A hybrid encryption scheme based on optical scanning cryptography and Fibonacci–Lucas transformation

Cite as: AIP Advances **11**, 015117 (2021); https://doi.org/10.1063/5.0030619
Submitted: 24 September 2020 • Accepted: 30 November 2020 • Published Online: 08 January 2021

A. Meril Cyriac and B. Sheeja M. K.

A hybrid encryption scheme based on optical scanning cryptography and Fibonacci–Lucas transformation

Cite as: AIP Advances 11, 015117 (2021); doi: 10.1063/5.0030619
Submitted: 24 September 2020 • Accepted: 30 November 2020 •
Published Online: 8 January 2021

A. Meril Cyriac[1,2,3,a] and B. Sheeja M. K.[1,2]

AFFILIATIONS

[1] SCT College of Engineering, Kerala 695018, India
[2] APJ Abdul Kalam Technological University, Kerala 695016, India
[3] LBS Institute of Technology for Women, Kerala 695012, India

[a] Author to whom correspondence should be addressed: meril_cyriac@yahoo.co.in

ABSTRACT

This paper describes a new opto-hybrid technique of two-stage encryption for the secure transmission and reception of sensitive information contained in the form of images and data. An advanced encryption–decryption technique based on optical scanning holography (optical scanning cryptography) and Fibonacci–Lucas transformation is proposed. The first stage of this hybrid system includes a point spread function engineered optical scanning cryptographic system. A new key based on fused biometric array is used in this stage. A digital encryption strategy follows this stage. This hybrid encryption scheme can be used for the secure transfer and storage of medical images in the Internet, especially in cloud-based services. The quantitative analysis is performed using different figure of merits. The quantitative investigations have been conducted through computer simulations. The parameters analyzed for establishing the performance characteristics of this system are Structural Similarity Index, Correlation Coefficient, Maximum Absolute Deviation, etc. This system shows a remarkable performance improvement during encryption. The method can be explicitly used in the radiograph image transfer over the Internet for telemedicine applications.

I. INTRODUCTION

The whole digital world today enforces an extended demand for information security and confidentiality at various levels of communication. The current field of interest includes secret transfer of personal data, medical data, and radiograph records of patients, restricted defense and intelligence information of countries, data related to examinations, etc. Medical images are regarded as important and sensitive data in the medical informatics systems. The confidentiality of health records are of primary concern while dealing with telemedicine or tele-health platforms. Medical image security in both intranet and Internet faces severe threats. Except for the intranet environment, medical image transmission over wired or wireless networks has elevated in demand. Cryptographic methods and encryption standards are revolutionary methods of securing information that transforms the original information to an unreadable format. To retrieve the original information, knowledge about encryption keys and encryption methods is required. As an advancement of the primary image encryption, optical image encryption methods have been developed. The optical means of encryption has the advantage of high speed and many degrees of freedom. Coherent optical systems are used for implementing most investigated optical encryption techniques. Refregier and Javidi first proposed and implemented this optical image encryption.[1] The above optical encryption uses the Double Random Phase Encoding (DRPE). This is the most established and well implemented optical encryption methodology.[2–9] Rajput and Nishchal introduced another implementation of DRPE with fractional Fourier transform.[10] Instead of using random phase mask, Zamran *et al.* proposed[11] a scheme that uses deterministic phase masks. Others also developed various optical image encryption schemes.[12–19] References 20 and 21 employ the technique of compressive sensing for image encryption. Multiple image encryption based on optical methods is also implemented.[22,23]

The aforementioned optical encryption uses coherent techniques. However, there are only a few incoherent optical encryption techniques implemented until now. These offer better Signal-to-Noise ratio (S/N) compared with the coherent systems. In conventional incoherent optical systems, the intensity of the object is manipulated by real and positive Point Spread Functions (PSFs). This gives an extra bonus that limits the way one can access the information. Optical scanning holography is one such example.[24–27] Advances in OSH and OSC are implemented in Refs. 28–30. The OSC, by using biometric key, was proposed by Tang and Zhang.[31] Applying this principle, OSC for multidepth objects is discussed in Ref. 32. More sophisticated digital encryptions are done with the help of chaotic maps, and other diffusion models are also implemented.[33–41] Recently, several research studies on encryption schemes based on optical, chaotic, or both have been implemented.[42–57]

A hybrid encryption scheme that uses incoherent holography followed by Fibonacci–Lucas transform[58] is proposed here. The first stage encryption uses OSC with Fused Biometric Array (FBA) key. The second high-security level is provided by the application of a post-processing step on the encrypted hologram. Fibonacci–Lucas transformation provides the second stage encryption. The technique finds applications in securing large sized e-documents or medical documents safe.

This paper is arranged as follows. Section II explains the basic theory behind the cryptographic system design. The succeeding subsections of Sec. II deal with the Optical Scanning Cryptography with enhanced security. Section III contains the results of the proposed method. For effective evaluation of the proposed methodology, various figure of merits like Correlation Coefficient (CC) analysis, Structural Similarity Index Measure (SSIM), maximum deviation analysis, etc. are taken into account. The proposed system is tested against differential attacks also.

II. THE SYSTEM DESIGN

Due to the recent progress in the development of optical components and their improved and reliable performance, and the effectiveness of chaotic maps in scrambling the information randomly, a two-layer encryption–decryption system using these concepts is designed.

A. Cryptographic system through optical scanning (OSC)

The section deals with the basic theory of optical scanning cryptography. Figure 1 shows the optical setup of encryption and decryption. Here, the traditional pupil set is used. Figure 2 represents the flowchart for the simulation of the optical setup of OSC.

1. Encryption

A terahertz optical source, such as laser or visible light, acts as the light source. A beam splitter divides the light into two, and one of its frequencies is slightly shifted and passed to two pupils. These two pupils, $p_1(x, y)$ and $q_1(x, y)$, are illuminated by the laser beam of angular frequencies $\boldsymbol{\Omega}$ and $\boldsymbol{\Omega} + \omega$. The beam combiner combines two beams. The combined beam passes through a lens, and it is the scanning beam, which is used for 2D scanning of the object or image to be encrypted. The amplitude of object to be encrypted is denoted by $U_0(x, y, z_c)$. Here, z_c (coding distance) represents the distance of object from the back focal plane of the lens. The X–Y scanner performs 2D scanning over the object.

