بیست و یکمین کنفرانس اپتیک و فوتونیک ایران
و هفتمین کنفرانس مهندسی و فناوری فوتونیک ایران
۲۳ تا ۲۵ دی ماه ۱۳۹۳، دانشگاه شهید بهشتی

مقایسه روشهای رمزنگاری نوری براساس تصویرسازی گوست

محمد ظفری، سهراب احمدی کندجانی و رضا خردمند

دانشگاه تبریز، پژوهشکده فیزیک کاربردی و تحقیقات ستاره‌شناسی

چکیده - تصویرسازی گوست یک روش تصویرسازی نوین است که ماهیت آن بر مبنای محاسبه تابع همبستگی مرتبه دوم دو پرتو همبسته یا درهم‌تنیده استوار است. این ویژگی استفاده از دو پرتو باعث اهمیت تصویرسازی گوست در رمزنگاری نوری شده است. در این مقاله، ضمن معرفی روش گزینشی به عنوان یک تکنیک جدید برای تصویرسازی گوست و رمزنگاری نوری بر اساس این روش به صورت تجربی، مقایسه‌ای بین روش‌های رمزنگاری قبلی به انجام رسیده است. مقدار محاسبه‌شده پارامتر مربوط به میزان خطا در رمزگشایی غیرمجاز، برتری و امنیت بالای روش گزینشی در رمزنگاری نوری را نسبت به روش‌های قبلی نشان می‌دهد.

کلید واژه- تابع همبستگی، تصویرسازی گوست، رمزنگاری نوری، روش گزینشی

Comparison of optical encryption methods based on ghost imaging

Mohammad Zafari, Sohrab Ahmadi kandjani, Reza Kheradmand

Research Institute for Applied Physics and Astronomy (RIAPA), University of Tabriz, Tabriz, Iran

Abstract- Ghost imaging is a novel imaging technique which the nature of it is based on calculating the second-order correlation function of two correlated or entangled beams. This feature of using two beams has been caused ghost imaging significance in optical encryption. In this paper, with the introducing of the selective method as a novel technique for ghost imaging and optical encryption based on this method experimentally, a comparison between previous encryption methods has been accomplished. Calculated value of the error rate parameter in unauthorized decryption shows the superiority and high security of selective method in optical encryption over previous methods.

Keywords: Correlation function, ghost imaging, optical encryption, selective method

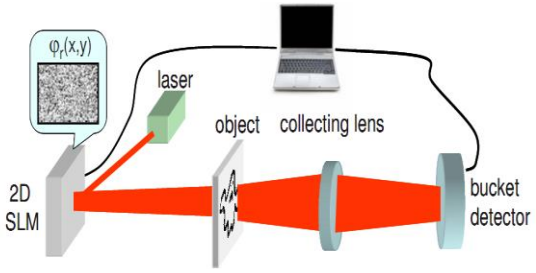
۱- مقدمه

در یک چیدمان تصویرسازی گوست متداول، پرتو لیزر پس از عبور از یک شیشه مات چرخان، به دو باریکه همبسته فضایی شکافته می‌شود که در دو مسیر جداگانه حرکت می‌کنند و معمولا به عنوان بازوهای مرجع و جسمی شناخته می‌شوند. در بازوی جسمی، باریکه به جسم برخورد کرده و نور عبوری یا بازتابی از آن توسط یک آشکارساز تک-پیکسل که قدرت تفکیک فضایی ندارد، آشکارسازی می‌شود. در بازوی مرجع یک آشکارساز با قدرت تفکیک فضایی بالا قرار دارد و اطلاعات مربوط به باریکه مرجع را که هیچ برخورد یا اندرکنشی با جسم ندارد را اندازه‌گیری می‌کند. در نتیجه تصویر گوست جسم با اندازه‌گیری تابع همبستگی متقابل شدت باریکه جسمی و باریکه مرجع به دست می‌آید[۵-۱].

