بیست و ششمین کنفرانس اپتیک و
فوتونیک ایران و دوازدهمین کنفرانس
مهندسی و فناوری فوتونیک ایران،
دانشگاه خوارزمی،
تهران، ایران.
۱۶-۱۵ بهمن ۱۳۹۸

رمزنگاری براساس تصویربرداری گوست محاسباتی جاروبی

سجاد رجبی قلعه[۱]، سهراب احمدی کندجانی[۱و۲] و رضا خردمند[۱و۲]

[۱]پژوهشکده فیزیک کاربردی و ستاره شناسی دانشگاه تبریز ، بلوار ۲۹ بهمن دانشگاه تبریز، تبریز

[۲]گروه فوتونیک و فناوری پلاسما دانشکده فیزیک، بلوار ۲۹ بهمن دانشگاه تبریز، تبریز

چکیده - اخیرا روش جدیدی در تصویربرداری گوست محاسباتی بنام تصویربرداری گوست محاسباتی جاروبی معرفی شده است. در این روش با اعمال دو الگوی کاتوره‌ای جاروبی سطری و ستونی، تصویر بدست می‌آید که نتایج حاصل از این کار به صورت تئوری و تجربی ارائه شده است. در این کار، از این روش برای رمزنگاری اطلاعات استفاده شده است. در روش جاروبی، عملگر بین این دو تصویر به عنوان کلید رمزنگاری خصوصی و تصاویر حاصل از سطر و ستون به عنوان کلید عمومی در نظر گرفته شده است. با اعمال چهار عمل اصلی بر دو تصویر سطری و ستونی بدست آمده از نتایج تئوری و تجربی، مشاهده می‌شود که با لورفتن ۱۰۰٪ اطلاعات بازهم نمی‌توانند به اطلاعات موردنظر دست یابند. همچنین با در نظر گرفتن سیستم رمزنگاری متقارن، فقط تصاویر سطری و ستونی بدست می‌آیند. در نتیجه می توان براحتی با این روش اطلاعات خود را برای کاربر موردنظر فرستاد حتی بدون اینکه از قبل اطلاعات رمزگذاری شوند.

کلید واژه- تصویربرداری گوست محسباتی جاروبی، الگوهای رندوم جاروبی، رمزنگاری.

Encryption based on sweeping computational ghost imaging

Sajjad Rajabi-Ghaleh[1], Sohrab Ahmadi-Kandjani[1, 2], and Reza Kheradmand[1, 2]

[1]Research Institute for Applied Physics and Astronomy, Tabriz, 29 Bahman Blvd, university of Tabriz.

[2]Photonics and plasmonics technology group, Faculty of Physics, Tabriz, 29 Bahman Blvd, university of Tabriz.

Abstract- In this paper we introduce new method for computational ghost imaging (CGI). This method call sweeping computational ghost imaging (SCGI). By introducing row and column sweep speckle patterns that was illuminated on the object, final image are retrieved via cross product of row and column matrices from images that are reconstructed with row and column sweep speckle patterns. Results of this method was performed both theoretical and experimental. This method was used for data encrypt by symmetric and asymmetric systems. In the symmetric, four main actions and select row and column of images are as private key. In the asymmetric, reconstructed images of row and column sweep speckle patterns and four main actions are as public and private keys, respectively. Because of final image reconstructed by cross product operator, therefore was used four main actions for decrypt of information. Experimental and simulation results show that eavesdrop 100 percentage of data transfer, users couldn't achieved basic information. In result, this method provide full security for data transfer between two users.

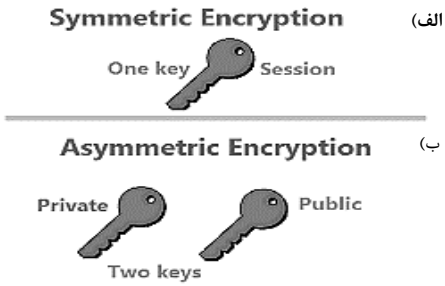
Keywords: Encryption, speckle pattern, and sweeping computational ghost imaging

۱. مقدمه

اخیرا، توسعه ارتباطات نیازمند رمزنگاری بر روی اطلاعات ارسالی است تا اینکه اطلاعات لو نروند. در این حالت به جای ارسال داده‌های اصلی به کاربر موردنظر از داده‌های ناخوانا استفاده می‌شود. اولین رمزنگاری اطلاعات در سال ۱۹۸۰ گزارش شده است [۱]. رمزنگاری در حالت کلی به دو صورت رمزنگاری متقارن و نامتقارن انجام می‌شود. در حالت متقارن، فقط یک کلید رمزنگاری وجود دارد که آن هم فقط در اختیار دو کاربر فرستنده و گیرنده است. اما در حالت نامتقارن، دو کلید رمزنگاری وجود دارد که یکی از آنها به عنوان کلید رمزنگاری است که در اختیار همه قرار دارد (کلید عمومی) و دیگری کلید رمزگشایی (کلید خصوصی) است که در اختیار کاربرهای فرستنده و گیرنده است [۲] شکل ۱.

