bmod 257$$
$$G_3^1 = g_3 - u_{16387} = 126 - 70 = 56 \bmod 257$$
$$G_4^1 = g_4 - u_{16388} = 122 - 256 = 123 \bmod 257$$

پیکسل های بعدی کانال سبز تصاویر سایه با توجه به تساوی ۱۰ به روش مشابه محاسبه می‌شوند. در نهایت واسطه با استفاده از جملات $u_{32769} = 93, u_{32770} = 218, u_{32771} = 98, u_{32772} = 2$ اولین پیکسل کانال آبی تصاویر سایه $SH_1, SH_2, \ldots, SH_n$ را با استفاده از تساوی ۱۱ می‌سازد:

$$B_1^1 = b_1 - u_{22769} = 115 - 93 = 22 \bmod 257$$
$$B_2^1 = b_2 - u_{22770} = 117 - 218 = 156 \bmod 257$$
$$B_3^1 = b_3 - u_{22771} = 111 - 98 = 13 \bmod 257$$
$$B_4^1 = b_4 - u_{22772} = 104 - 2 = 102 \bmod 257$$

پیکسل‌های بعدی کانال آبی تصاویر سایه به روش مشابه با توجه به تساوی ۱۱ محاسبه می‌شوند. واسطه چهار تصویر سایه $SH_1, \ldots, SH_4$ با ابعاد ۶۴ × ۶۴ را به‌ترتیب میان چهار شرکت‌کننده $P_1, \ldots, P_4$ توزیع می‌کند. برای بازسازی فرض کنید

چهار سهام‌دار $P_1,...,P_4$ تصاویر سایه $SH_1,\ldots,SH_4$ خود را به اشتراک گذاشته‌اند. مراحل بازسازی اولین بلوک چهار پیکسلی تصویر راز را توضیح می‌دهیم. مقدار پیکسل اول کانال قرمز تصاویر سایه به‌ترتیب $r_1=224, r_2=219, r_3=220, r_4=239$ است. بنابراین آن‌ها می توانند تمام جملات HLR را به یکی از سه روش زیر محاسبه کنند:

۱. استفاده از رابطه بازگشتی:

$$u_{4+i}=-253u_{3+i}-6u_{2+i}-253u_{i+1}-u_i\ (i\geq 1)$$

۲. حل دستگاه واندرموند زیر:

$$\begin{cases} A_1+A_2+A_3+A_4=224 \\ A_1+2A_2+4A_3+8A_4=219 \\ A_1+3A_2+9A_3+27A_4=220 \\ A_1+4A_2+16A_3+64A_4=239 \end{cases}$$

بنابراین اعداد $A_1=223, A_2=8, A_3=248, A_4=2$ به دست می‌آیند و در نتیجه رابطه بدیهی دنباله به‌صورت زیر است:

$$u_i=223+8i+24i^2+2i^3 \bmod 257$$

۳. درون‌یابی چندجمله‌ای:

$$u_i=p(i)=\sum_{j=1}^{4} r_j \sum_{k=1,k\neq j}^{4}\frac{i-k}{j-k}$$
$$=223+8i+248i^2+2i^3 \bmod 257$$

سپس شرکت‌کننده‌ها را به‌عنوان پیکسل‌های اولین بلوک چهارتایی $r_1=224, r_2=219, r_3=220, r_4=239$ کانال قرمز تصویر راز با ابعاد 128×128 قرار می‌دهند. مقدار پیکسل اول کانال سبز تصاویر سایه به‌ترتیب $G_1^1=128, G_2^1=227, G_3^1=56, G_4^1=123$ هستند؛ بنابراین عبارات زیر را محاسبه می‌کنند:

$$u_{16385}=223+8\times16385+248\times(16385)^2+2\times(16385)^3=6 \bmod 257$$
$$u_{16386}=223+8\times16386+248\times(16386)^2+2\times(16386)^3=162 \bmod 257$$
$$u_{16387}=223+8\times16387+248\times(16387)^2+2\times(16387)^3=70 \bmod 257$$
$$u_{16388}=223+8\times16388+248\times(16388)^2+2\times(16388)^3=256 \bmod 257$$
$$g_1=G_1^1+u_{16385}=128+6=134 \bmod 257$$
$$g_2=G_2^1+u_{16386}=227+162=132 \bmod 257$$
$$g_3=G_3^1+u_{16387}=56+70=126 \bmod 257$$
$$g_4=G_4^1+u_{16388}=123+256=122 \bmod 257$$

$g_1=134, g_2=132, g_3=126, g_4=122$ را به‌عنوان پیکسل‌های اولین بلوک چهارتایی کانال سبز تصویر راز قرار می‌دهند. در نهایت مقدار مؤلفه آبی پیکسل اول تصاویر سایه به ترتیب $B_1^1=22, B_2^1=156, B_3^1=13, B_4^1=102$ است. بنابراین شرکت‌کنندگان مقادیر زیر را محاسبه می‌کنند:

$$u_{32769}=223+8\times32769+248\times(32769)^2+2\times(32769)^3=93 \bmod 257$$
$$u_{32770}=223+8\times32770+248\times(32770)^2+2\times(32770)^3=218 \bmod 257$$
$$u_{32771}=223+8\times32771+248\times(32771)^2+2\times(32771)^3=98 \bmod 257$$
$$u_{32772}=223+8\times32772+248\times(32772)^2+2\times(32772)^3=2 \bmod 257$$