The photodetector collects all the light transmitted from the object. The subsequent step is the electronic processing. In electronic processing stage, the current from the photodetector is given to a narrow Band Pass Filter (BPF) tuned at frequency ω, which delivers a heterodyne current $i_\omega(x, y, z_c)$. This current is demodulated by an electronic multiplier and a Low Pass Filter (LPF), which forms a lock-in amplifier. By multiplying the incoming signal $i_\omega(x, y, z_c)$ by $\cos(\omega t)$ and $\sin(\omega t)$ and through low-pass filtering, we obtain two signals, $i_{\cos}(x, y, z_c)$ and $i_{\sin}(x, y, z_c)$, respectively, which can be added in a complex way with the aid of a computer to give a final encrypted image, $i(x, y, z_c)$,

$$i(x, y, z_c) = i\cos(x, y, z_c) + j i\sin(x, y, z_c). \tag{1}$$

The optical transfer function of the encryption stage at coding distance z_c is

$$OTF\omega(k_x, k_y, z_C) = C1 \iint C2 p_1^*(x, y) q_1 \times \left(x + \frac{f}{k_0}k_x, y + \frac{f}{k_0}k_y\right) dx dy, \tag{2}$$

$$C1 = exp\left[j\frac{z_c}{k_0}(k_x^2 + k_y^2)\right], \tag{3}$$

$$C2 = exp\left[j\frac{z_c}{k_0}(xk_x + yk_y)\right], \tag{4}$$

where k_0 is the wave number. Here, only the intensity of the input pattern is processed and hence called incoherent system. OTF is determined by pupil function $p_1(x, y)$ and $q_1(x, y)$. Set $q_1(x, y)$ as a pinhole and $p_1(x, y)$ as a delta function. The derived OTF is

$$OTF\omega(k_x, k_y, z_c) = exp\left[-j\frac{z_c}{k_0}(k_x^2 + k_y^2)\right] p1^*\left(\frac{-f}{k_0}kx, \frac{-f}{k_0}ky\right). \tag{5}$$

2. Decryption

For decryption, the optical system is the same and the laser beams are now scanning pinhole. This helps in retrieving the key for the transmission section. Through electronic processing circuitry, the output of the photodetector will then be processed. The process can be repeated but by replacing z_c with z_d. Here, choose $p_1(x, y)$ as a pinhole and keep $q_1(x, y)$ as is,

$$OTF\omega(k_x, k_y, z_d) = exp\left[-j\frac{z_c}{k_0}(k_x^2 + k_y^2)\right] p1^*\left(\frac{-f}{k_0}k_x, \frac{-f}{k_0}k_y\right)\Big]. \tag{6}$$

This is the output generated at the decryption stage, where the decryption key has been inserted into the stage. The information is now stored in the digital computer to be used later to decrypt the information.

B. Fibonacci–Lucas transformation

Fibonacci–Lucas transformation[58] is a 2D transformation that is specially meant for the encryption of images. The Lucas series is a Fibonacci series' special case.

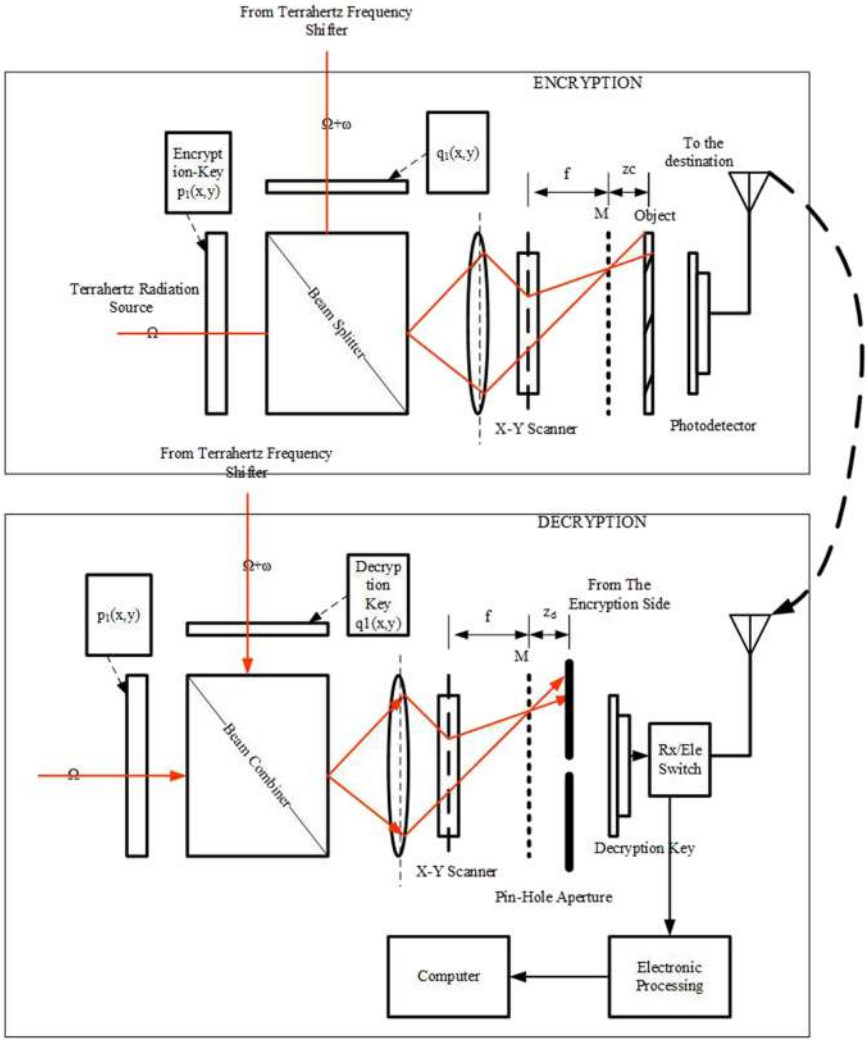

FIG. 1. Optical setup of optical scanning cryptography.

Several special cases of the Fibonacci series can be constructed by changing the seed values. By choosing an appropriate seed value for the Fibonacci series and selecting the same seed value for the Lucas series, a new transformation can be achieved. The Fibonacci–Lucas transformation is described as follows:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\, N. \tag{7}$$

Here, F_n is given by

$$F_n = \begin{cases} 0, & \text{if } n = 1 \\ 1, & \text{if } n = 2 \\ F_{n-1} + F_{n-2}, & \text{Otherwise} \end{cases} \tag{8}$$

Here, L_n is given by

$$L_n = \begin{cases} 2, & \text{if } n = 1 \\ 1, & \text{if } n = 2 \\ L_{n-1} + L_{n-2}, & \text{Otherwise,} \end{cases} \tag{9}$$

where N is the size of the input and n is the seed or initial point of Fibonacci or Lucas transformation. This is similar to the modified Arnold transform. FLT is periodic in nature with a maximum possible periodicity of $N^2 - 1$. Since this can produce different scrambling patterns with different periodicities, FLT will provide a more secure encryption compared to basic Arnold transform and modified Arnold transform.

