IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10758

SECURING COLOR IMAGE TRANSMISSION USING COMPRESSION-ENCRYPTION MODEL WITH DYNAMIC KEY GENERATOR AND EFFICIENT SYMMETRIC KEY DISTRIBUTION

Annalakshmi.N[1], Mandapaka Gayathri[1], Mrs.K.Amsavalli M.E.,[2]

UG Scholar, Computer Science Engineering, Anand Institute Of Higher Technology, Chennai, India[1]
Assistant professor, Computer science and Engineering,
Anand Institute of Higher Technology, Kazhipattur, Chennai -603103[2]

Abstract: Color image encryption is important to ensure its confidentiality during its transmission on insecure networks or its storage. A compression-encryption model to solve these problems. This model consists of three processes. The first process is the dynamic symmetric key generation. The second one is the compression process, which is followed by encryption using key streams and S-Boxes that are generated using a chaotic logistic map. The last process is the symmetric key distribution. The asymmetric key is encrypted twice using Rivest-Shamir-Adleman (RSA) to provide both authentication and confidentiality. Then, it is inserted into the cipher image using the End of File (EoF) method. The evaluation shows that the symmetric key generator model can produce a random and dynamic symmetric key. Hence, the image data is safe from ciphertext-only attacks. This model is fast and able to withstand entropy attacks, statistical attacks, differential attacks, and brute-force attacks.

Keywords: Encryption,Decryption,Symmeteric Key,Dynamic key

I. INTRODUCTION

Today, the exchange of data and information is usually carried out through insecure public networks. the use of unsafe communication channels, such as social media, is very vulnerable to the misuse of information by third parties. therefore, it is important to maintain the confidentiality of data, including images, which are sent through unsecured channels.There are two main problems related to the exchange of image data through public networks. firstly, the size of image data is getting bigger because of the need for high image quality. it takes longer to transmit image data. this problem can be overcome by applying a compression method to the data before it is sent. the second problem is the weak security of image data as it uses a public network to distribute image data. this problem can be overcome by encrypting the message using an encryption method. compression and encryption are highly interrelated, and they interact with each other. data compression is done by reducing the redundancy in image data, while data encryption will produce a high level of security if the redundancy in the image data is low. therefore, compression and encryption are often done together to provide the data with a smaller size, good quality, fast transmission, and high security. various techniques for combining compression and encryption methods based on the sequence of processes have been developed with their advantages and disadvantages. based on the process of combining the methods, there are 3 techniques, i.e., encryption-compression compression-encryption and hybrid compression-encryption.all of the above three techniques still implement symmetric cryptography to encode the image data. symmetric encryption is chosen because it is faster than asymmetric encryption. however, symmetric encryption has a few weaknesses in key management, which is one of the important security aspects. the key management issues of symmetric encryption are:

1) the difficulty in generating a symmetric key that cannot be easily predicted by cryptanalyst
2) the need to maintain the confidentiality of symmetrical keys
3) the distribution of the symmetric key.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10758