۴- نتایج تجربی

در این بخش نتایج شبیه‌سازی و آزمایش طرح تسهیم راز تصاویر رنگی بر مبنای *HLP* ارائه شده و نتایج به‌دست‌آمده از این آزمایش‌ها از دو منظر کیفیت تصاویر بازسازی شده و امنیت تصاویر سایه تولیدشده موردبررسی قرار گرفته است. به این منظور برای تحلیل نتایج به‌دست‌آمده از مقیاس‌های سنجش متداول برای طرح‌های تسهیم راز تصویری همچون ضریب همبستگی، *MSE* ، *PSNR* و *SSIM* برای سنجش کیفیت تصویر بازسازی شده و همچنین از آنتروپی، همبستگی پیکسل‌های مجاور، هیستوگرام، *UACI* و *NPCR* برای بررسی امنیت تصاویر سایه استفاده شده است. تمامی شبیه‌سازی‌ها در نرم‌افزار متلب 2019b، توسط کامپیوتر با پردازنده Core i7 2/2GH و رم ۶ گیگابایت انجام گرفته است.

۴-۱- کیفیت تصویر بازسازی شده

از ویژگی‌های مهم یک طرح تسهیم راز تصویری کیفیت بالای تصویر بازسازی شده و شباهت آن به تصویر راز است. برای بررسی کیفیت تصویر بازسازی شده از مقیاس‌های زیر برای سنجش شباهت تصاویر استفاده شده است:

- ضریب همبستگی: میزان تشابه دو تصویر را می‌توان با ضریب همبستگی[1] آن‌ها سنجید. فرض کنید p_1 و p_2 دو تصویر با N پیکسل باشند، ضریب همبستگی آن‌ها به‌صورت زیر اندازه‌گیری می‌شود:

$$corr=\frac{N\sum p_1p_2-(\sum p_1)(\sum p_2)}{\sqrt{(N\sum p_1^2-(\sum p_1)^2)(N\sum p_2^2-(\sum p_2)^2)}}$$

بنا به نامساوی کوشی شوارتز[2] مقدار تساوی بالا بین ۱- و ۱ است که مقدار ۱ به معنی یکسان بودن دو تصویر است. مقدار ۱- یعنی دو تصویر کاملاً مخالف هم هستند. همچنین مقادیر نزدیک به صفر نشان‌دهنده تفاوت بالای دو تصویر است. در جدول (۲) مقدار ضریب همبستگی تصویر راز و تصویر بازسازی شده در طرح ارائه شده ثبت شده است که برابر ۱ است و این یعنی بازسازی بدون نقص انجام شده است.

- میانگین مربع خطا(*MSE*):روشی آماری برای سنجش شباهت تصاویر است. فرض کنید S تصویر راز و R تصویر بازسازی شده با ابعاد $M\times N$ باشند در این صورت مقدار *MSE* به‌صورت زیر اندازه‌گیری می‌شود:

$$MSE=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(S(i,j)-R(i,j))^2$$

[1] Correlation coefficient
[2] Cauchy shcwartz inequality

بنا به تساوی بالا همواره مقدار MSE مثبت است و هر چه مقدار آن کمتر باشد تصویر بازسازی شده به تصویر راز شباهت بیشتری دارد و اگر مقدار آن برابر صفر باشد به این معنی است که دو تصویر یکسان هستند. با توجه به جدول (۲) مقادیر MSE به‌دست‌آمده همگی برابر صفر است.

pa نسبت سیگنال به نویز تصویر ($PSNR$): این مقیاس برای سنجش شباهت تصویر و کیفیت تصویر بازسازی شده است و مقدار آن بین صفر تا بی‌نهایت متغیر است. این نسبت به روش زیر محاسبه می‌شود:

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right)$$

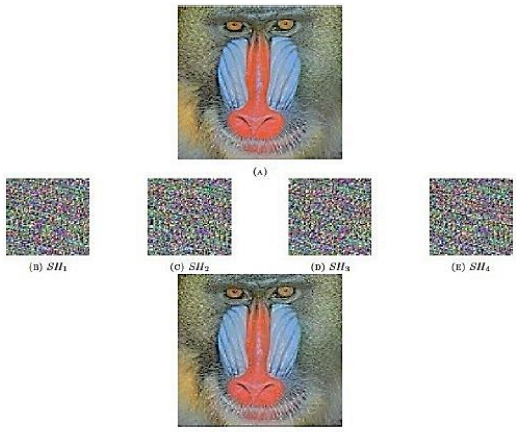
بنا بر تساوی بالا هر چه مقدار آن بزرگ‌تر باشد یعنی کیفیت تصویر راز بالاتر است. در واقع برای چشم انسان تفاوت دو تصویر با $30db < PSNR$ قابل‌تشخیص نیست [۶۱]. در جدول (۲) مشاهده می‌شود که مقادیر $PSNR$ طرح برابر بی‌نهایت است.