Let m_i represent elements of a plain text in which i varies from 1 to 64. Table I represents elements of the plain text. Table II shows the elements of the transformed text using the FLT.

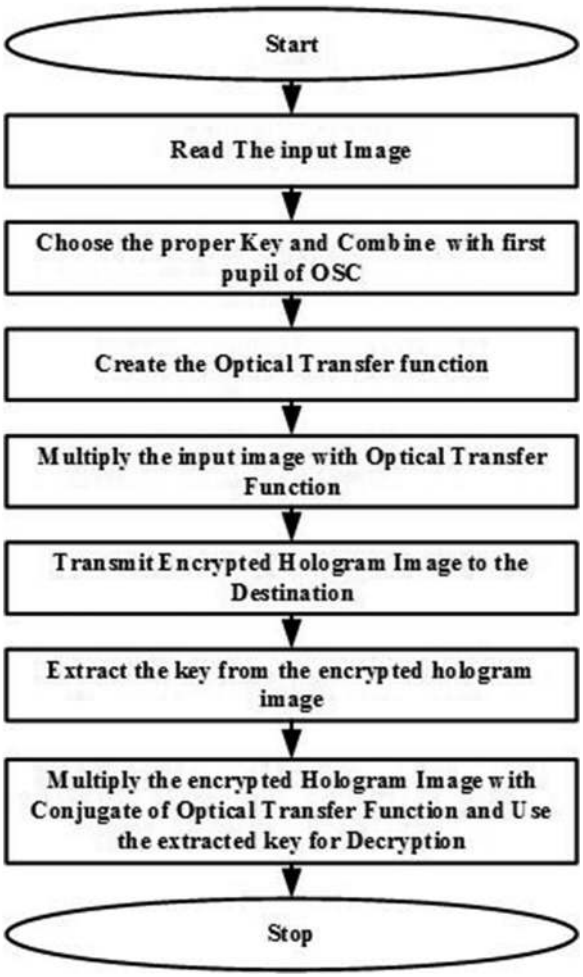

FIG. 2. Flowchart for simulation of OSC.

C. Proposed cryptosystem

An optical cryptographic system based on optical scanning holography is proposed. In this system, the encryption stage consists of two levels. In the first stage, the encryption using incoherent holography (OSC) is performed at a coding distance of z_c. The second level of encryption consists of Fibonacci–Lucas transformation. The applied Fibonacci–Lucas transformation converts the pixels of the sine hologram image and cosine hologram image in the order given in Table II. The traditional pupils or any other pupils can be for this experiment are a pinhole and a unity function. The key used for encryption can also be varied.

TABLE I. Coefficients of plain text.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8
m_9	m_{10}	m_{11}	m_{12}	m_{13}	m_{14}	m_{15}	m_{16}
m_{17}	m_{18}	m_{19}	m_{20}	m_{21}	m_{22}	m_{23}	m_{24}
m_{25}	m_{26}	m_{27}	m_{28}	m_{29}	m_{30}	m_{31}	m_{32}
m_{33}	m_{34}	m_{35}	m_{36}	m_{37}	m_{38}	m_{39}	m_{40}
m_{41}	m_{42}	m_{43}	m_{44}	m_{45}	m_{46}	m_{47}	m_{48}
m_{49}	m_{50}	m_{51}	m_{52}	m_{53}	m_{54}	m_{55}	m_{56}
m_{57}	m_{58}	m_{59}	m_{60}	m_{61}	m_{62}	m_{63}	m_{64}
m_{65}	m_{66}	m_{67}	m_{68}	m_{69}	m_{70}	m_{71}	m_{72}
m_{73}	m_{74}	m_{75}	m_{76}	m_{77}	m_{78}	m_{79}	m_{80}

TABLE II. Coefficients of transformed pixels after FLT.

m_{14}	m_{40}	m_{58}	m_4	m_{30}	m_{56}	m_{74}	m_{20}
m_{73}	m_{19}	m_{45}	m_{71}	m_9	m_{35}	m_{61}	m_7
m_{60}	m_6	m_{32}	m_{50}	m_{76}	m_{22}	m_{48}	m_{66}
m_{47}	m_{65}	m_{11}	m_{37}	m_{63}	m_1	m_{27}	m_{53}
m_{26}	m_{52}	m_{78}	m_{24}	m_{42}	m_{68}	m_{14}	m_{40}
m_{13}	m_{39}	m_{57}	m_3	m_{29}	m_{55}	m_{73}	m_{19}
m_{80}	m_{18}	m_{44}	m_{70}	m_{16}	m_{34}	m_{60}	m_6
m_{59}	m_5	m_{31}	m_{49}	m_{75}	m_{21}	m_{47}	m_{65}
m_{46}	m_{72}	m_{10}	m_{36}	m_{62}	m_8	m_{26}	m_{52}
m_{25}	m_{51}	m_{77}	m_{23}	m_{41}	m_{67}	m_{13}	m_{39}

D. OSC and FLT based cryptographic system with FBA

The simulation experiment is conducted on a two-dimensional grayscale object. The two keys used for this Optical Scanning Holography (OSC) based encryption are a random phase key and a Fused Biometric Array (FBA) key.[57]

Figures 3 and 4 show the biometric keys used for the proposed system.[58] Figure 5 shows the fused biometric array, which is created by fusing Figs. 3 and 4. The FBA is an array of iris images of the sender arranged in a specific order and then combined with the fingerprint of the sender. Each element of iris array corresponds to various eye movements of the same person (sender). The array used in the system consists of nine elements. In order to achieve PSF engineering, the pupils used for optical scanning are 2D rectangular function and 2D Gaussian function. The change in pupil functions in the OSC system finally results in a different pattern of light distribution for the encryption. From the optical encryption section, the encrypted hologram image is digitally encrypted once again. The second encryption is done separately for the real and imaginary parts of the OSC encrypted image. After the second level of encryption, the real and imaginary parts are combined to form a complex hologram image. The flow diagram of the encryption system is shown in Fig. 6. The optical stage in this experiment is conducted by taking into account the mathematical equivalents of components used in the optical system. The appropriate optical system transfer function for OSC (while taking the new pupil set into consideration) is implemented. Then, the second level of encryption is experimentally conducted by the mathematical modeling of the FLT. The optical decryption is done with the same fused biometric array and random phase key. The pupil set used is the same as that of the encryption side. The actual result will be reproduced only at a decoding distance, which is equal to the coding distance, exactly the same seed point for FLT that is used in the encryption. Figure 7 shows the implemented block diagram representation for the simulation experiment of the PSF engineered optical scanning cryptosystem. The amplitude distribution corresponding to the new pupil set is shown in this block.