رمزنگاری نوری اطلاعات با استفاده از تصویرسازی گوست موضوعی است که اخیرا مطرح شده و دارای قابلیت انتقال اطلاعات با امنیت بالا است. در این مقاله با معرفی یک روش جدید برای تصویرسازی گوست محاسباتی با عنوان روش گزینشی و اثبات برتری این روش نسبت به روش محاسباتی مرسوم، رمزنگاری نوری بر اساس روش گزینشی به انجام رسیده و با روش‌های قبلی مقایسه شده است.

۲- تصویرسازی گوست محاسباتی

در روش جدید تصویرسازی گوست که به تصویرسازی گوست محاسباتی معروف است، به‌جای استفاده از شیشه مات چرخان، پرتو لیزر از یک مدولاتور فضایی نور(SLM) عبور داده می‌شود[۶،۷]. در این روش نور غیر همدوس فضایی با اعمال الگوهای شبه‌تصادفی روی SLM تولید می‌شود؛ بنابراین بازوی مرجع را می‌توان با محاسبات عددی جایگزین کرد. شکل (۱) چیدمان تصویرسازی گوست محاسباتی را نشان می‌دهد.



شکل ۱: چیدمان تصویرسازی گوست محاسباتی[۷]

در تصویرسازی گوست، برای بازسازی تصویر گوست جسم با تابع عبور $T(x,y)$ و در فاصله z=L از SLM از رابطه زیر استفاده می‌شود:

$$G(x,y)=\frac{1}{N}\sum_{r=1}^{N}(B_r-<B>)I_r(x,y) \quad (۱)$$

که در آن $B_r=\int dxdyI_r(x,y,L)T(x,y)$ شدت اندازه‌گیری‌شده توسط آشکارساز بوکت و $I_r=|E_r(x,y,z=L)|^2$ الگوی شدت محاسبه شده در سطح جسم است.

۳- تصویرسازی گوست محاسباتی گزینشی

در تصویرسازی گوست محاسباتی مرسوم الگوهای لکه‌ای به صورت ماتریس‌های تصادفی روی SLM نقش می‌بندند، به طوری که به هر یک از عناصر ماتریس، یک مقدار تصادفی به عنوان مدولاتور شدت نسبت داده می‌شود. در نتیجه در هر اندازه‌گیری، تمامی عناصر ماتریس دارای یک مقدار تصادفی دلخواه خواهد بود. به طور مشابه، در تصویرسازی گوست گزینشی ما در هر اندازه‌گیری یک ماتریس تصادفی در نظر می‌گیریم؛ اما یک درایه آن مقدار متفاوت و بسیار بزرگ‌تر از درایه‌های دیگر به خود می‌گیرد. بنابراین، شدت عبوری از این درایه بسیار بیشتر درایه‌های دیگر خواهد بود. در این حالت چون در کل اندازه‌گیری‌ها هر درایه تنها یک بار مقدار متفاوت به خود می‌گیرد، در نتیجه ماکزیمم شات یا اندازه‌گیری لازم برای تشکیل یک تصویر با بهترین کیفیت، برابر حاصل‌ضرب تعداد سطرها در ستون‌های ماتریس خواهد بود. البته در این روش بسته به کاربرد می‌توان به جای استفاده از ماتریس تصادفی، از یک ماتریس با عناصر یکسان و یک عنصر متفاوت در هر اندازه‌گیری استفاده کرد. همچنین در این روش با انتخاب دو نقطه، چهار نقطه و یا تعداد نقاط بیشتر کنار هم با مقدار متفاوت به عنوان واحد در هر اندازه‌گیری، می‌توان تعداد اندازه‌گیری‌ها را به ترتیب به نصف، یک‌چهارم و یا کمتر، کاهش داد. شکل (۲) تصاویر گوست بازسازی‌شده به ابعاد ۶۵×۶۵ پیکسل و با تعداد ۴۲۲۵ اندازه‌گیری را با استفاده از شبیه‌سازی عددی به روش تصویرسازی گوست محاسباتی مرسوم و گزینشی نشان می‌دهد. برای مقایسه دقت بازسازی تصاویر گوست از خطای میانگین مربع (MSE) استفاده می‌شود که از