تصویربردای گوست (GI) یکی از جدیدترین روش‌های تصویربرداری است که از دو بازوی مجزا تشکیل شده است، باریکه خروجی از منبع به دو بازوی مجزا تقسیم می‌شود. در یکی از بازوها، باریکه به طور مستقیم به یک آشکارساز آرایه‌ای به نام CCD یا CMOS می‌رسد، که اطلاعات فضایی باریکه را ثبت می‌کند، که این بازو به بازوی مرجع معروف است و در بازوی دیگر (بازوی جسمی)، باریکه ابتدا به جسم برخورد می‌کند و شدت نور عبوری/انعکاسی از آن به آشکارساز بوکت (تک‌پیکسل) می‌رسد و آن را اندازه‌گیری می‌کند [۳-۵]. سپس شاپیرو [۶] تصویربرداری گوست محاسباتی را ارائه کرد که در آن، بازوی مرجع حذف شده است و فقط با استفاده از بازوی جسمی، تصویر بازسازی می‌شود. در این کار نیز با استفاده از چیدمان معرفی شده در [۵]، نتایج تئوری و تجربی تصویربرداری گوست محاسباتی جاروبی [۷] برای رمزنگاری داده‌ها استفاده شده است.

با معرفی تصویربرداری گوست و رمزنگاری نوری با استفاده از آن، داده‌ها با امنیت و سرعت بالا و حجم کم ارسال می‌شوند [۸-۱۱].



شکل ۱: سیستم رمزنگاری متقارن (الف) و نامتقارن (ب).

در این کار، داده‌ها با استفاده از دو سیستم رمزنگاری متقارن و نامتقارن در تصویربرداری گوست محاسباتی جاروبی رمزنگاری شده است.

۲. روش محاسباتی

در تصویربرداری گوست محاسباتی شدت بازوی جسمی با استفاده از آشکارساز بوکت به وسیله رابطه زیر بدست می‌آید [۱۲]:

$$B_r = \int dxdy I_r(x,y) T(x,y) \qquad (۱)$$

که، $I(x,y)$ و $T(x,y)$ به ترتیب شدت میدان فرودی و تابع جسم را مشخص می‌کنند که $I(x,y)$ نیز با رابطه زیر بدست می‌آید:

$$I_r = \left| E^{(in)} e^{i\varphi_r(x,y)} \right| \qquad (۲)$$

در نهایت، تصویر با استفاده از رابطه همبستگی مرتبه دوم بین دو شدت، بدست می‌آید:

$$G(x,y) \equiv \frac{1}{N}\sum_{r=1}^{N}\left(B_r - \langle B\rangle\right) I(x,y) = \langle BI(x,y)\rangle - \langle B\rangle\langle I(x,y)\rangle$$

(۳)

که در آن، $\langle . \rangle$ میانگین آنسامبلی و N تعداد اندازه‌گیری‌ها را نشان می‌دهند.

برای بررسی میزان امنیت بین تصاویر رمزنگاری شده تحت حمله‌های متفاوت از $NPCR$ استفاده شده است که برای اولین بار در سال ۲۰۰۴ مطرح شده است[۱۳]:

$$D(i,j)=\begin{cases}0, if\ C^1(i,j)=C^2(i,j)\\1, if\ C^1(i,j)\neq C^2(i,j)\end{cases} \quad (۴)$$

$$NPCR: N\left(C^1,C^2\right)=\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{D(i,j)}{T}\times 100 \quad (۵)$$

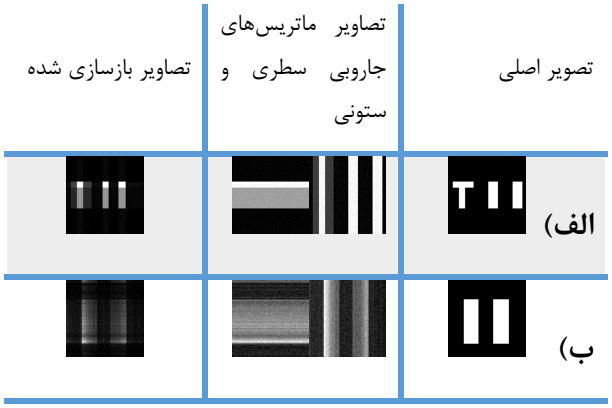
نتایج $NPCR$ برای نتایج تجربی و شبیه‌سازی در شکل۳ آورده شده است. مقادیر ۱و۰ به ترتیب بالاترین و پایین‌ترین امنیت را نشان می‌دهند.