- شاخص تشابه ساختاری $(SSIM)$:

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

که در آن μ_x و μ_y مقدار میانه تراکم رنگ پیکسل‌ها در جهت افقی و عمودی و σ_x و σ_y مقدار واریانس تراکم رنگ پیکسل‌ها در جهت افقی و عمودی و σ_{xy} کوواریانس تراکم رنگ پیکسل‌ها است. مقدار $SSIM$ همواره کوچک‌تر یا مساوی یک است. این مقیاس در مقایسه با MSE و $PSNR$ کارآمدتر است زیرا تنها به‌صورت آماری شباهت تصاویر را نمی‌سنجد و بر اساس روشنایی و شفافیت نیز تصاویر را مقایسه می‌کند و ازاین‌جهت با دید چشم انسان تطابق بیشتری دارد. بالا بودن مقدار $SSIM$ نشان‌دهنده تشابه بالای دو تصویر است [۳۳] و در اینجا به معنی بالا بودن کیفیت تصویر استتار شده است. همان‌طور که مشاهده می‌کنید در جدول (۲) مشاهده می‌شود که مقدار $SSIM$ در آزمایش با هر دو تصویر لنا و بابون برای هر سه مؤلفه R، G و B برابر یک است. در نتیجه طرح ارائه شده بازسازی بدون نقص دارد. در شکل‌های (۳) و (۴) نتیجه پیاده‌سازی طرح $(۴,۴)$ روی تصاویر راز لنا و بابون قابل‌مشاهده است. تصاویر سایه کاملاً نویزگونه هستند و هیچ اطلاعاتی از راز را نشان نمی‌دهند. همچنین رازهای بازسازی شده کاملاً بدون نقص هستند.

شکل (۳). تصویر راز لنا، سایه‌ها و تصویر بازسازی شده



شکل (۴). تصویر راز بابون، سایه‌ها و تصویر بازسازی شده

جدول (۲). نتایج آزمایش کیفیت تصویر بازسازی شده

تصویر راز و بازسازی شده	مولفه	MSE	PSNR	SSIM	ضریب همبستگی
RL and L	R	۰	∞	۱	۱
	G	۰	∞	۱	۱
	B	۰	∞	۱	۱
RB and B	R	۰	∞	۱	۱
	G	۰	∞	۱	۱
	B	۰	∞	۱	۱

۴-۲- تحلیل آماری

در این بخش نتایج به‌دست‌آمده از آزمایش طرح تسهیم راز تصویری ارائه شده توسط مقیاس‌های هیستوگرام، آنتروپی و همبستگی پیکسل‌های مجاور مورد تحلیل آماری قرار گرفته است.

آنتروپی: یک روش برای سنجش احتمال قابل پیش‌بینی بودن اطلاعات است. فرمول آنتروپی اطلاعات شانون[1] به‌صورت زیر است:

$$E(m) = -\sum_{i=0}^{n-1} p(m_i) \times \log_2 p(m_i)$$

[1] Shanon

که در آن m نماد اطلاعات $p(m_i)$ احتمال پیشامد m_i و n تعداد کل حالاتی است که برای m ممکن است رخ دهد. دامنه طیف خاکستری در کامپیوتر [۰و۲۵۵] است پس $n=256$. هر چه مقدار آنتروپی تصویر بالاتر باشد به این معنی است که اطلاعات آن با احتمال پایین‌تری قابل پیش‌بینی می‌باشد[۶۲]. به‌طور طبیعی امکان پیش‌بینی اطلاعات در تصاویر نویزگونه از تصاویر عادی کمتر است و در نتیجه میزان آنتروپی آن‌ها بالاتر از تصاویر عادی است. در تسهیم راز تصاویر سایه باید حالت نویزگونه داشته باشند تا هیچ اطلاعاتی از تصویر راز افشا نکنند. همان‌طور که در تصاویر ۳ و ۴ مشاهده می‌شود تصاویر سایه تولیدشده در طرح ما کاملاً حالت نویزگونه دارند و هیچ‌گونه اطلاعاتی را راجع به تصویر راز افشا نمی کنند. بنابراین تولید تصاویر سایه با آنتروپی بالا یکی از مزیت‌های یک طرح SIS مناسب است زیرا احتمال پیش بینی شدن تصاویر سایه همچون تصاویر نویزگونه کم خواهد بود و در نتیجه اطلاعات تصویر راز را فاش نخواهند ساخت. بالاترین میزان آنتروپی ۸ است پس در یک طرح تسهیم راز تصویری مطلوب است میزان آنتروپی تصاویر سایه نزدیک به ۸ باشد. همان‌طور که در جدول ۳ مشاهده می‌کنید مقادیر آن‌ها همگی نزدیک به ۸ است و بنابراین از نظر آنتروپی با تصاویر رندوم تفاوتی ندارند.

جدول (۳). نتایج آنتروپی تصویر لنا و یک تصویر سایه‌اش در طرح (۴ و ۴)

B	G	R	Image
۷,۱۲۲۳	۷,۵۹۰۲	۷,۳۰۷۷	image Secret
۷,۹۵۰۴	۷,۹۵۲۱	۷,۹۴۷۷	SH_1
۷,۹۵۱۵	۷,۹۵۳۳	۷,۹۵۰۹	SH_2
۷,۹۵۰۸	۷,۹۴۴۴	۷,۹۴۶۵	SH_3
۷,۹۵۳۰	۷,۹۵۳۵	۷,۹۴۶۴	SH_4

