Secure Optical Image Encryption and Data Hiding Technique in Compression Domain Using Dual Key-Based Bit Swapping

L. Anusree and M. Abdul Rahiman

Abstract Over the last twenty years or more, researchers have suggested a significant variety of optical information security systems that take advantage of the inherent benefits of optics to outperform existing digital security methods. Along with encryption, hiding secret data plays added advantages in various applications such as defense, biomedical diagnostics, and other security-related imaging applications. In this work, a new technique is proposed along with secret data hiding in the compressed bitstream. American Standard Code For Information Interchange (ASCII) representation is used directly to hide the secret text into the image using least significant bit (LSB) replacing technique. To evaluate the performance, various performance measures such as correlation coefficient (CC) of 0.99, peak signal to noise ratio (PSNR) of 28.53, mean square errors (MSE) of 0.0056, structural similarity index measure (SSIM) of 0.99, mean absolute errors (MAE) of 0.015, and root mean square error (RMSE) of 0.056 values are calculated. From the acquired result, it is quite obvious that this work delivers 0.2% high performance when compared to existing optical encryption methods.

Keywords Optical information · Data hiding · Image compression · Lossless compression · ASCII · Bit swapping

Introduction

Convert bit sequences with high coding capacity and efficient authentication are required in modern high-security encryption and optical communication. As photonic information technology advances, secret tags with high density and security are urgently needed and have piqued curiosity [1]. Information security is becoming

L. Anusree (✉)
LBSITW, Thiruvananthapuram, Kerala, India

M. A. Rahiman
LBSCST, Thiruvananthapuram, Kerala, India

V. Bindhu et al. (eds.), *Proceedings of Third International Conference on Communication, Computing and Electronics Systems*, Lecture Notes in Electrical Engineering 844,
https://doi.org/10.1007/978-981-16-8862-1_6

increasingly important in a variety of applications, such as secure communication routes, secure identification, and safe data storage. Optical approaches have been developed in recent years as prospective alternatives in a variety of specific applications. Because of the exceptional capabilities of optical methods, there is a growing interest in using optical methods to build more complex information security solutions. The groundwork for today's optical encryption technologies was laid by Refregier and Javidi. The recorded speckle pattern is white noise, and no information is shown graphically. To encode an image, double random phase encoding (DRPE) was originally suggested by applying two uncorrelated random phase-only masks within the input image plane and the Fourier transform domain. The plaintext may be transformed into stationary text using the DRPE. Many researchers have been inspired by the DRPE system and have further refined it by adopting it [2].

Integral imaging is a true three-dimensional (3D) imaging technology based on an integrated photographic method that allows us just to record numerous two-dimensional (2D) images from a 3D scene using a lenslet array. These 2D images are referred to as elemental images since they contain the direction and brightness information of a 3D scene [3]. In addition to random phase encryption, characteristics of a light field, including spatial ranges and polarized phases, can be employed as encoding and decoding keys. A technique of space-based optical encryption in which the plaintext picture pixels are randomly relocated to various depth ranges prior to diffractive light field transmission [4].

Deep learning method is also used for optical encryption [5]. Depending on the input, noise following decoding might result in the loss of minor details, prompting the addition of approaches in which the input is encrypted in parts, making use of the fact that each piece is simpler and less impacted by noise [6]. Individual parts can be multiplexed into a single ciphertext, which can result in a significant improvement in decryption quality when recovered. Yet, because each component must be processed separately, the time and effort necessary to access the encrypted data are increased [7].

In this work, a new technique is proposed to perform optical image encryption in the compressed bitstream. The encryption is performed using dual key-based bit patch swapping. Also, the secret text is inserted in the image using LSB replacing technique.

The remainder of this work is structured as follows: Section 2 describes the optical encryption techniques that have been published. Section 3 discusses the suggested optical encryption technology. Section 4 explains the outcome and discussion of the suggested approach, comparative research, and analysis. Finally, Sect. 5, explored the conclusion.

Literature Survey

Previously, a large number of works were presented to implement the optical encryption approach. These various strategies aim to minimize design complexity by

improving the algorithm's architecture. This section contains some of the previously suggested efforts for performing optical encryption implementation.