رابطه زیر بدست می‌آید[۸]:

(۲)

$$MSE = \frac{1}{N_{pix}} \sum_{i,j} [T_{GI}(x_i, y_j) - T_{ref}(x_i, y_j)]^2$$

در این رابطه T_{GI} و T_{ref} به ترتیب شدت‌های مربوط به تصویر گوست بازسازی‌شده و تصویر اصلی هستند.

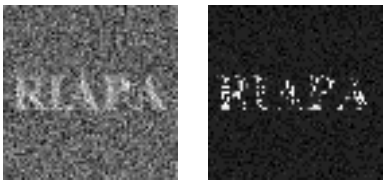
(الف) (ب) (ج)

شکل ۲: تصاویر حاصل از شبیه‌سازی عددی. الف) تصویر اصلی. ب) تصویر گوست به روش محاسباتی مرسوم. ج) تصویر گوست به روش گزینشی.

مقادیر محاسبه‌شده MSE برای تصاویر فوق نشان می‌دهد که دقت بازسازی تصویر گوست به روش گزینشی بیش از **۱۴** مرتبه بهتر از روش مرسوم است. قابلیت منحصربه‌فرد تصویرسازی گوست گزینشی توانایی آن در بازسازی تصویر جداگانه از بخش‌های مختلف یک جسم است (شکل ۳). این امر با انتخاب اندازه‌گیری‌های معین و قرار دادن مقادیر متفاوت به صورت ترتیبی در سطرها یا ستون‌های ماتریس در اندازه‌گیری‌های متوالی صورت می‌گیرد.

شکل ۳: تصاویر گوست بازسازی‌شده از بخش‌های مختلف تصویر اصلی به صورت جداگانه.

یکی دیگر از تفاوت‌های تصویرسازی گوست گزینشی با روش مرسوم این است که در روش مرسوم با کاهش تعداد اندازه‌گیری‌ها کیفیت تصویر گوست کاهش می‌یابد، اما با کاهش تعداد اندازه‌گیری‌ها در روش گزینشی، تعداد نقاط بازسازی‌شده تصویر گوست کاهش می‌یابد که این ویژگی در رمزنگاری نوری اطلاعات یک مزیت بسیار مهم به‌شمار می‌رود. این ویژگی در شکل (۴) نشان داده شده است.



شکل ۴: تصاویر گوست حاصل از ۱۵۰۰ اندازه‌گیری. روش مرسوم (سمت چپ) و روش گزینشی (سمت راست).

۴- رمزنگاری نوری

در رمزنگاری نوری اطلاعات براساس تصویرسازی گوست، الگوهای تصادفی که روی باریکه لیزر اثر می‌کنند، قسمت اصلی مولفه‌های رمز هستند و با معلوم بودن شدت‌های مربوط به هر الگوی تصادفی، تصویر گوست جسم بازسازی می‌شود[۱۴-۹]. برای بدست آوردن میزان خطا در رمزگشایی غیرمجاز تصویر، از خطای ریشه نرمال میانگین مربع استفاده می‌شود. این کمیت، تصویر رمزگشایی‌شده ناموفق را با تصویر ورودی اصلی مقایسه می‌کند و به صورت زیر محاسبه می‌شود[۱۴،۱۰]:

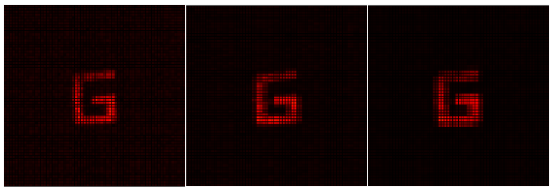
$$NRMS = \frac{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} |I_d(i,j) - I_o(i,j)|^2}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} |I_o(i,j)|^2}} \qquad (۳)$$