$NPCR$ و $UACI$: محاسبه تعداد تغییر پیکسل ($NPCR$) و میانگین شدت تغییر یکپارچه تصاویر سایه ($UACI$) دو روش متداول برای تعیین رندوم بودن تصاویر سایه است. در واقع $NPCR$ و $UACI$ مقیاس‌هایی برای محاسبه میزان تفاوت دو تصویر هستند. $NPCR$ میزان رندوم بودن دو تصویر را مشخص می‌کند و $UACI$میزان تنوع شدت رنگ در پیکسل‌های دو تصویر را اندازه‌گیری می‌کند. روش محاسبه این دو نسبت برای دو تصویر با Im_1 و Im_2 با $M \times N$ ابعاد به‌صورت زیر است:

$$NPCR = \frac{\sum_{i,j} D_{ij}}{M \times N} \times 100\% \quad D_{ij} = \begin{cases} 1 \; if \; \mathrm{Im}_1(i,j) \neq \mathrm{Im}_2(i,j) \\ 0 \; if \; \mathrm{Im}_1(i,j) = \mathrm{Im}_2(i,j) \end{cases}$$

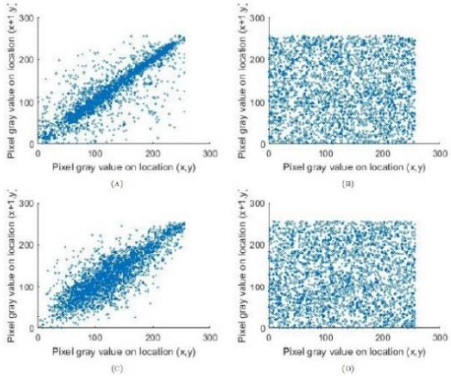
$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|\mathrm{Im}_1(i,j) - \mathrm{Im}_2(i,j)|}{255}\right] \times 100\%$$

نتایج این دو نسبت در جدول (۴) ثبت شده‌اند. مقدار $NPCR$ نشان‌دهنده تفاوت حدوداً ٪ ۹۹،۵ پیکسل‌های هر دو تصویر راز با هم است. همچنین میزان $UACI$ برای هر کانال رنگ بیشتر از ٪ ۰،۲۳ است. بنا به [۶۳] مقادیر قابل قبولی از جهت تشابه تصاویر سایه به تصاویر تصادفی دارند.

جدول (۴). نتایج NPCR و UACI تصویر لنا و تصاویر سایه‌اش

SH_2, SH_3	SH_1, SH_2		تصویر لنا
۰,۹۹۵۳۶۱۳۲۸۱	۰,۹۹۵۸۴۹۶۰۹۳	R	
۰,۹۹۵۳۶۱۳۲۸۱	۰,۹۹۵۸۴۹۶۰۹۳	G	NPCR
۰,۹۹۵۶۰۵۴۶۸۷	۰,۹۹۸۲۹۱۰۱۵۶	B	
۰,۳۵۳۰۲۷۳۴۳۷	۰,۴۰۱۱۰۴۳۲۸۱	R	
۰,۳۴۸۱۶۱۷۶۴۷	۰,۴۰۱۱۰۴۳۲۸۱	G	UACI
۰,۳۴۸۵۵۵۲۶۱۹	۰,۳۵۳۹۶۲۷۳۷۴	B	

• همبستگی پیکسل‌های مجاور[1]: به‌طور معمول در تصاویر با معنی اغلب پیکسل های مجاور از نظر مقدار بسیار به هم نزدیک هستند و ضریب همبستگی بالایی دارند. این همبستگی در جهات افقی، عمودی و یا قطری می تواند وجود داشته باشد. در تصاویر رندوم این میزان کاهش می‌یابد پس در یک طرح SIS قابل‌قبول همبستگی پیکسل‌های مجاور در تصاویر سایه ایجاد شده باید نزدیک به صفر باشد. ۳۰۰۰ جفت از نقاط مجاور در تصویر راز لنا و همچنین یکی از تصاویر سایه آن در شکل (۳) را برای محاسبه مقدار ضریب همبستگی‌شان به‌طور تصادفی انتخاب شده‌اند. همین روند برای تصویر راز بابون و یکی از تصاویر سایه آن در شکل (۴) نیز انجام شده است. در شکل (۵) نمودار همبستگی پیکسل‌های مجاور تصویر سایه هر دو تصویر راز به خوبی پراکندگی نقاط، که به معنی پایین بودن همبستگی جفت پیکسل ها در آن‌ها و تصادفی بودن تصاویر سایه است، قابل‌مشاهده است.



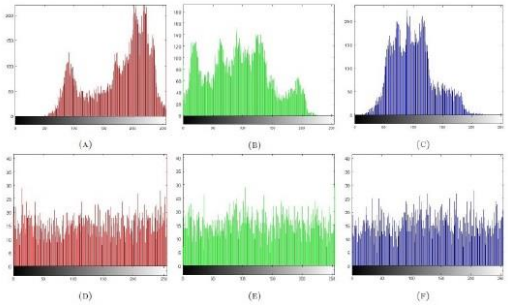
شکل (۵). به ترتیب نمودار همبستگی پیکسل‌های مجاور در تصویر لنا و تصویر سایه‌اش و تصویر بابون و تصویر سایه‌اش

1. Correlation of adjacent pixels

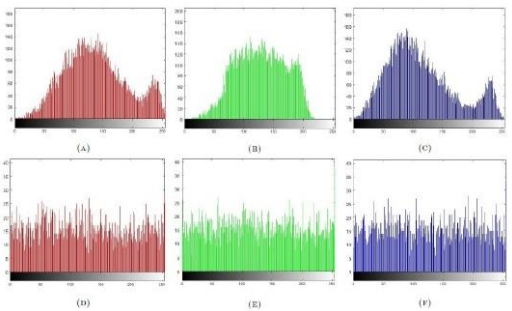
جدول (۵). مقایسه‌ی طرح ارائه شده با کارهای قبلی