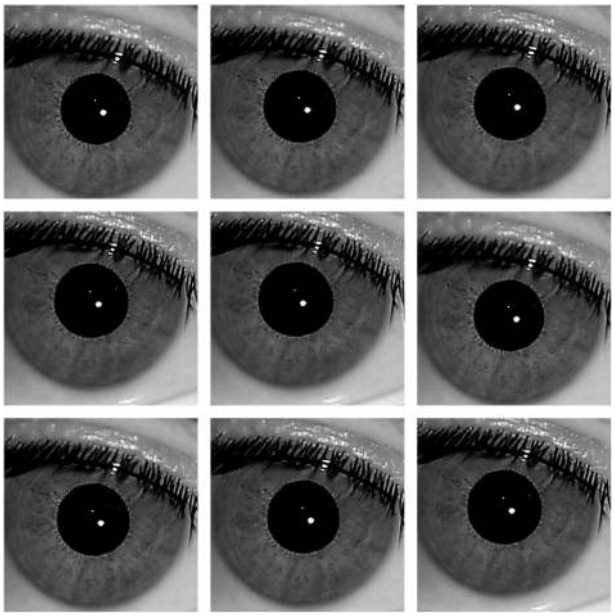

FIG. 3. Iris array.

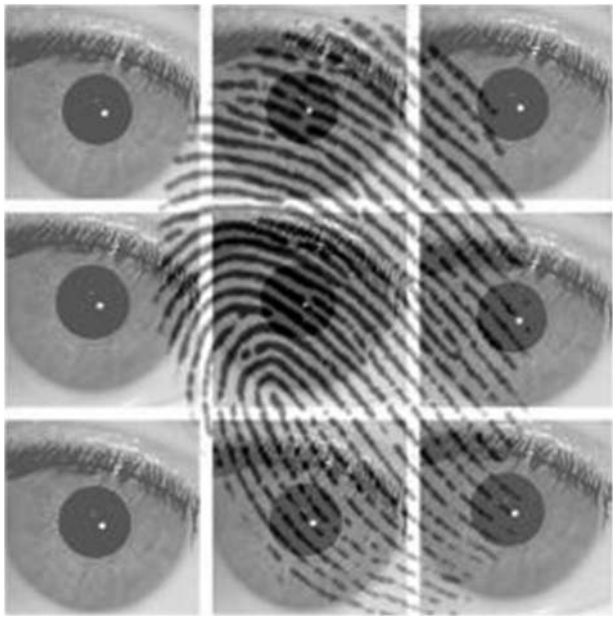

FIG. 5. Fused biometric key.

In the decryption side, the inverse transformation is applied to the encrypted hologram to get back the original complex hologram image. After that, an optical decryption is done with the same fused biometric array and random phase key. The actual result will be obtained only at a decoding distance, which is equal to the coding distance. The flowchart for decryption is shown in Fig. 8.

1. Pupils used for optical scanning cryptography

The experiment is conducted with two sets of pupils. First, the experiment is carried out with a traditional pupil set, i.e., the pinhole and the unity. Since this experiment has resulted in poor encryption in the first stage, a new set of pupils is used for the implementation

FIG. 4. Fingerprint.

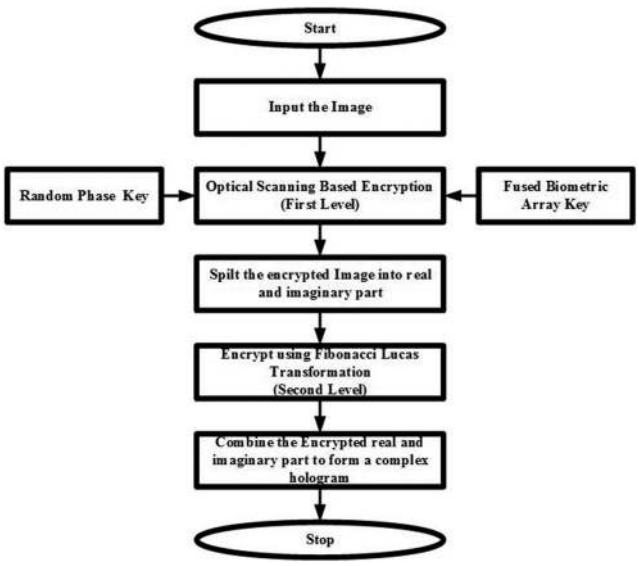

FIG. 6. Encryption.

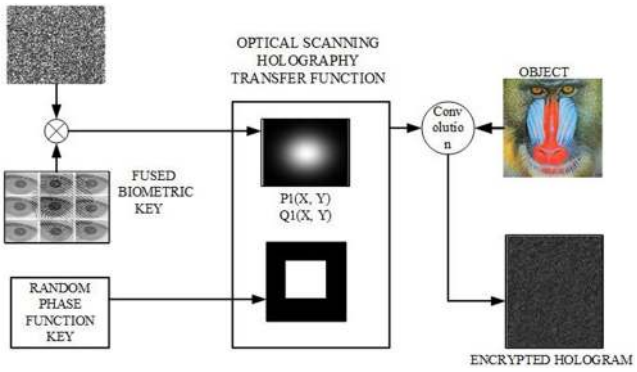

FIG. 7. PSF engineered optical scanning cryptographic system.

of the OSC system. $p_1(x, y)$ is chosen as a Gaussian function, and $q_1(x, y)$ is chosen as a rectangular function. The encryption and decryption keys are the same as in Sec. II D. The theoretical expressions for the used pupil pair and the corresponding OTF are shown as follows:

$$p_1(x,y) = Exp[-\gamma(x^2 + y^2)], \tag{10}$$

$$q1(x,y) = Rect(x,y), \tag{11}$$

where γ is a constant in Eq. (10). With these pupils, the transfer function becomes

$$OTF\omega\,(k_x,k_y;z_c) = [G(k_x,k_y)H*(k_x,k_y;z_c)] \times [R(k_x,k_y)H(k_x,k_y;z_c)], \tag{12}$$

where $k_x = \frac{k_{0x}}{f}$, $k_y = \frac{k_{0y}}{f}$ and k_0 is the wave number, and G(k_x, k_y) and R(k_x, k_y) are the spectral domain representations of p_1(x, y) and q_1(x, y), respectively. While decryption, the following condition is to satisfied:

$$OTF\omega(k_x,\, k_y; z_c) * OTF\omega(k_x, , k_y; z_d) = K. \tag{13}$$

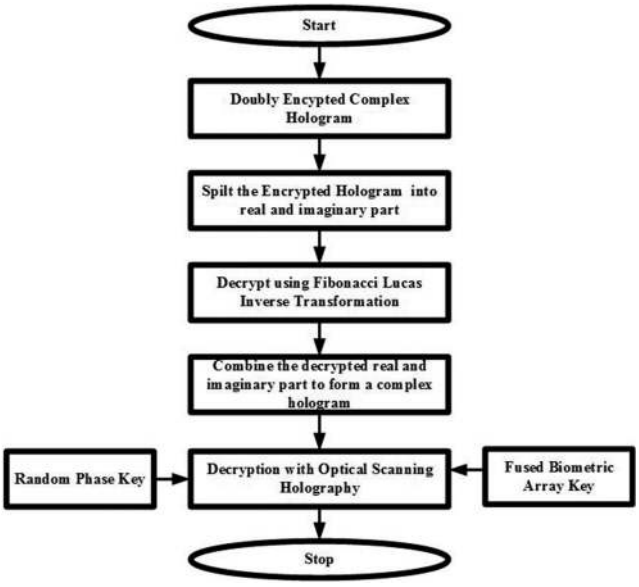

FIG. 8. Decryption.