در تصویربرداری گوست محاسباتی جاروبی، دو نوع الگوی کاتوره‌ای تولید می‌شود که الگوهای کاتوره‌ای جاروبی سطری و ستونی نامیده شده‌اند. در الگوی جاروبی سطری، یک ستون از ماتریس و در الگوی جاروبی ستونی، یک سطر از ماتریس نسبت به مقادیر پس‌زمینه‌اش دارای شدت زیادتر است و این دو ماتریس جسم را اسکن می‌کنند و تصاویر حاصل از هر دو با استفاده از رابطه ۳ بدست می‌آیند سپس یک سطر از تصویر ماتریس جاروبی سطری و یک ستون از تصویر ماتریس جاروبی ستونی انتخاب و با استفاده از عملگر ضرب خارجی، تصویر نهایی بازسازی می‌شود.

رمزنگاری انجام شده با استفاده از روش تصویربرداری گوست محاسباتی جاروبی در دو سیستم رمزنگاری متقارن و نامتقارن انجام شده است و نتایج نشان می‌دهند که اطلاعات با امنیت بسیار بالا فرستاده می‌شوند.

۳. نتایج تئوری و تجربی

در روش تصویربرداری گوست محاسباتی جاروبی، ابتدا ماتریس جاروبی سطری، و سپس ماتریس جاروبی ستونی جسم را اسکن کرده و تصویر حاصل از آنها بازسازی می‌شوند و در نهایت با انتخاب یک سطر از تصویر حاصل از ماتریس جاروبی سطری و یک ستون از تصویر ماتریس جاروبی ستونی و با حاصل‌ضرب خارجی بین این دو ماتریس، تصویر نهایی بازسازی می‌شود. در این کار برای نتایج تئوری و تجربی یک ماتریس در ابعاد ۶۴×۶۴ انتخاب شده است که برای بازسازی نهایی به تعداد ۱۲۸ (۱۲۸=۶۴+۶۴) شات نیاز است. در نتایج تجربی و تئوری به ترتیب از "II" و "TII" به عنوان جسم انتخاب شده‌اند که نتایج شبیه‌سازی و تجربی در شکل ۲ قابل مشاهده است.

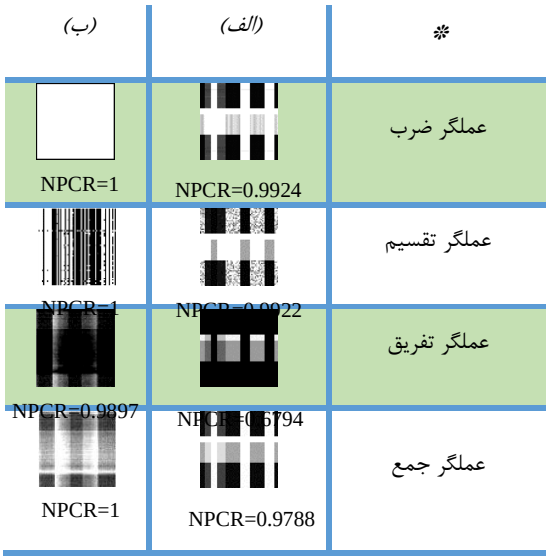


شکل۲: نتایج شبیه‌سازی (الف) و تجربی (ب) ور روش (SCGI)

در روش نامتقارن، انتخاب سطر و ستون از تصاویر حاصل از ماتریس‌های جاروبی سطری و ستونی (ستون میانی شکل ۱) به عنوان کلید عمومی و عملگر ضرب خارجی به عنوان کلید خصوصی انتخاب شده‌اند. برای رمزگشایی از چهار عملگر اصلی استفاده شده است که نتایج در شکل ۳ قابل مشاهده است.

