ISSN 0201-744X, ISSN 0321-2211

У запропонованому алгоритмі використовуються комбінації перетворень: побітного додавання по mod2, матричне перетворення по mod256, S-блоку і таблиці стиснення, здійснює шифрування 128 (в модифікації 128 + 32l) бітових блоків даних за допомогою 128 (в модифікації 128 + 32l) бітового ключа k , де l = 1,2, ..., d, d <∞.
Ключові слова: алгоритм, шифрування, S-блок перетворень байтів, таблиця стиснення, матричне перетворення.

D. E. Akbarov, Sh. A. Umarov
Fergana branch of the Tashkent university information technologies, Fergana, Uzbekistan
NEW ALGORITHM OF BLOCK ENCRYPTION OF DATA WITH THE SYMMETRIC KEY
In this article, continuing idea of development of the symmetric block data encryption algorithms which aren't based on Feystel's network the new symmetric block algorithm is offered.
In the offered algorithm are used a combination of conversions: bit-by-bit addition on mod2, matrix transformation on mod256, the S-unit and the table of compression, realizes encoding 128 (in modification 128+32l) bit data units by means of 128 (in modification 128+32l) a bit key of k, where l=1,2,…, d, d<∞.
Keywords: algorithm, encodings, S-block conversions of bytes, table of compression, matrix transformation.

Надійшла до редакції
26 квітня 2016 року

Рецензовано
11 травня 2016 року

УДК 681.7.067

АВТОМАТИЗОВАНИЙ РОЗРАХУНОК ШИРОКОКУТНИХ ОБ'ЄКТИВІВ

Сокуренко В. М., Буйлов І. С.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

E-mail: sokurenko2@meta.ua, enekotrade@gmail.com

Однією із затребуваних задач сучасної обчислювальної оптики є задача повної автоматизації процедури знаходження параметрів оптичної системи (ОС), оптимальних за різними критеріями. Широко розповсюджені методи локальної оптимізації мають суттєвий недолік, який полягає в тому, що для їх результативного застосування, як правило, потрібна якісна вихідна ОС. Поставлену задачу пошуку найменшого значення оціночної функції в заданому просторі допустимих значень параметрів потенційно дозволяють вирішити методи глобальної оптимізації (ГО). У зв'язку з цим стосовно автоматизованого розрахунку ОС різними авторами було запропоновано використовувати такі методи ГО як імітаційний відпал, генетичні алгоритми тощо. У даній роботі чисельно досліджуються можливості адаптивного методу диференційної еволюції Коші, запропонованого в 2013 році. Алгоритм цього методу відрізняється наявністю внутрішнього механізму адаптації параметрів-коефіцієнтів класичного методу диференційного еволюції, а також застосуванням розподілу Коші для генерації нових «випадкових» значень цих коефіцієнтів. Зазначений вище алгоритм був реалізований у власній комп'ютерній програмі автоматизованого розрахунку ОС довільного призначення. В роботі здійснена експериментальна перевірка ефективності реалізації вибраного методу під час розрахунку аналогів ОС, запропонованих нещодавно в патентах США.

Ключові слова: *об'єктив, оптична система, адаптивний метод диференційної еволюції Коші, автоматизований розрахунок, глобальна оптимізація.*

Вступ

На відміну від широко поширених методів локальної оптимізації, істотним недоліком яких є "застрягання" в першому ж знайденому мінімумі,

глобальна оптимізація потенційно дозволяє знайти розв'язок з найменшим значенням цільової функції на всьому просторі допустимих значень параметрів системи.

На жаль, наявність багатьох локальних мінімумів в багатомірному просторі розв'язків та суттєві затрати часу є суттєвими перешкодами, які потребують подолання.

Варіанти алгоритмів глобальної оптимізації, запропоновані та модифіковані в останні роки, мають ряд переваг та дозволяють достатньо швидко отримувати розв'язок в автоматизованому режимі [1-5].

Дослідження, представлені в даній роботі, підтверджують практичну результативність застосування сучасних алгоритмів оптимізації в сучасній оптичній інженерії. Вони показують, що вдосконалення таких алгоритмів є перспективним напрямком досліджень, оскільки його результати сприяють розробці нових оптичних систем (ОС) з поліпшеною якістю зображення.