E. FLT based encryption of the encrypted hologram

The encrypted hologram is once again transformed with the help of Eqs. (14) and (15),

$$H_T(x) = F_i H_X + F_{i+1} H_y, \tag{14}$$

$$H_T(y) = L_i H_x + L_{i+1} H_y. \tag{15}$$

Here, H_T is the transformed hologram and H is the encrypted hologram.

III. RESULTS AND DISCUSSION

The following figures show the simulation results of the proposed system. Simulations are done with Matlab R2016a. These are done with the help of a personal computer (i3 processor and 4 GB RAM). Many Matlab experiments have been carried out to test the

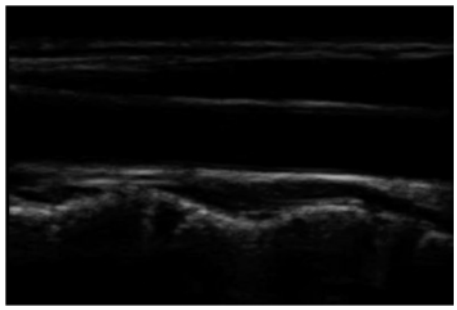

FIG. 9. Ultra sound image.

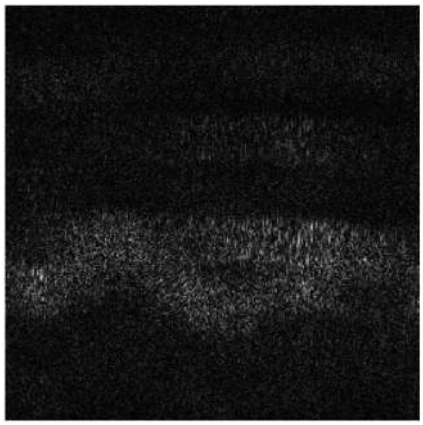

FIG. 10. Intensity of the encrypted hologram image using OSC (traditional pupil set).

FIG. 11. Doubly encrypted hologram image using FLT.

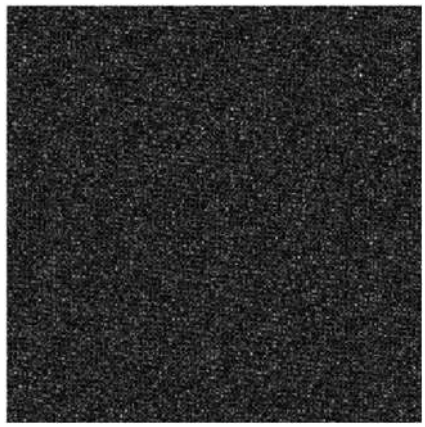

FIG. 13. Intensity of encrypted hologram image with PSF engineered OSC and FLT.

proposed technique. A total of 10 images is used in experiments. Visual results for an ultra sound medical image are shown in this paper, and the results for all other images are tabulated. Figure 9 shows the sample ultrasound image taken from the database[56] for doing the simulation experiment. Figures 10 and 11 show the results obtained from the proposed technique with the traditional pupil set. These figures help in the qualitative evaluation of the technique.

Figures 12 and 13 represent the encrypted hologram images obtained for the first stage (engineered pupil) and the proposed hybrid scheme, respectively. Figures 14 and 15 show the decrypted results for correct key and wrong key (mismatched decoding distance for OSC), respectively. Qualitative analysis shows that the PSF engineering in the proposed method outweighs the traditional pupil based OSC. This can be justified by the tabulated results in the tables.

The sample data images are tested for this proposed crypto system. The parameters used for the verification of the quality of encryption are structural similarity index (SSIM), correlation (CC) between the original and encrypted images, and Maximum Absolute Deviation (MAD), a parameter that indicates the absolute deviation between pixel values of original and encrypted images. Next two parameters considered for the quantitative analysis of the proposed method are Maximum Deviation Analysis (Max Dev), a parameter that shows the area under graph of the absolute difference or deviation between the histogram curves of the original and encrypted images, and Irregular Deviation (Irr. Dev) Analysis, a measure that is calculated on each individual pixel value and its input image before getting the histogram. It does not preserve any information about the positions of the pixels. Tables III and IV indicate the values of different quality metrics calculated between the original image and the encrypted hologram image when the first stage of the proposed hybrid method uses traditional pupil pair and point spread function engineered pupil pair, respectively. SSIM and CC for all the sample sets are remarkably low, which indicates that the signal dependency for the test and reference image is very weak. The metric maximum deviation is more, and irregular deviation is less, which is an essential requirement of good encryption. The analysis reveals that the modified pupil with double encryption gives steady values so that this method could be more advisable for implementations.

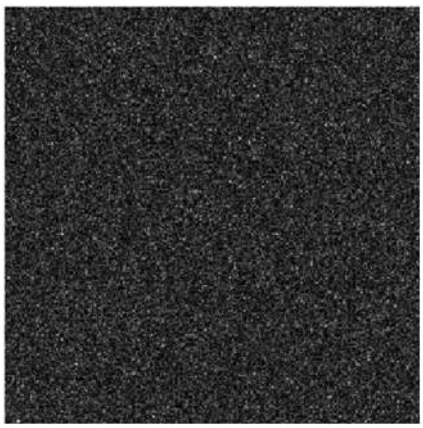

FIG. 12. Intensity of encrypted hologram image with OSC (modified pupil).

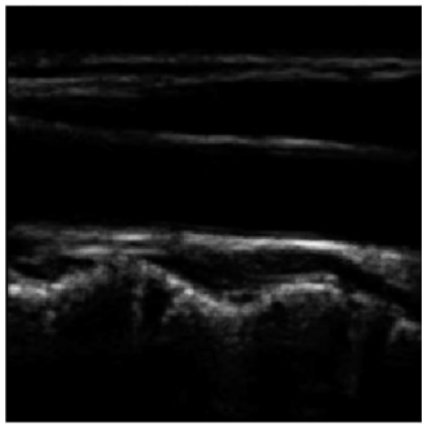

FIG. 14. Decrypted image with correct key.