Shuming Jiao et al. a realistic technique for optically encrypting and decrypting a grayscale image using QR codes is provided, which is compatible with standard QR code producers and readers. A grayscale image is converted to a decimal number sequence, which may then be translated to numerous QR codes. A numerical simulation depicts the full process of encrypting and decrypting a grayscale image using this approach. The findings show that a grayscale image may be effectively encrypted and lastly retrieved in a noise-free manner using the suggested approach [8].

Yonggang Su et al. proposed an optical encoding based on the full trinary tree structure for multiple color images. The approach uses encryption modules as branched nodes and raw image components of color as leaf nodes. Each encryption modulesencodes three input images into a complex function, which is subsequently encrypted to a real-value image using phase truncated Fresnel transformations and random amplitude-phase masks. This encryption approach may encrypt several color images into a real-value grayscale cipher image while separating the encryption and decryption routes for each color image. This encryption method enables high-security authority management among several users [9]. Furthermore, the suggested system has benefits such as strong resilience against diverse attacks and good encryption efficiency. Furthermore, when the quantity of plain color photos grows, the excellent quality of the decrypted color images can be retained with embedding capacity enhancement using a hybrid technique [10].

Kang Yi et al. proposed optical encryption using ghost imaging and public key cryptography. The RSA public key algorithm is utilized to overcome the key distribution problem in this system. In addition, the cost of setting up security channels is decreased. In the event of fewer ciphertexts, the use of the CS method provides good quality plaintext reconstruction. This system combines the benefits of the RSA public key algorithm with ghost imaging (GI) encryption techniques to provide security and ease for efficient data transmission [11]. The simulation results validate the method's viability. It has a high level of resistance to statistical analysis and repeated attacks, as well as a high level of resilience [12].

Lina Zhou et al. proposed diffractive imaging optical encryption is subject to learning-based attacks. An opponent can recover anonymous plaintexts from provided ciphertexts using a machine learning assault. In this technique, end-to-end learning is utilized to derive a superior mapping link between plaintexts and ciphertext. Unauthorized users can use trained supervised learning to retrieve unknown plaintexts from provided ciphertexts without the need for optical encryption key retrieval or estimation [13]. As optical experimental and simulation results show, the proposed learning approach is practical and useful for assessing the susceptibility of optical encryption systems with embedding capacity enhancement using a hybrid technique. The trained learning model's ubiquity is also proven, as is the reality that the machine learning model taught to use a database is powerful enough to target multiple databases [14].

Kang Yi et al. proposed a ghost imaging-based camouflaged encryption technique is suggested. A light source lights a camouflaged image with certain modulated patterns during the encryption process, and a produced sequence of intensity is communicated to the recipient as ciphertext. Authorized receivers and prospective eavesdroppers obtain the ciphertext [15]. Only authorized receivers with keys may acquire the hidden image, but eavesdroppers can only obtain camouflaged images if they steal both the ciphertext and the keys. The camouflaged image hides the secret image, which preserves its security by confounding the eavesdropper [16]. GauravVerma et al. proposed based on the phase retrieval method and the phase truncated Fourier transforms (PTFT) scheme, an asymmetric cryptosystem for optical image encryption utilising biometric keys, which tackles the issue of key distribution with increased security in the optical encryption process [17].

It is obvious from the preceding discussion that numerous works have previously been offered to undertake to increase the robustness. The primary disadvantages of prior efforts are their poor quality and lack of security. The major purpose of this effort is outlined in the parts below:

1. To improve the security of optical encryption.
2. To preserve the quality of the image.
3. To create a versatile methodology for developing real-time applications.

The details of the implementation of the proposed work are given below sections.

Secure Optical Image Encryption and Data Hiding Technique in Compression Domain Using Dual Key-Based Bit Swapping

In this work, first, read the image and resize it into 128 × 128. Using bitplane slicing extract LSB. In lossless compression extracting bitstream. Then convert bitstream to matrix blocks. Using two secret keys swap the position of bit randomly. Then it can be converted into the bitstream. The bitstream converts to matrix patch and reverse swapping using two secret keys. After swapping bits converted into the bitstream and decompress the image. Using bitplane slicing extract LSB and ASCII number of image. Finally, receive the secret text behind in the image. Figure 1 shows the secure optical image encryption and data hiding technique in compression domain using dual key-based bit swapping. Fig. 2 showswork flow diagram of proposed optical encryption.