II. ANALYSIS

The first problem arises because the secret key that is agreed by both the sender and the receiver is usually short for it is to be memorized easily. the secret key that has been shared is referred to as the initial symmetric key. the symmetric key can be used to form session keys. since the strength of symmetric cryptographic algorithms depends on the size of the key, the session key generation scheme must support the generation of a long and random key. a chaotic system can be used to obtain such a key because of its characteristics, such as ergodicity, non-periodicity, and randomicity. many researchers focus on developing chaos-based cryptosystems. to produce a cryptosystem that is safe and strong against the possibility of cryptographic attacks, confusion and diffusion properties must be used, which can be achieved in three stages: block permutation, substitution, and diffusion. still, this model of a cryptosystem is not safe from ciphertext-only attacks because the session key will always be the same if the symmetric key is not changed.the second problem can be solved by using a one-time-key or a dynamic session key. the use of a dynamic session key is expected to improve security and make attacks more difficult. however, the proposed model requires symmetrical keys that have been agreed between the sender and the receiver. in addition to using a one-time-key, symmetric key security is also done by encrypting a public key using elliptic curve cryptosystem (ecc) or rivest-shamir-adleman (rsa). RSA is efficient in the encryption process but inefficient in the decryption process. therefore, to improve the efficiency of RSA decryption, the chinese remainder theorem (crt) algorithm can be used.the third problem involves the distribution of keys among a set of legitimate users while ensuring key confidentiality. the widely used method distributes keys through secure channels that require expensive costs. this method becomes inefficient when the key size is large, the communication is carried out jointly by many users, and each pair of users must always exchange the secret key to be used by them. therefore, it is necessary to develop a more efficient symmetric key distribution model.in image encryption, efficient symmetric key distribution can be achieved by inserting the encrypted symmetric key (cipher key) into the cipher image. the insertion method in the frequency domain, e.g., discrete cosine transform (dct), discrete wavelet transform (dwt), and discrete fourier transform (dft), cannot be used here because it makes the cover image change, even though it is resistant to attacks. the other insertion method is in spatial domains, such as least significant bit (lsb), singular value decomposition (svd), and end of file (eof). although LSB and SVD have advantages in terms of speed and ease of implementation, they make both the cover image and the inserted cipher key change. the EOF method is the most suitable method for this purpose because it does not change either the inserted cipher key or the cover image. A new cryptosystem model that is able to overcome the key management problems and maintain the data security of the transmitted images is proposed. the model consists of three processes. the first process is the generation of dynamic symmetric and session keys, which aims to generate different symmetric and session keys for each image to be transmitted. symmetric keys are created by utilizing the characteristics of the image, dwt 2d transformation, chaos function arnold cat map (acm) and cipher block chaining (cbc) operations. the mechanism will produce symmetric keys that are random, not containing any patterns that can be utilized by the cryptanalyst. the session keys are generated using the chaos-based logistic map. the chaos parameter values are adjusted using the symmetric keys that have been formed previously. thus, the values of the chaos parameters do not need to be exchanged between the sender and the receiver. the second process uses a selective method of compression that is followed by encryption. this process is performed by utilizing three key streams and two s-boxes that are generated using the chaos logistic map. the selective compression and cryptographic processes are performed on the LL subband and LH, HL, HH subbands of the DWT 2d transformation. this separation process is used to improve image data security by encryption using different session keys according to the characteristics of each sub-band. furthermore, the concept of layered encryption using two s-box session keys and one key stream is applied to increase the security in the substitution and permutation stages. the method is applied to each of red, green, and blue channels. the third process is the process of distributing symmetric keys safely and efficiently. this process is started by giving authentication of the sender, continued with the encoding of symmetric keys. the keys are then inserted into the cipher image using the eof method to be sent simultaneously with the cipher image.

The Main Contributions are:

1) A secure key generation model that always generates different keys for each communication session.

2) A cryptosystem model that uses a selective compression-cryptographic method, which is followed by applying the concept of multiple encryptions (super-encipherment) to improve data confidentiality

3) A model of distributing symmetric keys securely and efficiently. the models have been evaluated using several techniques to test the performance.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10758

BLOCK DIAGRAM:

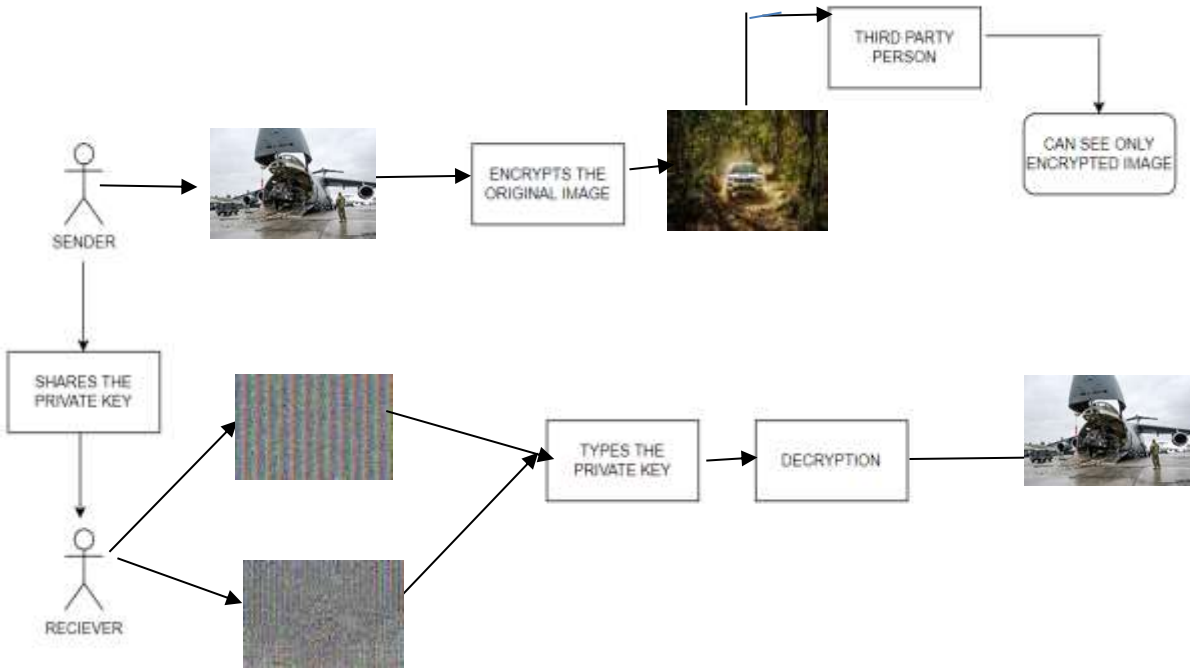


Figure3.1 : Block Diagram

III.SYSTEM REQUIREMENTS

3.1.PROCESSOR:Intel Core i3:

Developed and manufactured by Intel, and first introduced and released in 2010, the **Core i3** is a dual-core computer processor, available for use in both desktop and laptop computers. It is one of three types of processors in the "i" series (also called the Intel Core family of processors).

The Core i3 processor is available in multiple speeds, ranging from 1.30 GHz up to 3.50 GHz, and features either 3 MB or 4 MB of cache. It utilizes either the LGA 1150 or LGA 1155 socket on a motherboard. Core i3 processors are most often found as dual-core, having two cores. However, a select few high-end Core i3 processors are quad-core, featuring four cores.

The most common type of RAM used with a Core i3 processor is DDR3 1333 or DDR3 1600.

Power usage varies for the Core i3 processors:

- Slower speeds (1.30 GHz to 1.80 GHz) use 11.5 W, 15 W or 25 W of power
- Medium speeds (2.00 GHz to 2.50 GHz) use 28 W, 35 W or 37 W of power
- Faster speeds (2.90 GHz to 3.50 GHz) use 35 W, 37 W or 54 W of power

Core i3 processors are often used in laptop computers, due to their lower heat generation and conservative battery usage. Some laptops can be used for up to five or six hours on a single battery charge when running a Core i3 processor.

3.2. DDR2 RAM:

Double Data Rate (DDR) is a common type of memory used as RAM for most every modern processor. First on the scene of this stack of acronyms was Dynamic Random-Access Memory (DRAM), introduced in the 1970s. DRAM is not regulated by a clock. DRAM is asynchronous, i.e., not synchronized by any external influence. This posed a problem in organizing data as it comes in so it can be queued for the process it's associated with. Because DRAM was asynchronous, it was not going to work as fast with processors that were just getting faster. SDRAM is synchronous, and therefore relies on a clock to synchronize signals, creating predictable orderly cycles of data fetches and writes. However, SDRAM transfers data on *one* edge of the clock. DDR SDRAM means that this type of SDRAM fetches data on both the leading

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10758

edge and the falling edge of the clock signal that regulates it, thus the name "Double Data Rate." Prior to DDR, RAM would fetch data only once per clock cycle. Synchronous data lends itself to faster operation when coordinating memory fetches with the processor's requirements.Many people refer to a processor's RAM as simply "DDR", using the terms interchangeably because DDR is so widely used as CPU RAM and has been since the late 1990s. DDR is not flash memory like the kind that is used for Solid State Drives (SSDs), Secure Digital (SD) cards, or Universal Serial Bus (USB) drives. DDR memory is volatile, which means that it loses everything once power is removed.