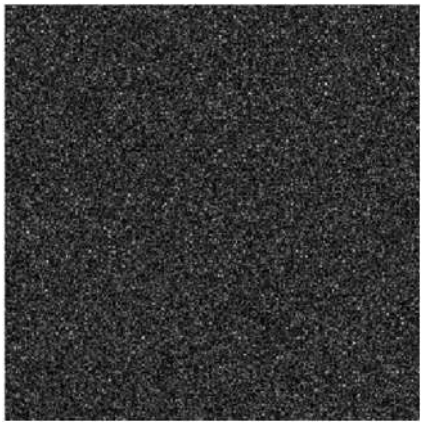

FIG. 15. Decrypted image with mismatched key and decoding distance $z_d = 2.5zc$.

Another set of results between the encrypted and decrypted images for the proposed technique with unity and delta function pupil is shown in Table V. Tables VI and VII show a quantitative comparison between the proposed PSF engineered method and traditional OSC based encryption. The tables clearly indicate a visible hike in the SSIM (66.6%), MAD (8.67%) for the double encryption using PSFE-OSC, and FLT compared to the encryption based on PSFE-OSC only. Considering the quantitative analysis of single encryption based on traditional optical scanning cryptography only and proposed encryption system, the performance measures are superior in terms of SSIM (23.4%), CC (53.94%), and MAD (7.5%). It is clear that the proposed hybrid method provides good quality results.

TABLE III. The results obtained between the original image and the intensity of the encrypted hologram image with traditional optical scanning cryptography and FLT.

Image	SSIM	CC	MAD	Max dev	Irr dev
Cameraman.tif	0.0303	0.001 4	82.984	91 863	49 609
MRI Image.jpg	0.0384	0.000 19	82.984	59 543	45 377
Boat.png	0.0338	0.000 5	79.3437	214 600	49 465
Hestain.png	0.0317	0.003 5	87.308	103 455	48 967
ColoredChips.png	0.0347	−0.001 4	118.2081	216 250	50 734
Lena.jpg	0.0414	0.002 7	73.4354	61 962	48 420
MR1.png	0.057	−0.001 2	30.9953	59 981	45 125
Autumn.tif	0.0405	0.002 6	81.4525	60 118	45 003
Tissue.png	0.0166	−0.001 4	110.2389	386 150	48 984
Football.jpg	0.0707	−0.002 4	43.0346	82 708	45 129

TABLE IV. The results obtained between the original image and the intensity of the encrypted hologram image with the proposed hybrid encryption.

Image	SSIM	CC	MAD	Max dev	Irr dev
Cameraman.tif	0.0252	−0.0031	81.847	90 627	49 297
MRI Image.jpg	0.0372	0.0038	60.4774	65 821	45 351
Boat.png	0.032	0.0013	77.8739	876 559	49 345
Hestain.png	0.0264	−0.0071	120.6097	109 480	50 139
ColoredChips.png	0.0234	0.0011	130.4007	116 105	50 564
Lena.jpg	0.0371	0.0007	73.5815	76 827	48 203
MR1.png	0.0164	0.0004	36.719	73 615	45 706
Autumn.tif	0.0343	−0.0018	86.4032	60 044	45 333
Tissue.png	0.019	0.0026	110.6488	103 705	49 060
Football.jpg	0.0555	−0.0014	51.858	73 922	44 722

TABLE V. The results obtained between the intensity of the encrypted hologram image and decrypted image with the proposed method for traditional pupil.

Image	SSIM	CC	MAD
Cameraman.tif	0.962	0.9922	3.4079
MRI Image.jpg	0.9668	0.9944	4.0596
Boat.png	0.9114	0.9822	6.7434
Hestain.png	0.9655	0.9911	3.5579
ColoredChips.png	0.9644	0.9971	6.7892
Lena.jpg	0.9802	0.9959	6.1257
MR1.png	0.9653	0.9898	4.3661
Autumn.tif	0.9581	0.9973	9.1287
Tissue.png	0.8695	0.9278	14.36
Football.jpg	0.9291	0.9916	2.8905

TABLE VI. The results obtained between original and encrypted hologram images for OSC (unity and delta function pupil) only with FBA key.

Image	SSIM	CC	MAD	Max dev	Irr dev
Cameraman.tif	0.052	0.3406	71.1724	91 368	48 963
MRI Image.jpg	0.0555	0.3956	50.82	58 055	44 700
Boat.png	0.0391	0.1907	74.1735	213 036	49 285
Hestain.png	0.0283	0.0646	88.1129	104 730	48 956
ColoredChips.png	0.0344	0.1748	111.2047	208 158	50 348
Lena.jpg	0.0419	0.1859	68.9388	60 331	48 045
MR1.png	0.0267	0.5877	26.902	68 060	44 534
Autumn.tif	0.0931	0.565	71.6083	54 541	45 266
Tissue.png	0.0193	0.0564	107.7852	393 649	49 005
Football.jpg	0.1451	0.4844	44.1285	102 084	45 946

TABLE VII. The results obtained between original and encrypted hologram images for OSC (rectangular and Gaussian pupil) only with FBA key.

Image	SSIM	CC	MAD	Max dev	Irr dev
Cameraman.tif	0.0965	0.443	73.1168	93 782	49 680
MRI Image.jpg	0.1162	0.5531	46.5769	60 090	44 475
Boat.png	0.0749	0.3098	74.967	90 610	49 559
Hestain.png	0.0507	0.2094	117.68	108 110	49 600
ColoredChips.png	0.0414	0.2591	129.7974	117 207	50 731
Lena.jpg	0.081	0.3524	70.3894	79 251	48 405
MR1.png	0.0588	0.7082	22.4303	72 871	44 906
Autumn.tif	0.1105	0.6058	78.1772	62 906	45 681
Tissue.png	0.0602	0.1464	107.7852	101 404	49 018
Football.jpg	0.2208	0.7	37.3426	71 224	43 000

TABLE VIII. Differential attack analysis of the proposed work.

Name	NPCR score	UACI score
Cameraman.tif	0.9884	0.0576
Lena.bmp	0.9896	0.06
Baboon.png	0.9883	0.0754
MRI.tif	0.9884	0.7072

TABLE IX. Comparison of variance analysis between the proposed hybrid encryption scheme and other similar works.