در این رابطه I_d و I_o به ترتیب نشان‌دهنده شدت‌های مربوط به تصویر رمزگشایی‌شده و تصویر اصلی هستند. مقدار NRMS بین صفر و یک تغییر می‌کند ($0 \le NRMS \le 1$) که $NRMS = 0$ نشان‌دهنده کمترین امنیت یا همان رمزگشایی کامل و $NRMS = 1$ نشان‌دهنده بیشترین امنیت در سیستم رمزنگاری است.

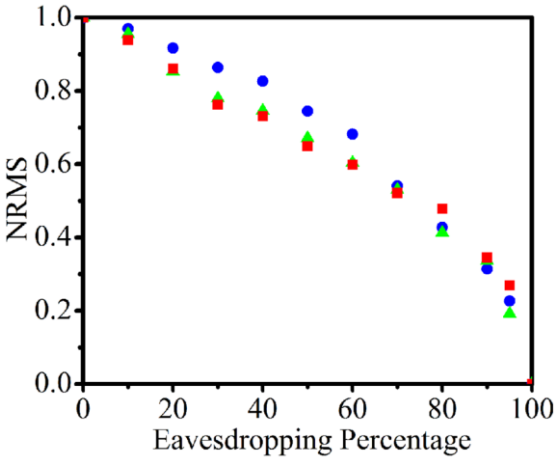
رمزنگاری نوری اطلاعات بر اساس تصویرسازی گوست محاسباتی برای اولین بار در سال ۲۰۱۰ مطرح شد که در آن از الگوهای فازی اختیاری و با مقادیر فازی متغیر در بازه [0-2π] به عنوان قسمت اصلی مؤلفه‌های رمز استفاده می‌شد[۹]. نتایج حاصل از این روش به گونه‌ای بود که یک کاربر غیرمجاز با دسترسی به تنها ٪۱۰ از اطلاعات می‌توانست تصاویر را رمزگشایی کند. در سال ۲۰۱۲ رمزنگاری تصاویر گوست با استفاده از مواد نورتاب برای بالا بردن سطح امنیت اطلاعات کدگذاری‌شده به انجام رسید[۱۰]. در این روش مقدار محاسبه‌شده NRMS برای دزدیده شدن ٪۲۰ اطلاعات برابر ۰/۳۸ است که نسبت به

روش قبلی از امنیت بهتری برخوردار است. اما در سال ۲۰۱۳ رمزنگاری تصاویر گوست با استفاده از روش دو پرتو و چیدمان متداول مطرح شد[۱۱]. بهره‌گیری از این روش سطح امنیت اطلاعات کدگذاری‌شده را نسبت به دو روش قبلی بسیار بالا برد به طوری که مقدار NRMS محاسبه‌شده تحت ٪۵۰ لو رفتگی اطلاعات به ۰/۶۸ رسید.

برای نشان دادن برتری روش گزینشی در رمزنگاری نوری اطلاعات به صورت تجربی، ما از یک لیزر هلیوم- نئون با طول‌موج $\lambda = 632.8nm$ یک SLM به ابعاد ۱۳۰×۱۳۰ پیکسل (اندازه هر پیکسل برابر$2\times2\mu m^2$ است) و یک دوربین CMOS به ابعاد ۴۴۰×۶۴۰ پیکسل ($4\times3mm^2$) استفاده کردیم. به منظور محاسبات کمّی، تصویر گوست جسم با در نظر گرفتن تعداد نقاط مختلف کنار هم با مقدار متفاوت به عنوان واحد در هر اندازه‌گیری، بازسازی شده و مقدار NRMS برای درصدهای مختلف لو رفتگی اطلاعات محاسبه شد.