IV.TECHNOLOGY

4.1 PYTHON

Python features a dynamic type system and automatic memory management. It supports multiple programming paradigms, including object-oriented, imperative, functional and procedural

Python interpreters are available for many operating systems. CPython, the reference implementation of Python, is open source software and has a community-based development model, as do nearly all of Python's other implementations. Python and CPython are managed by the non-profit Python Software Environment.

Python is a multi-paradigm programming language. Object-oriented programming and structured programming are fully supported, and many of its features support functional programming and aspect-oriented programming (including by metaprogramming and meta-objects). Many other paradigms are supported via extensions, including design by contract and logic programming.

Most Python implementations (including CPython) include a read–eval–print loop (REPL), permitting them to function as a command line interpreter for which the user enters statements sequentially and receives results immediately.

Other shells, including IDLE and IPython, add further abilities such as auto-completion, session state retention and syntax highlighting.

As well as standard desktop integrated development environments, there are Web browser-based IDEs; SageMath (intended for developing science and math-related Python programs); Python Anywhere, a browser-based IDE and hosting environment; and Canopy IDE, a commercial Python IDE emphasizing scientific computing..

The language's core philosophy is summarized in the document The Zen of Python (PEP 20), which includes aphorisms such as:[49]

- Beautiful is better than ugly
- Explicit is better than implicit
- Simple is better than complex
- Complex is better than complicated
- Readability counts

Rather than having all of its functionality built into its core, Python was designed to be highly extensible. Compact modularity has made it particularly popular as a means of adding programmable interfaces to existing applications. Van Rossum's vision of a small core language with a large standard library and easily extensible interpreter stemmed from his frustrations with ABC, which espoused the opposite approach.

Python's developers strive to avoid premature optimization, and reject patches to non-critical parts of the CPython reference implementation that would offer marginal increases in speed at the cost of clarity. When speed is important, a Python programmer can move time-critical functions to extension modules written in languages such as C, or use PyPy, a just-in-time compiler. Cython is also available, which translates a Python script into C and makes direct C-level API calls into the Python interpreter.

An important goal of Python's developers is keeping it fun to use. Now it is reflected in the language's name—a tribute to the British comedy group Monty Python[52]—and in occasionally playful approaches to tutorials and reference materials, such as examples that refer to spam and eggs (from a famous Monty Python sketch) instead of the standard foo and bar.

A common neologism in the Python community is pythonic, which can have a wide range of meanings related to program style. To say that code is pythonic is to say that it uses Python idioms well, that it is natural or shows fluency in the language, that it conforms with Python's minimalist philosophy and emphasis on readability. In contrast, code that is difficult to understand or reads like a rough transcription from another programming language is called unpythonic.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10758

Python is meant to be an easily readable language. Its formatting is visually uncluttered, and it often uses English keywords where other languages use punctuation. Unlike many other languages, it does not use curly brackets to delimit blocks, and semicolons after statements are optional. It has fewer syntactic exceptions and special cases than C or Pascal. Python has extensive built-in support for arbitrary precision arithmetic. Integers are transparently switched from the machine-supported maximum fixed-precision (usually 32 or 64 bits), belonging to the python type int, to arbitrary precision, belonging to the Python type long, where needed. The latter have an "L" suffix in their textual representation. (In Python 3, the distinction between the int and long types was eliminated; the behavior is now entirely contained by the int class.) The decimal type/class in module decimal (since version 2.4) provides decimal floating-point numbers to arbitrary precision and several rounding modes. The fraction type in module fractions (since version 2.6) provides arbitrary precision for rational numbers

Python's large standard library, commonly cited as one of its greatest strengths, provides tools suited to many tasks. For Internet-facing applications, many standard formats and protocols such as MIME and HTTP are supported. It includes modules for creating graphical user interfaces, connecting to relational databases, generating pseudorandom numbers, arithmetic with arbitrary precision decimals, manipulating regular expressions, and unit testing.