Reference	Maximum deviation	Irregular deviation
(Lena)[42]	37 980	20 053
(Lena)[42]	21 786	40 904
(Lena)[42]	21 339	40 480
(Lena)[42]	37 630	29 327
Proposed* (Lena)	76 827	48 203
(Cameraman)[46]	61 812	40 127
(Cameraman)[47]	41 256	57 987
(Cameraman)[48]	49 129	55 171
(Cameraman)[49]	38 912	58 173
(Cameraman)[50]	...	44 765
(Cameraman)[43]	63 199	33 038
Proposed*(Cameraman)	90 627	49 277

Table VIII represents the effect of differential attack analysis on this proposed system. The opto-digital encryption system is efficient in terms of correlation coefficient (CC) also (71%). The vertical coefficient (VCC) outweighs the existing works by about 88.27%. The diagonal correlation coefficient (DCC) is efficient by about 54.47% as compared with the mentioned existing works. The maximum deviation parameter is performing well about 50.49% in comparison with the shown existing research studies. These comparisons are based on Refs. 42–56 [Tables IX–X].

TABLE X. Comparison of statistical analysis parameters between the proposed hybrid encryption scheme and other similar works.

Reference	CC	HCC	VCC	DCC
As reported in Ref. 45				
AES (Cameraman)	0.014	...	...	...
(Cameraman)[39]	0.047 2	...	...	...
(Cameraman)[40]	...	−0.0017	−0.0035	0.0099
Proposed*(Cameraman)	−0.010 7	−0.0009	−0.0026	−0.0027
As reported in Ref. 45				
AES (Baboon)	0.011 2	...	...	...
(Baboon)[39]	0.031 5	...	...	...
(Baboon)[46]	0.006 2	−0.0026	−0.0015	−0.0014
(Baboon)[45]	...	0.0059	0.0027	0.0007
Proposed*(Baboon)	0.001 074	0.0001	0.0013	0.0017
(Lena)[5]	...	0.0358	0.0629	−0.0046
(Lena)[52]	...	0.0214	0.0176	0.0066
53	...	−0.003	−0.0024	−0.0034
54	...	−0.0048	−0.0112	−0.0045
(Lena Color-B)[43]	...	−0.0037	0.0095	0.0013
44	...	0.0693	0.0610	−0.0242
Proposed*(Lena)	0.007 549	0.0027	0.0028	0.0025

The number of arrangements possible with the iris array in the proposed system is ~362 880. A single order change in the array will lead to a wrong key, thereby resulting in a different light distribution from the object side.

IV. CONCLUSION

An optical scanning cryptographic system, which uses double encryption and fused biometric array key, is proposed here. The second level of encryption is performed using a new chaotic like series called Fibonacci–Lucas transformation. The change of seed points of FLT allows many degrees of freedom for the keys. The number of arrangements in the biometric array is the next option for the key space. While implementing with an optical setup, each of the arrangements produces separate light distributions. This ensures the decryption of correct output with exactly the same order of biometric array that is used for encryption. Even a single change in position will not reproduce the input. Two variants of double encryption are proposed. The first cryptosystem is implemented with a traditional pupil set of OSH with FBA key. The second cryptosystem uses Gaussian and rectangular pupils with FBA key. Analysis reveals that the proposed cryptosystem with modified pupil based gives better performance or encryption–decryption system, resulting in a steady distribution of parameters. The proposed double encryption cryptosystem is compared with the traditional cryptosystem based on OSC. According to the tabulated results, the proposed cryptosystem's performance is impressive.

To the best of our knowledge, this is the first time a post-encryption using a periodic chaotic like transformation is performed onto encrypted optical scanning hologram. This is a novel optical elucidation for the intruder problems that can affect medical image sharing. Current technology allows the sharing of these images using the cloud. In telemedicine, the current internal security gaps are lack of authentication and effectual encryption. By combining the proposed methodology with the existing digital cryptographic techniques, a system with more resistance to key based attacks can be achieved; simulation studies have been performed.

ACKNOWLEDGMENTS

We would like to acknowledge the support extended by Indian Institute of Space Science and Technology and Center for Development of Imaging Technology, Kerala, India; Group at the Center for Biometrics Security Research (CBSR); National Laboratory of Pattern Recognition (NLPR); and Institute of Automation, Chinese Academy of Sciences (CASIA). The ultrasound image used in this experiment has been taken from the database of The SP Lab research group, which is a part of the Brno University of Technology, Czech Republic.

The article receives no external funding.