Постановка задачі

Метою даної роботи є чисельне дослідження можливостей адаптивного методу диференційної еволюції Коші (ACDE) [1, 2] під час автоматизованого розрахунку ширококутних об'єктивів.

Алгоритм цього методу відрізняється наявністю внутрішнього механізму адаптації параметрів-коефіцієнтів *F* (scaling factor) та *CR* (crossover rate) класичного методу диференційної еволюції, а також застосуванням розподілу Коші для генерації нових «випадкових» значень цих коефіцієнтів. Особливістю методу є також те, що адаптація зазначених параметрів для кожної точки незалежна.

Зазначений вище алгоритм був інтегрований у власну комп'ютерну програму автоматизованого розрахунку ОС довільного призначення.

Вибір відомих оптичних систем об'єктивів з патентних джерел

В даній роботі проведена перевірка працездатності та ефективності адаптивного методу диференційної еволюції Коші на прикладі розрахунку ОС двох лінзових ширококутних об'єктивів. Параметрами оптимізації ОС обиралися радіуси кривизни поверхонь та осьові відстані. Остання сферична поверхня об'єктива використовувалася для контролю задньої фокусної відстані всієї системи (завданням фіксованого значення кута вихідного апертурного променю).

Як перший приклад було обрано ОС об'єктива з патенту US 8237842 B2 компанії Nikon Corporation [6] (рис. 1, табл. 1).

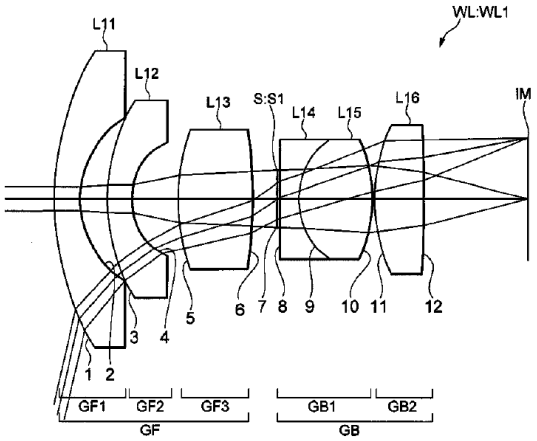

Рис. 1. Оптична схема об'єктива з патенту [6]

Представлений в патенті об'єктив містить дві групи лінз, а загальна кількість компонентів дорівнює шести.

Перша група лінз містить від'ємний меніск, ввігнутістю направленого до площини зображень, від'ємну лінзу, яка ввігнутістю направлена до площини зображень, та третю позитивну лінзу, яка опуклою стороною направлена до площини предметів.

Друга лінзова група містить склейку з від'ємної та позитивної лінз, яка має в цілому позитивну заломлюючу силу.

Як другий приклад було обрано ОС об'єктива з патенту US 8503110 B2 Nikon Corporation [7] (рис. 2, табл. 2).

Загальна кількість компонентів об'єктива - 6. Перша лінза виконана як від'ємний меніск, який опуклою стороною направлений до площини предметів, друга позитивна та третя від'ємна лінзи утворюють склейку, яка має позитивну заломлюючу силу в цілому, четверта лінза є від'ємною, а п'ята та шоста – позитивними.

Таблиця 1. Числові значення аберацій об'єктива з патенту [6]

Тип аберації	Значення аберації
Значення СКВ в широкому спектральному діапазоні:	
- для поля №1 (на оптичній осі)	30,6 мкм
- для поля №2 (під кутом 54,79°)	79,6 мкм
- для поля №3 (на периферії, під кутом 77,5°)	148,5 мкм
Дисторсія на краю поля зору W=77,5°	72 %

Загальна послідовність автоматизованого розрахунку

Для розв'язання поставленої задачі в даній роботі використано методику, яка передбачає виконання чотирьох етапів:

1. Задається загальна структура оптичної системи. Фактично встановлюються довільні значення радіусів поверхонь, товщин лінз та повітряних проміжків. В даних дослідженнях марки скла, довжини хвиль та апертура системи були фіксованими.
2. Обираються параметри оптимізації та формується оціночна функція. На цьому етапі конструктор має можливість встановити раціональні діапазони на кривизни поверхонь лінз, повітряні проміжки, осьові товщини лінз, допустимі товщини лінз на краю з урахуванням мінімальних допусків для подальшого закріплення та при необхідності – максимальну товщину ОС вздовж осі, максимальну дисторсію та інші вимоги.
3. Виконується основна процедура глобальної оптимізації.
4. Запускається локальна оптимізація для «кінцевого доведення» ОС.

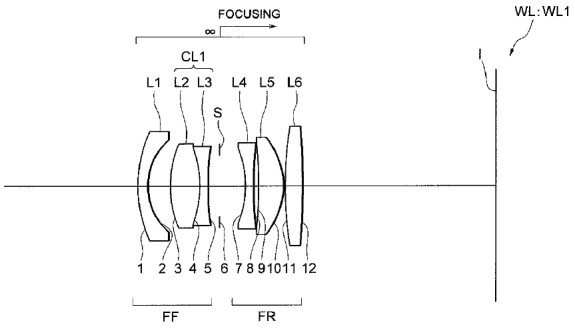

Рис. 2. Оптична схема об'єктива з патенту [7]

Таблиця 2. Числові значення аберацій об'єктива з патенту [7]

Тип аберації	Значення аберації
Значення СКВ в широкому спектральному діапазоні:	
- для поля №1 (на оптичній осі)	13,08 мкм
- для поля №2 (під кутом 21,59°)	22,94 мкм
- для поля №3 (на периферії, під кутом 30,54°)	83,93 мкм
Дисторсія на краю поля зору W=30,54°	2%

Результати автоматизованого розрахунку

Для параметричного синтезу ОС першого об'єктива було задано такі вхідні параметри: кутове поле зору в просторі предметів 155°; задня фокусна відстань 10 мм; спектральний діапазон 0,48...0,65 мкм (основна довжина хвилі - 0,58 мкм); максимальна довжина системи 95,14 мм.

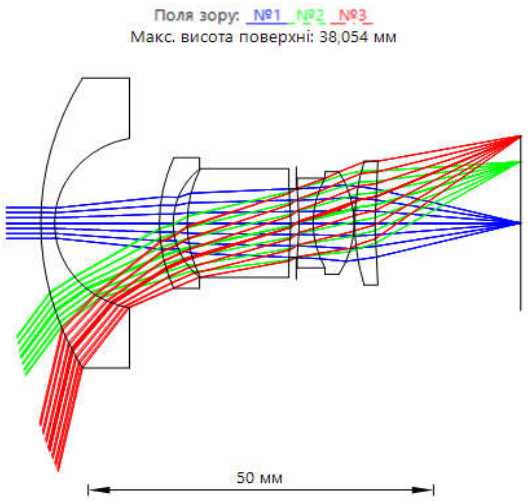

Рис. 3. Оптична схема отриманої ОС об'єктива №1 з ходом променів

Загальна кількість пошукових параметрів дорівнювала 21. На рис. 3 представлена оптична схема розробленого об'єктива, а в табл. 3 – його конструктивні параметри.

Для оцінки якості зображення на рис. 4 представлена поліхроматична МПФ в геометричному наближенні. Як видно, розроблена ОС є виправленою для заданих довжин хвиль та збалансованою по полю зору.