Bıtplane Slicing

Bit plane slicing is a way of expressing an image by using one or more byte bits for each pixel. Only most significant bit (MSB) may be used to represent a pixel,

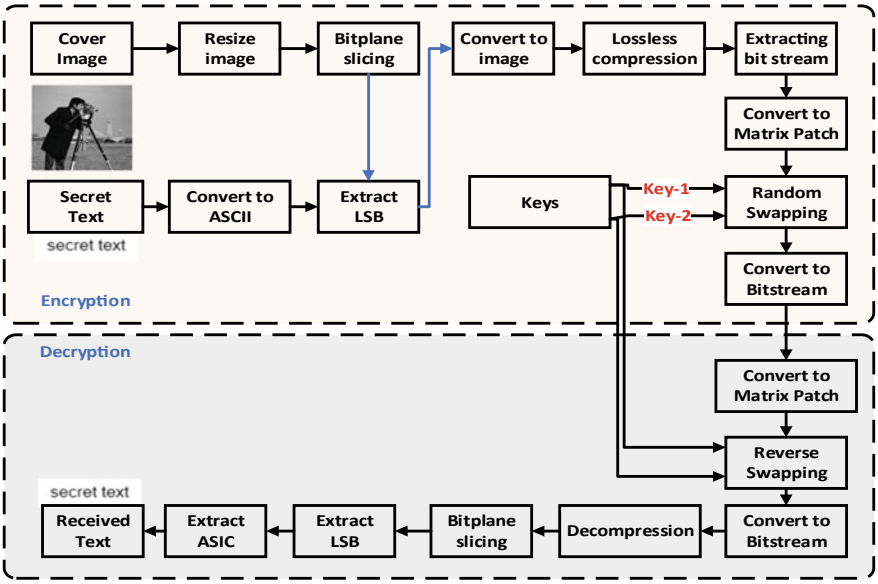

Fig. 1 Secure optical image encryption and data hiding technique in compression domain using dual key-based bit swapping

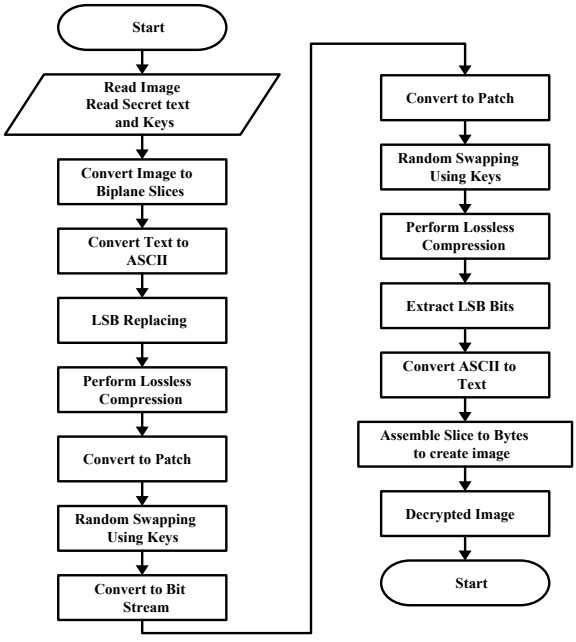

Fig. 2 Work flow diagram of proposed optical encryption

reducing the original gray level to a binary picture. Converting a grayscale image to a binary image is one of the three major aims of bit plane slicing. The supplied image is a 3-bit image because it has a maximum gray level of 7. Then convert the image to binary and separate the bit planes.

Extract LSB

The LSB is the lowest bit in a series of binary integers, positioned at the far right of a string. The least significant bit is also known as the rightmost bit in positional notation. It is the inverse of the MSB, which has the greatest value in a binary number with multiple bits, as well as the number closest to the right. The importance of a bit in a multi-bit binary number diminishes as it approaches the least significant bit. Because it is binary, the most important bit can only be 1 or 0 [18].