The authors declare no conflicts of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
[2] H. Huang and S. Yang, "Image encryption technique combining compressive sensing with double random-phase encoding," Math. Prob. Eng. **2018**, 6764052.
[3] A. Markman, B. Javidi, and M. Tehranipoor, "Photon counting security tagging and verification using optically encoded QR codes," IEEE Photonics J. **6**, 1 (2014).
[4] A. M. Elshamy, A. N. Z. Rashed, A. E.-N. A. Mohamed, O. S. Faragalla, Y. Mu, S. A. Alshebeili, and F. E. Abd El-Samie, "Optical image encryption based on chaotic baker map and double random phase encoding," J. Lightwave Tech. **31**(1), 2533–2539 (2013).
[5] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding," J. Opt. **16**(12), 125403 (2014).
[6] S. Xi, X. Wang, L. Song, Z. Zhu, B. Zhu, S. Huang, N. Yu, and H. Wang, "Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram," Opt. Exp. **25**(7), 8212–8222 (2017).
[7] H. Yu, J. Chang, X. Liu, and C. Wu, "Novel asymmetric crypto system based on distorted wavefront beam illumination and double-random phase encoding," Opt. Exp. **25**, 8860 (2017).
[8] K. Nakano, M. Takeda, and H. Suzuki, "Encrypted imaging based on algebraic implementation of double random phase encoding," Appl. Opt. **53**, 2956 (2014).
[9] X. Wang, G. Zhou, and J. Chen, "Optical image encryption with divergent illumination and asymmetric keys," IEEE Photonics J. **9**, 2 (2017).
[10] S. K. Rajput and N. K. Nishchal, "Optical double image security using random phase fractional Fourier domain encoding and phase-retrieval algorithm," Opt. Commun. **388**, 38–46 (2017).
[11] W. Zamran, E. Ahouz, A. Lizana, J. Campos, and M. J. Yzuel, "Optical image encryption technique based on deterministic phase masks," Opt. Eng. **55**, 103108 (2016).
[12] Yatish, A. Fatima, and N. K. Nishchal, "Optical image encryption using triplet of functions," Opt. Eng. **57**, 033103 (2018).
[13] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Opt. Laser Tech. **57**, 327–342 (2014).
[14] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Optical image encryption using devil's vortex toroidal lens in the fresnel transform domain," Int. J. Opt. **2015**, 926135.
[15] R. Kumar and B. Bhaduri, "Optical image encryption in Fresnel domain using spiral phase transform," J. Opt. **19**, 095701 (2017).
[16] X. Shen, S. Dou, M. Lei, and Y. Chen, "Optical image encryption based on a joint Fresnel transform correlator with double optical wedges," Appl. Opt. **55**, 30 (2016).
[17] W. Sun, W. J. Lei, W. Hua, and Li Q. Wu, "Optical image encryption using gamma distribution phase masks in the gyrator domain," J. Eur. Opt. Soc. **14**, 28 (2018).
[18] J. Li, J. S. Li, Y. Y. Pan, and R. Li, "Compressive optical image encryption," Sci. Rep. **5**, 10374 (2015).
[19] J. Zhu, X. Yang, X. Meng, Y. Wang, Y. Yin, X. Sun, and G. Dong, "Optical image encryption scheme with multiple light paths based on compressive ghost imaging," J. Mod. Opt. **65**(3), 306–313 (2017).
[20] H. Di, Y. Kang, Y. Liu, and X. Zhang, "Multiple image encryption by phase retrieval," Opt. Eng. **55**, 073103 (2016).
[21] W. Chen, "Optical multiple-image encryption using 3-dimensional space," IEEE Photonics J. **8**, 2 (2016).
[22] J.-P. Liu, T. Tahara, Y. Hayasaki, and T. C. Poon, "Optical incoherent digital holography: A review," Appl. Sci. **143**, 406–415 (2018).
[23] T.-C. Poon, "Optical scanning holography—A review of recent progress," J. Opt. Soc. Kr. **13**(4), 406–415 (2009).
[24] T. C. Poon and J. P. Liu, "Digital holography: Special techniques," in *Introduction to Modern Digital Holography with Matlab* (Cambridge University Press, Cambridge, UK, 2014), pp. 144–146.
[25] T. C. Poon, "Optical scanning cryptography," in *Optical Scanning Holography with Matlab* (Springer, USA, 2007), pp. 117–133.
[26] P. W. M. Tsang, T. C. Poon, J. P. Liu, T. Kim, and Y. S. Kim, "Low complexity compression and speed enhancement for optical scanning holography," Sci. Rep. **6**, 34724 (2016).
[27] P. W. M. Tsang, J.-P. Liu, and T.-C. Poon, "Compressive optical scanning holography," Optica **2**(5), 476–483 (2015).
[28] P. W. M. Tsang, T.-C. Poon, and J. P. Liu, "Adaptive optical scanning holography," Sci. Rep. **6**, 21636 (2016).
[29] A. Yan, T. C. Poon, Z. Hu, and J. Zhang, "Optical image encryption using optical scanning and fingerprint keys," J. Mod. Opt. **63**, S38–S43 (2016).
[30] A. Yan, Y. Wei, Z. Hu, J. Zhang, P. W. Ming Tsang, and T. C. Poon, "Optical cryptography with biometrics for multi-depth objects," Sci. Rep. **7**, 12933 (2017).
[31] Z. Tang and X. Zhang, "Secure image encryption without size limitation using arnold transform and random strategies," J. Multimedia **6**, 202 (2011).
[32] G. Ye and X. Huang, "Encryption algorithm based on hyper-chaotic maps and nucleotide sequences database," Secur. Commun. **34**, 1–9 (2016).
[33] Y. Niu, X. Zhang, and F. Han, "Image encryption algorithm based on hyper-chaotic maps and nucleotide sequences database," Comput. Int. Neural Sci. **2017**, 4079793.
[34] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," Opt. Eng. **56**, 116117 (2017).
[35] Y. Tian and Z. Lu, "Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation," AIP Adv. **7**, 085008 (2018).
[36] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on the 3D permutation model and chaotic system," Symmetry **10**, 11 (2018).
[37] C. Li, F. Mina, Q. Jin, and H. Ma, "Extreme multistability analysis of memristor-based chaotic system and its application in image decryption," AIP Adv. **7**, 125204 (2017).
[38] X. Wang, W. Chen, and X. Chen, "A parallel block-based encryption schema for digital images using reversible cellular automata," Eng. Sci. Tech. **17**, 85 (2014).
[39] M. Khan and H. Muhammad Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," PLoS One **13**, e0206460 (2018).
[40] I. Hussain *et al.*, "Image encryption based on Chebyshev chaotic map and S8 S-boxes," Opt. Appl. **XLIX**(2), 317–330 (2019).
[41] G. Kaur *et al.*, "Chaos based multiple order optical transform for 2D image encryption," Eng. Sci. Tech.: Int. J. **23**, 994–1014 (2020).
[42] M. Alawida *et al.*, "A new hybrid digital chaotic system with applications in image encryption," Sig. Proc. **160**, 45–58 (2019).
[43] X. Wang *et al.*, "A novel colour image encryption algorithm based on chaos," Sig. Proc. **92**(4), 1101–1118 (2012).
[44] A. Belazi *et al.*, "A novel image encryption scheme based on substitution-permutation network and chaos," Sig. Proc. **128**, 155–170 (2016).
[45] S. M. Ismail, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," Sig. Proc. **167**, 107280 (2020).
[46] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," Neural Comput. Appl. **30**(12), 847–938 (2018).
[47] F. Ahmed, M. Siyal, and Abbas, "A perceptually scalable and jpeg compression tolerant image encryption scheme," in *4th Pacific-Rim Symposium on Image and Video Technology (PSIVT)* (IEEE, 2020), pp. 232–238.
[48] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," Wireless Per. Commns. **77**, 2771–2791 (2014).
[49] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly auto-correlated data in encryption algorithm," Commun Nonlinear Sci. Numer. Simul. **19**, 3106–3118 (2014).
[50] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dyn. **87**(1), 127–133 (2016).

[51] J.-X. Chen *et al.*, "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic baker map and double random phase encoding," J. Opt. **2**(16), 125403 (2014).
[52] H. Ren, J. Wang, and Q.-H. Wang, "An image encryption schemeof logistic modulation using computer-generated hologram and chaotic map," J. Electr. Comput. Eng. **2018**, 3987105 (2018).
[53] G. Verma and A. Sinha, "Optical image encryption system using non-linear approach based on biometric authentication," J. Mod. Opt. **64**(13), 1321–1329 (2017).
[54] H. Singh, "Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain," Opt. Appl. **47**(4), 557–578 (2017).
[55] M. A. B. Farah *et al.*, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," Opt. Laser. Tech. **121**, 105777 (2020).
[56] See http://splab.cz/en/download/databaze/ultrasound for the sample input ultrasound image.
[57] See http://biometrics.idealtest.org for sample fingerprint and iris images.
[58] M. Mishra *et al.*, "Encryption using Fibonacci Lucas transformation," Int. J. Crpt. Inf. Sec. **2**(3), 131 (2012).