طرح	راهکار اصلی	بازسازی بدون نقص	آستانه	اندازه تصویر سایه	پیش پردازش	پیمانه	پردازش یک مرحله‌ای
[۴۴]	پولی	مشروط	$(2,n)$	۱	خیر	۲	خیر
[۵۷]	چندجمله‌ای	خیر	(t,n)	$\frac{1}{t}$	بله	۲۵۱	خیر
[۵۸]	چندجمله‌ای	بله	(t,n)	$\frac{t-1}{b}+\frac{1}{t-1}$	بله	بین $۲^۸$ و $۲^{۸b}$	بله
[۵۸]	چندجمله‌ای	خیر	(t,n)	$\frac{1}{t-1}$	بله	بین $۲^{۲۳}$ و $۲^{۲۳b}$	بله
[۵۹]	چندجمله‌ای	بله	(t,n)	$\frac{1}{t-1}$	خیر	بزرگ‌تر از $۲^{۲۳}$	بله
طرح ما	HLR	بله	(n,n)	$\frac{1}{n}$	خیر	۲۵۷	بله

● هیستوگرام: یک روش تحلیل آماری تصاویر استفاده از هیستوگرام فراوانی رنگ‌ها است. طیف خاکستری‌رنگ پیکسل‌ها در کامپیوتر به‌صورت هشت بیتی ذخیره می‌شود، پس دامنه خاکستری رنگ پیکسل ها در کامپیوتر[۰،۲۵۵] است. یکی از ویژگی‌های یک طرح تسهیم راز تصویری ایده‌آل تولید تصاویر راز با هیستوگرام یکنواخت است به‌طوری‌که از هیستوگرام یک تصویر رندوم قابل‌تمایز نباشد و در نتیجه هیچ‌گونه اطلاعاتی راجع به تصویر راز افشا نکند. هیستوگرام مؤلفه‌های RGB تصاویر رنگی لنا و بابون به همراه یک نمونه از تصاویر سایه‌شان، به‌طور جداگانه، به ترتیب در شکل‌های (۶) و (۷) رسم شده‌اند. همان‌طور که در هر دوی این تصاویر مشاهده می‌کنید، هیستوگرام‌های هر سه مؤلفه رنگ تصاویر سایه رفتاری یکنواخت دارند و طرح از این نظر موردقبول می‌باشد.



شکل (۶). هیستوگرام تصویر لنا و یکی از تصاویر سایه آن



شکل (۷). هیستوگرام تصویر بابون و یکی از تصاویر سایه آن

۴-۳- تحلیل امنیت

در این بخش امنیت طرح با آزمایش شرط آستانه بررسی شده است. در واقع نشان داده شده که برای یک طرح تعداد $n-1$ یا کمتر از شرکت‌کنندگان نمی‌توانند تصویر راز را بازسازی کنند و یا هر نوع اطلاعاتی راجع به آن به دست بیاورند. فرض کنید $SH_1,...,SH_{n-1}$ تصاویر سایه برای بازسازی راز باشند. شرکت‌کنندگان به سه روش می‌توان عملیات بازسازی را انجام دهند:

- ماتریس واندرموند: برای به دست آوردن n مجهول تنها $n-1$ تساوی موجود است و بنابراین جواب یکتا قابل‌محاسبه نیست. در نتیجه شرکت‌کنندگان نمی‌توانند رابطه صریح HLR را به دست بیاورند.
- درون‌یابی چندجمله‌ای: برای درون‌یابی یک چندجمله‌ای درجه $n-1$ به n جفت از نقاط نیاز است در نتیجه از این روش نیز رابطه صریح HLR قابل‌محاسبه نمی‌باشد.
- رابطه بازگشتی: با توجه به عبارت رابطه بازگشتی به‌وضوح برای به‌دست آوردن هر عضو HLR نیاز به داشتن n جمله متوالی از آن است و با $n-1$ عضو از آن نمی‌توان اعضای دیگر را محاسبه کرد.

۵- مقایسه با کارهای قبلی

در این بخش طرح SIS ارائه شده در این مقاله با تحقیقات گذشته مقایسه شده است. همچون تصاویر خاکستری طرح‌های تسهیم راز تصاویر رنگی موجود در دو دسته $PSIS$ و VSS قرار دارند، اگرچه تحقیقات بسیار کمتری در این زمینه نسبت به تصاویر خاکستری انجام شده است. در زمان نگارش این مقاله چهار طرح $PSIS$ موجود است [۴۴، ۵۷، ۵۸ و ۵۹]. در ادامه