Algorithm 0.1 shows the algorithm of an image encryption. Take the input image (I) with secret text (x) and two keys such as $k1$, $k2$. Firstly resize the input image (I_1) and slice bitplane wise (I_{slices}) and then extract LSB named as (I_{lsb}). Let take ASCII value of the text (X_{asci}) and replace the LSB of the ASCII as I_2.Then do lossless compression of the image (I_{stram}). Then convert the stream into patches (I_{sets}). Random swapping method is used for image encyption with $k1$, $k2$ keys and I_{sets}. Finally get the secret image $I_{\text{secret.}}$

Algorithm: 1

Input:	Input Image i, Secret Text x, Keys k1, k2
Output:	Encrypted Image
1	I_1 = Resize image(I)
2	I_{Slices} = Bitplane Slicing(I_1)
3	I_{lsb} = Extract LSB(I_{Slices})
4	X_{asci} = ASCII(x)
5	I_2 = LSB Replacing($X_{asci,}I_{lsb}$)
6	I_{stram} = Lossless Compression(I_2)
7	I_{sets} = Convert to Patch(I_{stram})
8	I_{secret} = Random swaping($I_{sets,}k_1,k_2$)

Losslessn Bit Compressıon

Lossless compression is a type of data compression algorithm that allows the compressed data to be completely rebuilt from the original data. Lossy compression, on the other hand, allows just an approximation of the original data to be reconstructed, but with significantly enhanced compression speeds. Lossless compression is employed when the original and decompressed data must be the same, or when changes from the original data would be detrimental. In this work, Huffman coding method can be used.

Each character, symbols and numerical value has distict ASCII, binary codes seperately. Table 1 shows the distinct binaryvalues of some characters. This method generates binary tree nodes. These may be kept in a standard array, the length of which is defined by the amount of symbols. A node can either be a leaf or an inner node. To begin, every nodes are leaf nodes that give the symbol, the weight of the symbol, optionally, a link to a parent node, which simplifies comprehending the code from a leaf node. Internal nodes have a weight, two-child node connections, and a relationship to a parent node that is optional. Following the left child is denoted by bit '0,' whereas following the right child is denoted by bit '1.' A fully grown tree can contain up to n leaf nodes and n-1 inner nodes.

A Huffman tree is used to generate the most optimal code lengths by eliminating superfluous symbols. The procedure starts with leaf nodes, which store the probability of the symbols that signify. The algorithm then selects the two nodes only with smallest probability and constructs a new internal node with these two as children. The weight of the new node is set to the sum of its children's weights. Then, repeat the process on the new internal node and the other nodes (excluding the two leaf nodes) so there is only one node left, which is the root of Huffman tree. Figure 2 shows compressed bitstream.

Decompression is actually turning a stream of prefixed code to single byte values, which is typically accomplished by visiting the Huffman tree node to nodes for every bit from the input stream is received. The Huffman tree should be rebuilt before this can happen. When character frequency is pretty consistent, the tree can be rebuild and therefore utilized each time, just at cost of certain compression performance.

Table 1 Distinct binary values of some characters

Character	Binary code	ASCII code
E	01000101	069
e	01100101	101
M	01001101	077
m	01101101	109
p	01110000	112

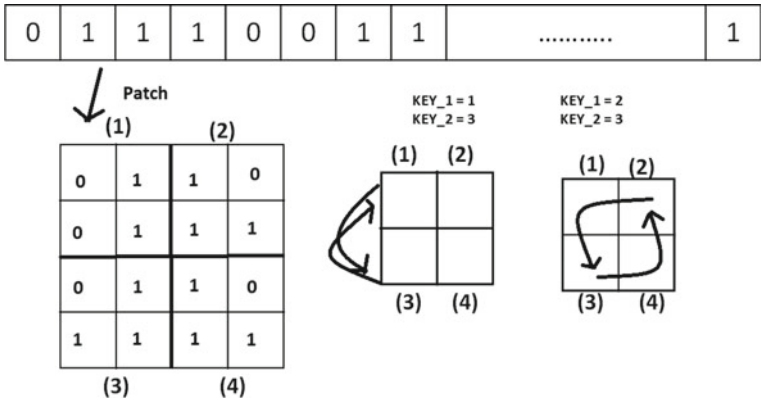

Fig. 3 Compressed bit stream

Bitstream

A bitstream is a bit sequence, sometimes referred to as a binary sequence. A bytestream is a collection of bytes. Because each byte is typically an 8-bit value, the terms octet stream and octet stream are frequently used interchangeably. Because one octet can be encoded as a series of 8 bits in a variety of ways, there is no distinct and direct conversion between bytestreams and bitstreams (Fig. 3).