شکل ۵: (به ترتیب از چپ به راست) تصویر گوست بازسازی‌شده با در نظر گرفتن یک نقطه، دو نقطه و چهار نقطه کنار هم با مقدار متفاوت به عنوان واحد در هر اندازه‌گیری به صورت تجربی.



شکل ۶: نمودار میزان خطا بر حسب درصد لو رفتگی اطلاعات. داده‌های مربوط به حالت‌های یک-نقطه، دو-نقطه و چهار-نقطه به ترتیب با دایره، مثلث و مربع نشان داده شده‌اند.

همان‌طور که در شکل (۶) مشاهده می‌شود، مقدار NRMS محاسبه‌شده تحت ٪۵۰ لو رفتگی اطلاعات با در نظر گرفتن حالت یک-نقطه برابر ۰/۷۵ است که در مقایسه با آخرین نتیجه گزارش‌شده، دارای مقدار بزرگ‌تری بوده و در نتیجه سطح امنیت اطلاعات رمزگذاری‌شده در این روش بالاتر از روش‌های قبلی است.

۵- نتیجه‌گیری

در این مقاله ابتدا روش گزینشی به عنوان یک تکنیک جدید برای تصویرسازی گوست معرفی شد. سپس با بیان قابلیت تصویرسازی گوست در رمزنگاری نوری، مقایسه‌ای بین روش‌های مختلف رمزنگاری بر اساس تصویرسازی گوست به انجام رسید. در نهایت با رمزنگاری نوری بر اساس روش گزینشی به صورت تجربی و محاسبه NRMS برای درصدهای مختلف لو رفتگی اطلاعات و مقایسه آن با روش‌های قبلی، برتری روش گزینشی در رمزنگاری به اثبات رسید.

مراجع

[1] Pittman T., et al., *Optical imaging by means of two-photon quantum entanglement*, **Phys. Rev.A**. 52 (1995) 3429-3432.

[2] Bennink R S., Bentley S J., Boyd R W., *"Two-Photon" Coincidence Imaging with a Classical Source*, **Phys. Rev. Lett.** 89 (2002) 113601.

[3] Valencia A., et al., *Two-photon imaging with thermal light*, **Phys. Rev. Lett**. 94 (2005) 063601.

[4] Erkmen B I., Shapiro J H., *Ghost imaging: from quantum to classical to computational*, **Adv. Opt. Photon**. 2 (2010) 405-450.

[5] Shapiro J H., Boyd R W., *The physics of ghost imaging*, **Quantum Inf Process**. 11 (2012) 949-993.

[6] Shapiro J H., *Computational ghost imaging*, **Phys. Rev. A**. 78 (2008) 061802.

[7] Bromberg Y., Katz O., Silberberg Y., *Ghost imaging with a single detector*, **Phys. Rev. A**. 79 (2009) 053840.

[8] Katz O., Bromberg Y., Silberberg Y., *Compressive ghost imaging*, **Appl. Phys. Lett**. 95 (2009) 131110.

[9] Clemente P., et al., *Optical encryption based on computational ghost imaging*, **Opt. Lett**. 35 (2010) 2391-2393.

[10] Tanha M., Kheradmand R., Ahmadi-Kandjani S., *Gray-scale and color optical encryption based on computational ghost imaging*, **Appl. Phys. Lett**. 101 (2012) 101108-101108-3.

[11] Kong L J., et al., *Encryption of ghost imaging*, **Phys. Rev. A**. 88 (2013) 013852.

[12] Sun M., et al., A simple optical encryption based on shape merging technique in periodic diffraction correlation imaging, **Opt. Express**. 21 (2013) 19395-19400.

[13] Chen W., Chen X., *Ghost imaging for three-dimensional optical security*, **Appl. Phys. Lett**. 103 (2013) 221106.

[14] Zafari M., Kheradmand R., Ahmadi-Kandjani S., *Optical encryption with selective computational ghost imaging*, **J.Opt**. 16 (2014) 105405.