نتایج مقایسه طرح ارائه شده و طرح‌های پیشین بیان شده است. نتایج این مقایسه‌ها در جدول (۵) قابل‌مشاهده است. در طرح (n,n) مقاله [۵۷] از فشرده سازی *GSBTC* برای تصویر راز استفاده شده است به‌طوری که هر بلوک شامل m^2 پیکسل را با نسبت $\frac{24m^2}{m^2+8}$ فشرده می‌سازد. اندازه تصاویر سایه تولیدشده در این طرح $\frac{1}{t}$ اندازه تصویر راز و بازسازی آن نقص دار است. در مقاله [۵۸]تصویر راز ابتدا به‌صورت یک رشته b-بایتی در نظر گرفته می‌شود. p عدد اول میدان استفاده شده در این مقاله است که $2^8 < p < 2^{8b}$ برای تصاویر خاکستری و $2^{24} < p < 2^{24b}$ برای تصاویر رنگی است. بازسازی این طرح نقص دار است اگرچه استفاده از عدد اول بزرگ‌تر موجب بالا رفتن کیفیت بازسازی می‌شود ولی از طرف دیگر بار محاسبات را افزایش می‌دهد. طرح [۴۴] *PSIS* پیش‌رونده بر مبنای عملیات بولی است که اندازه تصاویر سایه‌اش برابر اندازه تصویر راز است .همچنین این طرح تنها محدود به حالت آستانه ای $(2,n)$است. در [۵۹] هر پیکسل تصویر راز رنگی *RGB* به‌صورت یک سه‌تایی در $\mathbb{Z}_{۲۵۶} \times \mathbb{Z}_{۲۵۶} \times \mathbb{Z}_{۲۵۶}$ نظر گرفته می‌شود. سپس برای ایجاد امکان پردازش یک مرحله‌ای در تسهیم راز از نگاشت دوسویی[1] $\varphi: \mathbb{Z}_{۲۵۶} \times \mathbb{Z}_{۲۵۶} \times \mathbb{Z}_{۲۵۶} \rightarrow \mathbb{Z}_p$ که در آن p یک عدد اول بزرگ‌تر از 2^{24}است و $\varphi(r,g,b) = [256^2 r + 256g + b] \bmod p$ استفاده می‌شود. برای آستانه (t,n)اندازه تصاویر سایه $\frac{1}{t-1}$ تصویر راز است و همچنین بازسازی آن بی‌نقص است. برای جلوگیری از مشکل اثر تهمانده[2]تصویر راز در تصاویر سایه در [۵۷ و ۵۸] از جایگشت پیش از عملیات تسهیم راز استفاده شده تا همبستگی بین پیکسل های تصویر راز از بین برود. این عملیات باعث افزایش بار محاسبات می‌شود. همچنین این به معنا است که امنیت این طرح‌ها نه بر مبنای تسهیم راز بلکه وابسته به عملیات پیش پردازش است. در [۵۹] نیازی به پیش پردازش نیست اما نگاشت هر پیکسل پیش از انجام تسهیم راز انجام محاسبات اضافی را تحمیل می‌کند. استفاده از اعداد اول بسیار بزرگ در [۵۸ و ۵۹] محاسبات را زمان‌بر می‌سازد. طرح ارائه شده ما با استفاده از دنباله *HLR* یک طرح *PSIS* با بازسازی بدون نقص (n,n) است که اندازه تصاویر سایه آن $\frac{1}{n}$تصویر راز است که نسبت به طرح‌های بدون نقص مشابه کاهش یافته است. همچنین طرح ما نیازی به پیش‌پردازش برای تأمین امنیت ندارد که از نظر محاسباتی آن را بهینه می سازد. از طرف دیگر استفاده از روابط خطی به‌جای چندجمله‌ای‌ها محاسبات طرح ما را نسبت به طرح‌های مشابه ساده‌تر می‌کند.

1. Bijection
2. Residual Image Effect

۶- نتیجه‌گیری

در این مقاله یک طرح *PSIS* آستانه ای (n,n) بدون نقص برای تصاویر رنگی ارائه شد که در آن برخی از ویژگی‌های مهم نسبت به طرح‌های *PSIS* مشابه قبلی بهبود یافته است:

۱- اندازه تصاویر سایه نسبت به طرح‌های بدون نقص قبلی کوچک‌تر است.

۲- برای تأمین امنیت طرح نیازی به عملیات اضافی پیش از تسهیم راز نیست.

۳- استفاده از میدان عدد اول ۲۵۷ ، سرعت محاسبات را افزایش داده است.

۴- استفاده از روابط خطی به‌جای چندجمله‌ای محاسبات را آسان‌تر کرده است.

در کارهای آینده قصد داریم برای عدم جلب توجه دشمنان از نهان‌نگاری سایه‌های این طرح تسهیم راز در تصاویر معمولی استفاده کنیم و طرحی با سایه های معنادار ارائه نماییم. همچنین قصد داریم آستانه طرح را کاهش دهیم.

۶- مراجع

[1] T. Alkhodaidi, A. Gutub, Trustworthy Target Key Alteration Helping Counting-Based Secret Sharing Applicability, Arabian Journal for Science and Engineering, vol. 45, pp. 3403-3423, 2020.

[2] T. Bhattacharjee, S. P. Maity, Sh.Ra_ul Islam, Hierarchical Secret Image Sharing Scheme in Compressed Sensing, Signal Processing: Image Communication, vol. 61, pp. 21-32, 2018.

[3] Y.-Ch. Chen, T.-H. Hung, S.-H. Hsieh, Ch.-W. Shiu, A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms, IEEE Transactions on Information Forensics and Security, vol. 14, pp. 3332-3343, 2019.

[4] Y. Fu, P. Kong, H. Yao, Z. Tang, C. Qin, Effective reversible data hiding in encrypted image with adaptive encoding strategy, Inf. Sci. vol. 494, pp. 21-36, 2019.

[5] A. Gutub, Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons, Arabian Journal for Science and Engineering, vol. 45, pp. 2631-2644, , 2020.

[6] A. Gutub, M. Al-Ghamdi, Hiding shares by multimedia image steganography for optimized counting-based secret sharing, Multimedia Tools and Applications, vol. 79, pp. 7951-7985, 2020.