Results and Dıscussıon

This section discusses the outcomes of numerical simulations performed to determine the efficacy and robustness of the suggested solution. This work is done by MATLAB R2020b using a computer with CPU Intel(R) Core(TM) i5-3320 M CPU @ 1.60 GHz,1 0.60 GHz, and 4 GB of RAM. The dataset images with size 256×256 pixel as input sample used as the cameraman and mandrill. Figure 4 sample images from natural image database from Kaggle.

PSNR

The PSNR is the proportion of the signal's maximum potential strength to the power of completely corrupted input, which influences the accuracy of which it is represented [19].

$$\text{PSNR} = 20.\log_{10}\text{MAX}_{PY} - 10.\log_{10}\text{MSE} \tag{1}$$

Fig. 4 Sample images used for image encryption

where MAX_{PY} represents a maximum image pixel value.

CC

The CC is a graphical representation of a type of correlation, which is a statistical relationship between these two variables. The variables may be two columns from a given set of data or two components of a quantitative probability distribution with the good distribution [20].

$$\mathrm{CC}(K,k) = \frac{M\{[K - M(K)][k - M(k)]\}}{M\left\{[K - M(K)]^2\right\} M\left\{[k - M(k)]^2\right\}} \tag{2}$$

Here K and k represent the plain image and decrypted image.

SSIM

SSIM is a perspective paradigm that treats image loss as a perceived shift in structural details while often integrating core visual effects including intensity of light masking and intensity masking concepts [21].

$$\mathrm{SSIM}(i,\ j) = \frac{\left(2k_i k_j + r1\right)\left(2l_{ij} + r2\right)}{\left(k_i^2 + k_j^2 + r1\right)\left(l_i^2 + l_j^2 + r2\right)} \tag{3}$$

where k_i is the average of i, k_j is the average of j, k_i^2 variance of i, k_j^2 variance of j, l_{ij} the covariance of i and j, $r1$ and $r2$ are two variables to stabilize the division with weak denominator.

MSE

The MSE is a measure of an estimator's consistency; it is often non-negative, with values closest to zero being greater. The distinction between the original and decrypted images is represented by MSE [22].

$$\text{MSE} = \frac{1}{Px*Px} \sum_{i=1}^{Px} \sum_{j=1}^{Px} |\hat{I}(i, j) - I(i, j)|^2 \tag{4}$$

where $Px*Px$ denotes the number of image pixels, $\hat{I}(i, j)$, $I(i, j)$. signify original image values, decrypted image values, and at that pixel value (i, j).

RMSE

The RMSE is used to calculate the residuals' standard deviation. Residuals are a metric about how far apart the data points are all from the regression line; RMSE is a measure of how evenly distributed these residuals are. In other words, it denotes how dense the data is along the best fit line.

$$\text{RMSE} = \sqrt{\overline{E - K}} \tag{5}$$

where E is the expected value and K is known results.

MAE

MAE is a statistical aessment of error among matched data representing the same phenomenon. Comparisons of predicted vs observed future time vs starting time, as well as one measuring technique versus another.

$$\text{MAE} = \frac{\sum_{I=1}^{N} |Y_I - X_I|}{N} \tag{6}$$

where N is the number of predictions, Y_I is the vector of observed values of the variable, X_I is the predicted values.