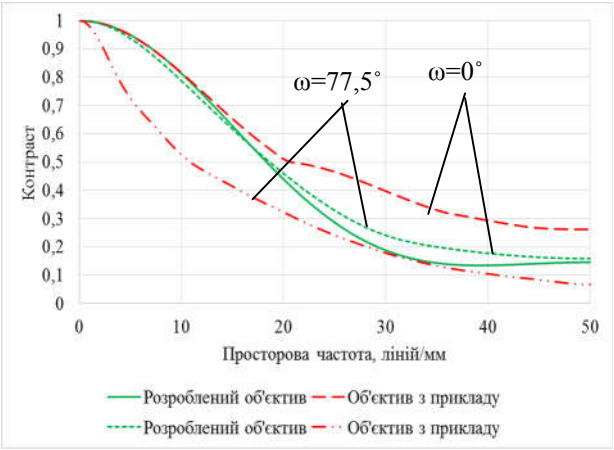

Рис. 4. Поліхроматична МПФ отриманої ОС та прикладу (об'єктива №1)

В табл. 4 наведені числові значення основних аберацій отриманої ОС та варіанту з патенту США [6].

Параметричний синтез ОС другого об'єктива проводився з такими параметрами: кутове поле зору в просторі предметів 61,08°; спектральний діапазон 0,43…0,65 мкм (основна довжина хвилі: 0,58 мкм); максимальна довжина системи 48,4 мм; задня фокусна відстань 24,6 мм.

Загальна кількість пошукових параметрів дорівнювала 21. Оптична схема розробленого об'єктива представлена на рис. 5, а його конструктивні параметри – в табл. 5.

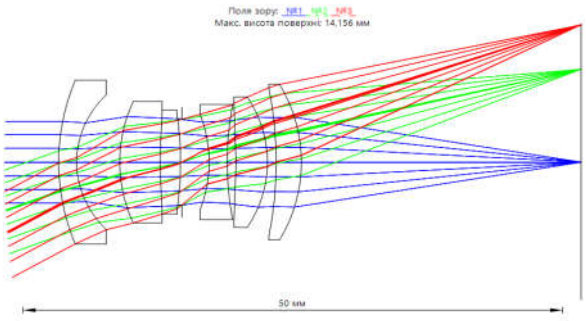

Рис. 5. Оптична схема отриманої ОС об'єктива №2 з ходом променів

Таблиця 3. Конструктивні параметри розробленої ОС об'єктива №1

Номер поверхні	Радіус, мм	Товщина, мм	Показник заломлення n_e та коефіцієнт дисперсії ν_e	Світловий радіус, мм
Предмет	∞	∞		
1	43,819	2,00	1,864; 40,77	22,19
2	13,15	15,17		12,95
3	24,90	2,00	1,864; 40,77	9,99
4	10,95	2,02		8,31
5	19,23	15,00	1,904; 17,98	8,31
6	-61,97	0,81		5,80
7 (апертурна діафрагма)	∞	0,42		5,25
8	-43,38	2,00	1,904; 17,98	5,31
9	14,55	5,93	1,758; 49,60	6,86
10	-15,02	0,1		7,85
11	33,53	2,91	1,887; 20,88	9,36
12	107,21	21,11		9,48
Зображення	∞	0,0		13,38

Таблиця 4. Порівняння основних аберацій

Вид аберації	Об'єктив з патенту[6]	Розроблений об'єктив
Поперечна сферична аберація на осі для основної довжини хвилі	34,21 мкм	42,58 мкм
Поперечна сферична аберація на осі у всьому спектральному діапазоні	58,71 мкм	51,37 мкм
Астигматизм для основної довжини хвилі по всьому полю зору	-0,03 мм	-0,03 мм
Поперечна аберація на краю поля зору для основної довжини хвилі в меридіональний площині	327,9 мкм	91,45 мкм
Поперечна аберація на краю поля зору для основної довжини хвилі в сагітальній площині	74,58 мкм	47,42 мкм
Поперечна аберація на краю поля зору у всьому спектральному діапазоні в меридіональний площині	400 мкм	97 мкм
Поперечна аберація на краю поля зору у всьому спектральному діапазоні в сагітальній площині	83,0 мкм	74,6 мкм
Дисторсія для основної довжини хвилі по всьому полю зору	72 %	70 %
Хроматизм збільшення на краю поля зору	0,28 мм	0,05 мм

На рис. 6 представлені геометричні поліхроматичні МПФ. З графіків видно, що досягнуте значне поліпшення якості.

В табл. 6 наведені числові значення основних аберацій отриманої ОС та патентного варіанту.