Some parts of the standard library are covered by specifications (for example, the Web Server Gateway Interface (WSGI) implementation follows PEP 333), but most modules are not. They are specified by their code, internal documentation, and test suites (if supplied). However, because most of the standard library is cross-platform Python code, only a few modules need altering or rewriting for variant implementations.

4.2. ARTIFICIAL INTELLIGENCE:

Artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience. Since the development of the digital computer in the 1940s, it has been demonstrated that computers can be programmed to carry out very complex tasks—as, for example, discovering proofs for mathematical theorems or playing chess—with great proficiency. Still, despite continuing advances in computer processing speed and memory capacity, there are as yet no programs that can match human flexibility over wider domains or in tasks requiring much everyday knowledge. On the other hand, some programs have attained the performance levels of human experts and professionals in performing certain specific tasks, so that artificial intelligence in this limited sense is found in applications as diverse as medical diagnosis, computer search engines, and voice or handwriting recognition. Building an AI system is a careful process of reverse-engineering human traits and capabilities in a machine, and using it's computational prowess to surpass what we are capable of.
To understand How Aritificial Intelligence actually works, one needs to deep dive into the various sub domains of Artificial Intelligence and and understand how those domains could be applied into the various fields of the industry. You can also take up an artificial intelligence course that will help you gain a comprehensive understanding.

- **Machine Learning** : ML teaches a machine how to make inferences and decisions based on past experience. It identifies patterns, analyses past data to infer the meaning of these data points to reach a possible conclusion without having to involve human experience. This **automation** to reach conclusions by evaluating data, saves a human time for businesses and helps them make a better decision.

- **Deep Learning** : Deep Learning ia an ML technique. It teaches a machine to process inputs through layers in order to classify, infer and predict the outcome.

- **Neural Networks** : Neural Networks work on the similar principles as of Human Neural cells. They are a series of algorithms that captures the relationship between various underying variabes and processes the data as a human brain does.

- **Natural Language Processing**c: NLP is a science of reading, understanding, interpreting a language by a machine. Once a machine understands what the user intends to communicate, it responds accordingly.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