[7] X.Li, D.Xiao, H.Mou, R.Zhang, A Veri_able Secret Image Sharing Scheme Based on Compressive Sensing, Wuhan University Journal of Natural Sciences, vol. 23, pp. 219-224, 2018.

[8] P.Singh, B.Raman, Reversible data hiding based on Shamirs secret sharing for color images over cloud, Information Sciences, vol. 422, pp. 77-97, 2018.

[9] C.C. Thien, J.C. Lin, Secret image sharing, Computers & Graphics, vol. 26 (5), pp. 765-770, 2002.

[10] D.-Sh. Tsai, G. Horng, T.-H. Chen, Y.-T. Huang, A novel secret image sharing scheme for true-color images with size constraint, Information Sciences, vol. 179(19) pp. 3247-3254, 2009.

[11] X. Wang, L. Feng , H. Zhao, Fast image encryption algorithm based on parallel computing system, Inf. Sci., vol. 486, pp. 340-358, 2019.

[12] X. Wang, S. Gao, Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensorproduct theory, Information Sciences, vol. 507, pp. 16-36, 2020.

[13] B. Xiao, J.Luo, X. Bi, W. Li, B. Chen, Fractional discrete Tchebyshev moments and their applications in image encryption and watermarking, Information Sciences, vol. 516, pp. 545-559, 2020.

[14] X.Yan, Y. Lu, L.Liu, and X. Song, Reversible Image Secret Sharing, IEEE Transactions on Information Forensics and Security, vo. 15, pp. 3848-3858, 2020.

[15] J. Zarepour-Ahmadabadi, M.S. Ahmadabadi, A. Latif, An adaptive secret image sharing with a new bitwise steganographic property, Information Sciences, vol. 369, pp. 467-480, 2016.

[16] Moradi, Meysam, Ahmadi Pari, Mehdi. (2017). "A proposed algorithm for encryption of gray images by patterning Bence interconnection networks and map Logistic chaos", Electronic and Cyber Defense, Volume 6, No. 1, pp. 37-46, (In Persian).

[17] Sham Alizadeh, Mohammad Ali. (2019). "Designing a hybrid image encryption algorithm based on game theory", Electronic and Cyber Defense, Volume 8, No. 1, pp. 133-145, (In Persian).

[18] M. Naor, A. Shamir, Visual Cryptography, Workshop on the Theory and Application of of Cryptographic Techniques, pp. 1-12, 1995.

[19] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theor Comput Sci., vol. 250 (1), pp. 143-161, 2001.

[20] Y.-C. Chen, D.-S. Tsai, G. Horng, A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography, J. Vis. Commun. Image. Represent., vol. 23 (8), pp. 1225-1233, 2012.

[21] Y. Cheng, Z. Fu, B. Yu, Improved Visual Secret Sharing Scheme for QR Code Applications, IEEE Transactions on Information Forensics and Security,vol. 13(9), pp. 2393-2403, 2018.

[22] M. Sasaki, Y. Watanabe, Visual Secret Sharing Schemes Encrypting Multiple Images, IEEE Transactions on Information Forensics and Security, vol. 13(2), pp. 356-365, 2018.

[23] D.R.Stinson, Visual cryptography and threshold schemes, IEEE Potentials, vol. 18, pp. 13-16, 1999.

[24] X. Yan, S. Wang, X. Niu, C.-N. Yang, Random grid-based visual secret sharing with multiple decryptions, Journal of Visual Communication and Image Representation, vol. 26, pp. 94-104, 2015.

[25] T.-H.Chen, X.-W. Wu, Multiple secret image sharing with general access structure, Multimedia Tools and Applications, vol. 79, pp. 13247-13265, 2020.

[26] W. Ding, K. Liu, X. Yan, L. Liu, Polynomial-Based Secret Image Sharing Scheme with Fully Lossless Recovery, Int. J. Digit. Crime Forens., vol. 10, pp. 120-136, 2018.

[27] R.Z. Wang, C.H. Su, Secret image sharing with smaller shadow images, Pattern Recognition Lett. vol. 27, pp. 551-555, 2006.

[28] K. Wu, A secret image sharing scheme for light images, EURASIP Journal on Advances in Signal Processing, no. 49, pp. 1-5, 2013.

[29] L. Xiong, X. Zhong, Chi.-N. Yang, X. Han, Transform Domain-Based Invertible and Lossless Secret Image Sharing With Authentication, IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2912-2925, 2021.

[30] A. Shamir, How to share a secret, Communications of ACM., vol.22(11), pp. 612-613, 1979.

[31] C.-C.Lin, W.-H.Tsai, Secret image sharing with steganography and authentication, J. Syst. Softw. vol. 73(3), pp. 405-414, 2004.

[32] X.Wu, C.-N.Yang. Invertible secret image sharing with steganography and authentication for AMBTC compressed images. Signal Processing: Image Communication, vol. 78, pp. 437-447, 2019.

[33] X.Wu, C.N.Yang, Partial reversible AMBTC-based secret image sharing with steganography, Digit Signal Process vol. 93, pp. 22-33, 2019.

[34] X.Yan, Y.Lu, and L.Liu, General Meaningful Shadow Construction in Secret Image Sharing. IEEE Access, vol. 6, pp. 45246-45255, 2018.

[35] X.Yan, Y. Lu, L.Liu, and D.Ma, Image Secret Sharing Construction for General Access Structure with Meaningful Share. IJDCF, vol. 10(3), pp. 66-67, 2018.