Висновки

В даній роботі було здійснено перевірку основних можливостей адаптивного методу диференційної еволюції Коші на прикладах автоматизованої розробки двох оптичних систем (ОС) ширококутних лінзових об'єктивів.

З результатів розрахунку розроблених систем видно, що вони не поступаються відомим аналогам-прототипам.

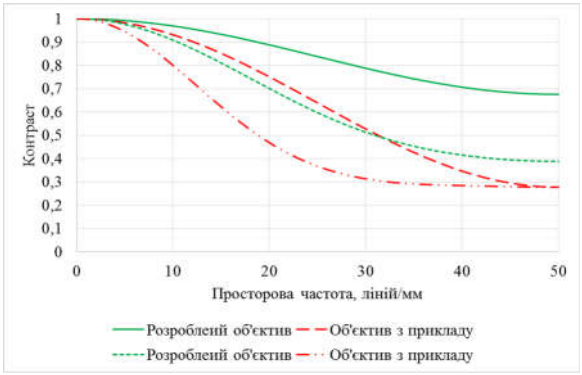

Рис. 6. Поліхроматична МПФ отриманої ОС та прикладу (об'єктива №2)

Таблиця 5. Конструктивні параметри розробленої ОС об'єктива №2

Номер поверхні	Радіус, мм	Товщина, мм	Показник заломлення n_e та коефіцієнт дисперсії ν_e	Світловий радіус, мм
Предмет	∞	∞		
1	23,89	1,66	1,618; 63,38	8,40
2	10,12	3,98		6,95
3	16,09	3,73	1,806; 40,94	6,24
4	72,58	1,90	1,603; 38,02	5,32
5	-36,80	0,12		4,80
6 (апертурна діафрагма)	∞	2,52		4,40
7	-14,69	1,66	1,805; 25,43	4,92
8	34,41	0,83		5,91
9	-90,54	2,90	1,713; 53,85	6,04
10	-12,99	0,81		6,70
11	-43,05	2,33	1,720; 50,24	7,64
12	-16,82	25,91		7,99
Зображення	∞	0,0		14,15

Таблиця 6. Порівняння основних аберацій

Вид аберації	Об'єктиву з патенту[7]	Розроблений об'єктив
Поперечна сферична аберація на осі для основної довжини хвилі	21,92 мкм	13,02 мкм
Поперечна сферична аберація на осі у всьому спектральному діапазоні	21,92 мкм	21,15 мкм
Астигматизм для основної довжини хвилі по всьому полю зору	-0,2 мм	0,27 мм
Поперечна аберація на краю поля зору для основної довжини хвилі в меридіональний площині	58,5 мкм	-52,8 мкм
Поперечна аберація на краю поля зору для основної довжини хвилі в сагітальній площині	-202,9 мкм	61,54 мкм
Поперечна аберація на краю поля зору у всьому спектральному діапазоні в меридіональний площині	61,7 мкм	-69,3мкм
Поперечна аберація на краю поля зору у всьому спектральному діапазоні в сагітальній площині	-225,5 мкм	76,0 мкм
Дисторсія для основної довжини хвилі по всьому полю зору	-2,07 %	-2,0 %
Хроматизм збільшення на краю поля зору	0,01 мм	0,01 мм

Отримані результати свідчать, що адаптивний метод диференційної еволюції Коші є потужним інструментом, за допомогою якого можна здійснювати параметричний синтез оптичних систем ширококутних об'єктивів.

Наступні дослідження раціонально направити на пошук та застосування удосконалених методів глобальної оптимізації, адже дієздатність та результативність таких методів підтверджується на практиці під час проектування ОС довільного призначення.