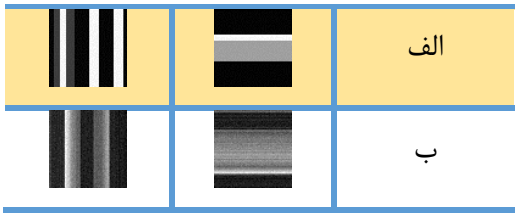
در روش متقارن، انتخاب سطر/ستون و عملگر ضرب خارجی به عنوان کلیدهای خصوصی سیستم متقارن در نظر گرفته می‌شوند. بنابراین در این سیستم رمزنگاری فقط می‌توان به تصاویر حاصل از ماتریس‌های جاروبی سطری و ستونی جسم دست یافت که هیچ اطلاعاتی از جسم در اختیار کاربر قرار نمی‌دهد. بنابراین نتایج رمزنگاری به صورت تئوری و تجربی در شکل۴ مشاهده می‌شود.

از شکل‌های ۳و ۴ می‌توان مشاهده کرد که در هر دو حالت تئوری و تجربی حتی با لو رفتن ۱۰۰٪ اطلاعات، هیچ



شکل۳: نتایج تئوری (الف) و تجربی (ب) سیستم رمزنگاری نامتقارن برای تصویربرداری گوست محاسباتی جاروبی همراه با NPCR

اطلاعاتی از جسم و تصویر نهایی در اختیار کاربر قرار نمی‌گیرد. بنابراین رمزنگاری با استفاده از SCGI، یکی از باامنیت‌ترین روش‌های رمزنگاری است.



شکل۴: نتایج تئوری (الف) و تجربی (ب) سیستم رمزنگاری متقارن برای تصویربرداری گوست محاسباتی جاروبی

۴. نتیجه‌گیری

در این کار، ابتدا روش تصویربرداری گوست محاسباتی جاروبی معرفی شده است و نتایج تئوری و تجربی، آورده شده است که تصویر نهایی با مجموع اندازه‌گیری سطر و ستون‌های ماتریس کاتوره‌ای بدست می‌آید. سپس رمزنگاری اطلاعات با استفاده از این روش و سیستم متقارن و نامتقارن انجام شده است. نتایج نشان می‌دهند که در هر دو روش حتی با لو رفتن ۱۰۰٪ داده‌های ارسالی به کاربر، نمی‌توان به داده‌های موردنظر برای بازیابی جسم دست یافت. بنابراین رمزنگاری با روش تصویربرداری گوست محاسباتی جاروبی دارای امنیت بسیار بالا در ارسال اطلاعات بین دو کاربر می‌باشد.

مرجع‌ها

[1] S. Lian, Multimedia content encryption: techniques and applications, Auerbach Publications, 2008.

[2] O. Goldreich, Foundations of cryptography: volume 2, Cambridge university press, 2009.

[3] Pittman, T.B., Shih, Y.H., Strekalov, D.V. and Sergienko, A.V. “Optical imaging by means of two-photon quantum entanglement,” Physical Review A,vol. 52, p.3429, 1995.

[4] Bennink, R.S., Bentley, S.J. and Boyd, R.W. ““Two-photon” coincidence imaging with a classical source,” Physical review letters, vol. 89, p. 113601, 2002.

[5] Ghaleh, S.R., Ahmadi-Kandjani, S., Kheradmand, R. and Olyaeefar, B. “Improved edge detection in computational ghost imaging by introducing orbital angular momentum,” Applied optics, vol. 57, p. 9609-9614, 2018.

[6] Shapiro, J.H., “Computational ghost imaging,” Physical Review A, vol. 78, p. 061802, 2008.

[7] Rajabi-Ghaleh, S. Kheradmand, R. and Ahmadi-Kandjani, S., “Improvement of computational Ghost Imaging Speed with Sweep Random Algorithm,” Annual Physics Conference of Iran, p.526-529, 2019.

[8] Tanha, M., Kheradmand, R. and Ahmadi-Kandjani, S., “Gray-scale and color optical encryption based on computational ghost imaging,” Applied Physics Letters, vol.101, p.101108, 2012.

[9] Clemente, P., Durán, V., Tajahuerce, E. and Lancis, J., “Optical encryption based on computational ghost imaging,” Optics letters, vol. 35, pp.2391-2393, 2010.

[10] Kong, L.J., Li, Y., Qian, S.X., Li, S.M., Tu, C. and Wang, H.T., “Encryption of ghost imaging,” Physical Review A, vol. 88, p.013852, 2013.

[11] Sun, M., Shi, J., Li, H. and Zeng, G., “A simple optical encryption based on shape merging technique in periodic diffraction correlation imaging,” Optics Express, vol. 21, pp.19395-19400, 2013.

[12] Bromberg, Y., Katz, O. and Silberberg, Y., “Ghost imaging with a single detector,” Physical Review A, vol. 79, p.053840, 2009.

[13] Wu, Y., Noonan, J.P. and Agaian, S., “NPCR and UACI randomness tests for image encryption” Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2), pp.31-38, 2011.