From Table 2 shows the better comparative performances are CC, PSNR, and MSE in previous works. This work has higher CC, PSNR, and lower MSE with compared to other previous methods. Double random polarization encoding (DRPO) returns only the PSNR values like 17.54, MAE of 0.05, and RMSE of 0.12. Trinary

Table 2 Comparative performance of previous works

Method	CC	PSNR	MSE	SSIM	MAE	RMSE
DRPO [6]	0.76	17.54	0.12	0.74	0.05	0.12
TTS [9]	0.65	–	0.10	–	–	0.26
GI [11]	0.97	–	–	0.93	0.43	0.11
DI [13]	0.63	33.17	–	–	–	0.101
CGI [15]	0.78	–	0.09	–	0.16	–
This work	0.99	35.53	0.0056	0.99	0.015	0.056

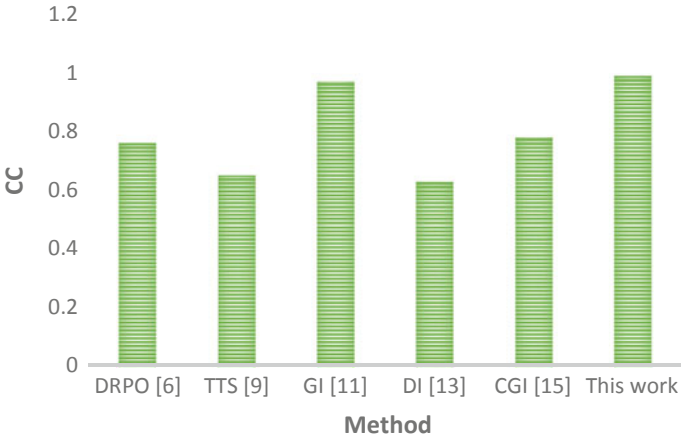

Fig. 5 Comparative performance of CC

tree structure (TTS) has CC of 0.65. The GI method returns the CC of 0.97. The diffractive imaging (DI) method has 33.17 PSNR only. Compressive ghost imaging (CGI) has 0.78 CC only. Figure 5 shows comparative performance of CC and Fig. 6. Comparative performance of PSNR. Fig. 7 shows comparative performance of PSNR with noise density.

Conclusion

This work experimentally demonstrates optical encryption in the compressed bitstream. A dual key-based binary patch swapping technique is used in this work to perform image encryption. Secret data hiding is performed LSB replacing technique followed by ASCII conversion. To validate the feasibility and effectiveness of the suggested technique, simulations, and optical tests were carried out. The suggested optical encryption technique can improve their security while also holding the potential of additional advancements in optical encryption cryptanalysis. From the obtained

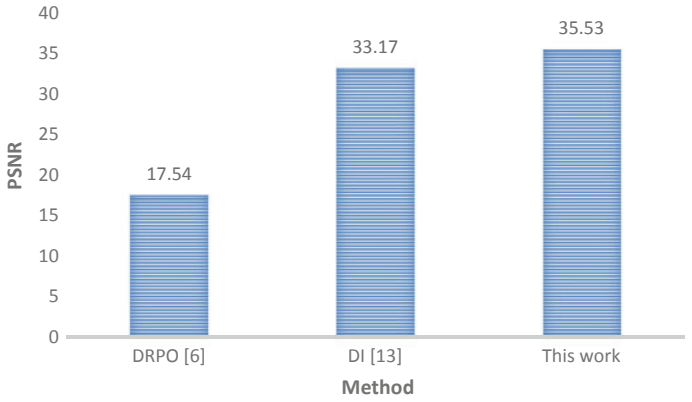

Fig. 6 Comparative performance of PSNR

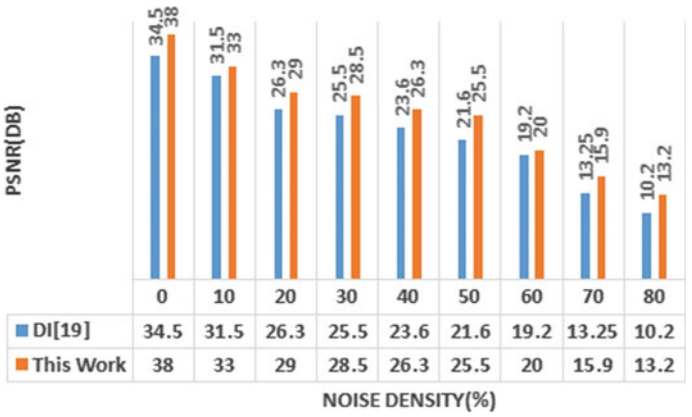

Fig. 7 Comparative performance of PSNR with noise density

result, it is very clear that this work provides good performance when compared to conventional optical encryption standards.