Література

1. *Choi T. J.* An adaptive Cauchy differential evolution algorithm for global numerical optimization / Choi T. J., Ahn C. W., An J. // The Scientific World Journal, Vol. 2013, 2013. 12 pages.
2. *Choi T. J.* An Adaptive Cauchy Differential Evolution Algorithm with Bias Strategy Adaptation Mechanism for Global Numerical Optimization / T. J. Choi, C. W. Ahn // Journal of Computers, Vol. 9, No 9, 2014. pp. 2139 - 2145.
3. *Ali M.* A Numerical Evaluation of Several Stochastic Algorithms on Selected Continuous Global Optimization Test Problems / Ali M., Zabinsky B. // Journal of Global Optimization. Vol. 31, 2005. pp. 635 – 672.
4. *S. Thibault*. Evolutionary Algorithms Applied to Lens Design: Case Study and Analysis / S. Thibault, Ch. Gagne, J. Beaulieu, and M. Parizeau // Proc. of the SPIE International Symposium on Optical Systems Design (EOD 2005), Jena, Germany, September 12-16, 2005. pp. 5962-5968.
5. *Haupt R*. Practical Genetic Algorithms. / Haupt R. Haupt S. // 2004. 253 p.
6. Patent US 8237842 B2. Wide-angle lens and imaging apparatus equipped therewith. Koichi Wakamiya. Filed: Aug. 1, 2008. Publication Date: Feb. 17, 2011.
7. Patent US 8503110 B2. Lens system, wide-angle lens, optical apparatus equipped with lens system, and method for manufacturing lens system. Koichi Oshita. Filed: Sep. 7, 2010. Publication Date: Jul. 5, 2012.

УДК 681.7.067

В. М. Сокуренко, И. С. Буйлов
Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», г. Киев, Украина

АВТОМАТИЧЕСКИЙ РАСЧЕТ ШИРОКОУГОЛЬНЫХ ОБЪЕКТИВОВ

Одной из востребованных задач современной вычислительной оптики является задача полной автоматизации процедуры нахождения параметров оптической системы (ОС), оптимальных по различным критериям. Широко распространенные методы локальной оптимизации имеют существенный недостаток, который заключается в том, что для их результативного применения, как правило, требуется качественная исходная ОС. Поставленную задачу поиска наименьшего значения оценочной функции в заданном пространстве допустимых значений параметров потенциально позволяют решить методы глобальной оптимизации (ГО). В связи с этим в отношении автоматизированного расчета ОС разными авторами было предложено использовать такие методы ГО как имитационный отжиг, генетические алгоритмы и тому подобное. В данной работе численно исследуются возможности адаптивного метода дифференциальной эволюции Коши, предложенного в 2013 году. Алгоритм этого метода отличается наличием внутреннего механизма адаптации параметров-коэффициентов классического метода дифференциального эволюции, а также применением распределения Коши для генерации новых «случайных» значений этих коэффициентов. Указанный выше алгоритм был реализован в собственной компьютерной программе автоматизированного расчета ОС произвольного назначения. В работе осуществлена экспериментальная проверка эффективности реализации выбранного метода при расчете аналогов ОС, предложенных недавно в патентах США.

Ключевые слова: объектив, оптическая система, адаптивный метод дифференциальной эволюции Коши, автоматизированный расчет, глобальная оптимизация.

V. Sokurenko, I. Builov
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

AUTOMATED DESIGN OF WIDE-ANGLE LENS

One of tasks of modern computational optics is the problem of complete automatization of an optical system (OS) design procedure according to different criteria. The widespread local optimization techniques have a significant drawback: initial OSs with good quality are typically required. To solve the problem of finding the lowest value of the evaluation (merit) function in given space of allowed parameters, modern global optimization (GO) methods can be applied. For purpose of automated lens design, different authors have proposed to use such GO techniques as simulation annealing, genetic algorithms, etc. In this paper, the possibilities of one adaptive method (namely,

differential evolution Cauchy, proposed in 2013) are numerically studied. An algorithm of the method is characterized by presence of an internal mechanism for self-adapting the coefficients of a classical differential evolution algorithm. Besides, it incorporates the Cauchy distribution to generate new "random" values of above-mentioned coefficients. The algorithm has been implemented in own computer program, developed for automated lens design. An experimental verification of the method's effectiveness has been done during the design of several OS systems, similar to those, presented recently in US patents.
Keywords: lens, optical system, adaptive Cauchy differential evolution, automated design, global optimization.

Надійшла до редакції
09 червня 2016 року

Рецензовано
05 вересня 2016 року