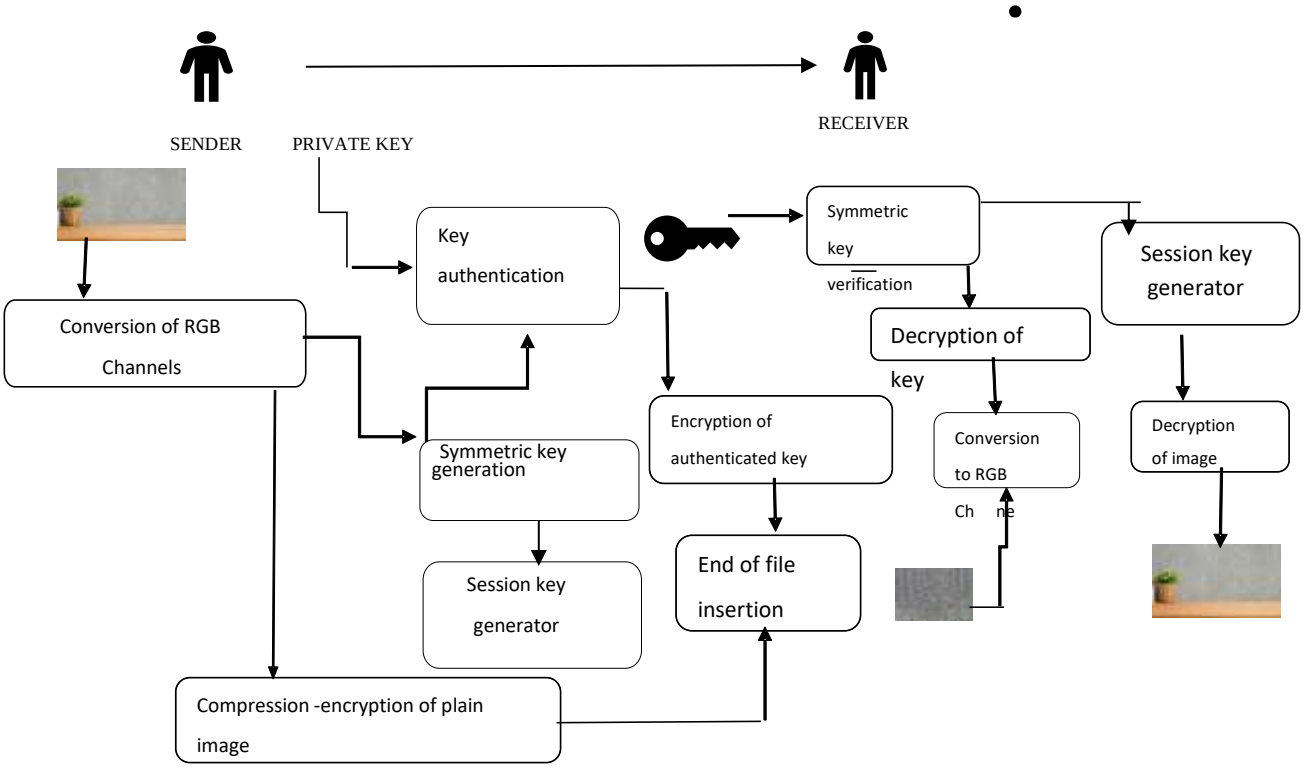
DOI 10.17148/IJARCCE.2021.10758

- **Computer Vision** : Computer vision algorithms tries to understand an image by breaking down an image and studying different parts of the objects. This helps the machine classify and learn from a set of images, to make a better output decision based on previous observations.

- **Cognitive Computing** : Cognitive computing algorithms try to mimic a human brain by anaysing text/speech/images/objects in a manner that a human does and tries to give the desired output.

FRAMEWORK MODEL

Figure4.1 :Framework model



V.CONCLUSION

With the rapid development of communication and computer network technology, the problem of secure transmission of information has received more and more attention, and encryption is an effective means to ensure the secure transmission of information. Due to the large amount of data, strong correlation and high redundancy of the image itself, the traditional encryption method is not suitable for image encryption, so it is necessary to seek a new solution. This research is successful in building a novel approach for improving the security of the color image data that needs to be exchanged and for distributing the symmetric keys that are used for securing the image. The proposed model consists of 3 main stages: a dynamic key generation model, a chaos-based selective compression-encryption model, and a symmetric key distribution model. For the key distribution model, the key that has been authenticated and encrypted is inserted into the cipher image using the EoF method. This is effective which shows the complexity of the overall model of O(mn). It is also able to reduce data redundancy but still capable of maintaining the quality of the reconstructed image data.

REFERENCES

[1] A. Belazi, A. El-Latif, and S. Belghith, ‘‘A novel image encryption scheme based on substitution-permutation network and chaos,’’ Signal Process., vol. 128, pp. 155–170, Nov. 2016.

[2] X. Kang, Z. Han, A. Yu, and P. Duan, ‘‘Double random scrambling encoding in the RPMPFrHT domain,’’ in Proc. IEEE Int. Conf. Image Process. (ICIP), Sep. 2017.

[3] J. Lang, ‘‘Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain,’’ Opt. Commun., vol. 338, pp. 181–192, Mar. 2015.

[4] C. Pak and L. Huang, ‘‘A new color image encryption using combination of the 1D chaotic map,’’ Signal Process., vol. 138, pp. 129–137, Sep. 2017.

[5] L. Xu, X. Gou, Z. Li, and J. Li, ‘‘A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion,’’ Opt. Lasers Eng., vol. 91, pp. 41–52, Apr. 2017.