[36] C.Yang, T.Chen, K.Yu, C.Wang, Improvements of image sharing with steganography and authentication,The Journal of Systems and Software, vol. 80, pp. 1070-1076, 2007.

[37] S.Charoghchi, S.Mashhadi, Three (t; n)-secret image sharing schemes based on homogeneous

linear recursion, Information Sciences, vol. 552, pp. 220-243, 2021.

[38] C.-C.Chen, Essential Secret Image Sharing Scheme with Equalsized Shadows Generation, Journal of Visual Communication and Image Representation, vol. 52, pp. 143-150, 2018.

[39] P. Li and Z.Liu, An Improved Essential Secret Image Sharing Scheme with Smaller Shadow Size. Int. J. Digit. Crime For., vol. 10(3), pp. 78-94, 2018.

[40] P.Li, Z.Liu and C.-N.Yang, A Construction Method of (t; k; n)-essential Secret Image Sharing Scheme. Signal Processing: Image Communication, vol.65, pp. 210-220, 2018.

[41] Z.Wu, Y.-N.Liu, D.Wang, C.-N.Yang, An Efficient Essential Secret Image Sharing Scheme Using Derivative Polynomial, Symmetry, vol. 11(1), pp. 69, 2019.

[42] C.-N.Yang, P.Li, C.-C.Wu, S.-R.Cai, Reducing Shadow Size in Essential Secret Image Sharing by Conjunctive Hierarchical Approach, Signal Processing: Image Communication, vol. 31, pp. 1-9, 2015.

[43] Y.-X.Liu, C.-N.Yang, S.-Y.Wu, and Y.-S.Chou, Progressive (k; n) Secret Image Sharing Schemes Based on Boolean Operations and Covering Codes, Signal Processing: Image Communication, vol. 66, pp. 77-86, 2018.

[44] H.Prasetyo and C.H.Hsia, Lossless progressive secret sharing for grayscale and color images, Multimedia Tools and Applications, vol. 78(17), pp. 24837-24862, 2019.

[45] X.Yan, Y.Lu, L.Liu, A general progressive secret image sharing construction method, Signal Processing: Image Communication, vol. 71, pp. 66-75, 2019.

[46] R.-Z.Wang and S.-J.Shyu, Scalable Secret Image Sharing, Signal Processing: Image Communication, vol. 22(4), pp. 363-373, 2007.

[47] S.Dutta, A.Adhikari and S.Ruj, Maximal contrast color visual secret sharing schemes, Designs, Codes and Cryptography, vol. 87(7), pp. 1699-1711, 2019.

[48] R.Lukac and K.N.Plataniotis, A color image secret sharing scheme satisfying the perfect reconstruction property, IEEE 6th Workshop on Multimedia Signal Processing, pp. 351-354, 2004.

[49] R. Lukac, K. N. Plataniotis, B. Smolka and A. N. Venetsanopoulos, A new approach to color image secret sharing, 2004 12th European Signal Processing Conference, pp. 1493-1496, 2004.

[50] S.J.Shyong, Efficient visual secret sharing scheme for color images, Pattern Recognition, Vol. 39(5), pp. 866-880, 2006.

[51] M.Karolin and D.T.Meyyapan, RGB based secret sharing scheme in color visual cryptography. International Journal of Advanced Research in Computer and Communication Engineering, vol. 4(7), 2015.

[52] D.C.Lou, H.H.Chen, H.C.Wu and C.S.Tsai, A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares, Displays, vol. 32(3), pp. 118-134, 2011.

[53] D.Wang, F.Yi, X.Li, Probabilistic visual secret sharing schemes for grey-scale images and color images, Information Sciences, vol. 181(11), pp. 2189-2208, 2011.

[54] Y.C.Hou, Z.Y.Quan, C.F.Tsai, and A.Y.Tseng, Block-based progressive visual secret sharing, Information Sciences, vol. 233, pp. 290-304, 2013.

[55] H.Luo, F.Yu, J.S.Pan and Z.M.Lu, Robust and progressive color image visual secret sharing cooperated with data hiding, 2008 Eighth International Conference on Intelligent Systems Design and Applications, Vol. 3, pp. 431-436, 2008.

[56] L. Bai, A Reliable (k; n) Image Secret Sharing Scheme, 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 31-36, 2006.

[57] C.C.Chang, C.C.Lin, C.H.Lin and Y.H.Chen, A novel secret image sharing scheme in color images using small shadow images, Information Sciences, vol. 178(11), pp. 2433-2447, 2008.

[58] M.Ghebleh and A.Kanso, A novel secret image sharing scheme using large primes, Multimedia Tools and Applications, vol. 77(10), pp. 11903-11923, 2018.

[59] M.K.Sardar and A.Adhikari, A new lossless secret color image sharing scheme with small shadow size, Journal of Visual Communication and Image Representation, vol. 68, pp.102-768, 2020.

[60] M. Hadian, S. Mashhadi, New efficient and practical veri_able multi-secret sharing schemes, Information Sciences, vol. 178 (9), pp. 2262-2274, 2008.

[61] K. Kyriakopoulos, D. J. Parish, A live system for wavelet compression of high speed computer network measurements, in Proceedings of the 8th International Conference on Passive and Active Network Measurement, pp. 241–244, 2007.

[62] S. Vajapeyam, Understanding Shannon's Entropy metric for Information, 2014.

[63] Y.Wu, J.P.Noonan, S.Agaian, NPCR and UACI Randomness Tests for Image Encryption, Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), vol. 1(2), pp. 31–38, 2011.