References

1. Gao, Z, Wang K, Yan Y, Yao J, Zhao YS (2021) Smart responsive organic microlasers with multiple emission states for high-security optical encryption. Nat Sci Rev 8(2):nwaa162
2. Zhou L, Xiao Y, Chen W (2019) Machine-learning attacks on interference-based optical encryption: experimental demonstration. Opt Express 27(18):26143–26154
3. Li X, Zhao M, Xing Y, Li L, Kim S-T, Zhou X, Wang Q-H (2017) Optical encryption via monospectral integral imaging. Opt Express 25(25):31516–31527

4. Haoxiang W, Smys S (2021) Big data analysis and perturbation using data mining algorithm. J Soft Comput Paradigm (JSCP) 3(01):19–28
5. Ranganathan G (2021) A study to find facts behind preprocessing on deep learning algorithms. J Innovative Image Proc (JIIP) 3(01):66–74
6. Jiao S, Gao Y, Lei T, Yuan X (2020) Known-plaintext attack to optical encryption systems with space and polarization encoding. Opt Express 28(6):8085–8097
7. Zea AV, Barrera JF, Torroba R (2017) Innovative speckle noise reduction procedure in optical encryption. J Opt 19(5):055704
8. Jiao S, Zou W, Li X (2017) QR code based noise-free optical encryption and decryption of a gray scale image. Opt Commun 387:235–240
9. Su Y, Tang C, Gao G, Fan G, Lei Z, Tang S (2017) Optical encryption scheme for multiple color images using complete trinary tree structure. Opt Lasers Eng 98:46–55
10. Manoharan JS (2012) Embedding capacity enhancement using a hybrid technique for medical images. Eur J Sci Res 75(1):25–38
11. Yi K, Leihong Z, Dawei Z (2018) Optical encryption based on ghost imaging and public key cryptography. Opt Lasers Eng 111:58–64
12. Xi S, Nana Y, Wang X, Ying M, Dong Z, Zhu Q, Wang W, Wang H (2019) Optical encryption method of multiple-image based on θ modulation and computer-generated hologram. Opt Commun 445:19–23
13. Zhou L, Xiao Y, Chen W (2020) Vulnerability to machine learning attacks of optical encryption based on diffractive imaging. Opt Lasers Eng 125:105858
14. Kumar P, Joseph J, Singh K (2016) Double random phase encoding based op-tical encryption systems using some linear canonical transforms: weaknesses and counter-measures. In: Linear canonical transforms. Springer, New York, pp 367–396
15. Yi K, Leihong Z, Hualong Y, Mantong Z, Kanwal S, Dawei Z (2020) Camouflaged optical encryption based on compressive ghost imaging. Opt Lasers Eng 134:106154
16. Liu J, Bai T, Shen X, Dou S, Lin C, Cai J (2017) Parallel en-cryption for multi-channel images based on an optical joint transform correlator. Opt Commun 396:174–184
17. Verma G, Liao M, Dajiang L, He W, Peng X, Sinha A (2019) An optical asymmetric encryption scheme with biometric keys. Opt Lasers Eng 116:32–40
18. El-Shafai W, Almomani IM, Alkhayer A (2021) Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication. IEEE Access 9:35004–35026
19. Chen W, Chen X (2014) Iterative phase retrieval for simultaneously generating two phase-only masks with silhouette removal in interference-based optical encryption. Opt Commun 331:133–138
20. Liu J, Bai T, Shen X, Dou S, Lin C, Cai J (2017) Parallel encryption for multi-channel images based on an optical joint transform correlator. Opt Commun 396:174–184
21. Mohammed EA, Saadon HL (2019) Sparse phase information for secure optical double-image encryption and authentication. Opt Laser Technol 118:13–19
22. Sui L, Lu H, Ning X, Wang Y (2014) Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain. Opt Eng 53(2):026108