Disclaimer: This is not the final version of the article. Changes may occur when the manuscript is published in its final format.

Hiding the information of QR codes and Medical Images using LCG and LFSR-based PRNG and Image Encryption on FPGA

Mangal Deep Gupta[1] and Pratham Srivastava[2]

[1]Department of Electronics and Communication Engineering, University Institute of Engineering & Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India

[1]mangaldeepgcet@gmail.com, [2]pratham.rbl2002@gmail.com

[1]ORCID iD: 0000-0003-1213-3487

KEYWORD

Cryptography; QR Codes; Medical Images; LCG; LFSR; Latency; Image encryption/decryption; Security; PRNG; FPGA

ABSTRACT

To protect digital image confidentiality, this study presents the encryption algorithm that hides the information of QR codes and medical images. Three different hardware-efficient pseudorandom number generators (PRNGs) based on LCG and LFSR are proposed. It is used to generate random keys and S-boxes as required in the encryption algorithm. The novelty of the proposed PRNG is four 16-bit LFSRs change the seed value of LCG blocks in every iteration independently. It is utilized in the encryption process to guarantee security strength. The Virtex-5 (XC5VLX50T) and Virtex-7 (XC7VH290T) FPGAs are used for the synthesis of proposed PRNGs which are constructed using Verilog HDL. Three 16 × 16 substitution boxes (S-boxes) are designed using proposed PRNGs. Thereafter, an image encryption algorithm is proposed in this work which encrypts the images (QR code and medical images like ultrasounds and infected lungs) up to three times in succession, using three different PRNGs and S-boxes each time. The security strength of encrypted images is analyzed by the correlation coefficients, Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), information entropy, and quantitative image-quality metrics, including Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index Measure (SSIM), obtained for five test images using the proposed encryption algorithms. The performance of the proposed algorithms is evaluated at three different levels of encryption.

1. Introduction

The fast developments in the Internet of Medical Things (IoMT), cloud-based healthcare systems, telemedicine, intelligent transportation, and multimedia communications have led to the significant increase in transmission and storage of medical images in both public and private communications[1], [2], [3] . Medical images generated by modalities like MRI, CT, ultrasound, and X-ray scanners are highly sensitive data and thus need to be kept confidential, complete, and authentic during their whole life cycle. Leaks or tampering of medical images not only cause violation of patient's privacy but can also result in erroneous diagnoses and treatments. Therefore, the design of a secure and effective technique for encryption of medical images has become necessary in today's cyber-physical medical system. With the quick advancement of information technology, cryptosystems are working expansively [4], [5], [6], [7]. Over time, the information exchange across an insecure network has become a serious worry in the evolutionary growth of smart mobile devices connected to the internet [8], [9], [10]. All physical systems connected by the Internet of Things (IoT), such as health care systems, improved metering in smart grids, and environmental monitoring systems, produce a lot of data that raises privacy and security concerns [5], [10], [11].

The security of QR codes becomes a very crucial aspect that should not be overlooked due to the various reasons like prevention of fraud and scams, protection of personal information, maintaining brand reputation, preventing unauthorized access, data integrity, compliance with regulations, enhancing user trust, preventing data breaches, etc. QR codes are easy to replicate or tamper with, making them susceptible to fraudulent activities [12], [13], [14]. Hackers can create malicious QR codes that link to phishing websites or malware downloads, putting users' sensitive information at risk. Ensuring the security of QR codes helps

prevent such fraudulent activities and protects users from falling victim to scams. QR codes often contain sensitive personal or financial information. For example, QR codes used for mobile payments may store credit card details or login credentials. If these codes are not secure, hackers can intercept the information and use it for identity theft or financial fraud. Proper security measures for QR codes are essential to safeguard users' personal information [15], [16], [17]. QR codes can be used to store important data such as product information, inventory details, or authentication codes. Without adequate security measures, this data can be altered or manipulated, leading to incorrect information being disseminated. By ensuring the security of QR codes, businesses can maintain data integrity and prevent unauthorized modifications [18], [19], [20], [21]. Therefore, recognizing the importance of security for QR codes is essential to mitigate risks, protect sensitive information, maintain brand reputation, and ensure compliance with regulations. The implementation of a robust encryption system can enhance the trustworthiness of QR codes and safeguard against potential threats and vulnerabilities.

The security of medical reports of the patient is of utmost importance due to the different reasons such as Patient Privacy and Confidentiality, Prevention of Identity Theft, Compliance with Healthcare Regulations, Preventing Medical Identity Theft, Maintaining Trust in Healthcare Providers, Preventing Data Breaches, Ensuring Accuracy of Patient Care, etc [3], [22], [23], [24]. Medical reports contain sensitive and personal information about patients, including medical history, diagnoses, treatments, and test results. Protecting the security of these reports is crucial to safeguard patient privacy and confidentiality. Unauthorized access to medical reports can lead to breaches of confidentiality and privacy violations, compromising trust between healthcare providers and patients. Medical reports often contain personally identifiable information such as names, addresses, dates of birth, and insurance details. If these reports are not secure, cybercriminals can use this information for identity theft and fraud. Safeguarding the security of medical reports helps prevent unauthorized individuals from accessing sensitive data and using it for malicious purposes. Medical reports contain critical information about a patient's health conditions, treatments, and medications[25], [26], [27], [28]. If these reports are compromised, cybercriminals can use this information to obtain healthcare services, prescriptions, or insurance coverage under false pretenses. Protecting the security of medical reports helps prevent medical identity theft and ensures that patients receive accurate and appropriate care. Patients expect their healthcare providers to protect the confidentiality and security of their medical information. Breaches or unauthorized access to medical reports can erode trust in healthcare institutions and professionals. By prioritizing the security of medical reports, healthcare providers demonstrate their commitment to patient confidentiality and trust, fostering positive relationships with patients [2], [29], [30], [31]. Therefore, the security of medical reports is vital for protecting patient privacy, preventing identity theft, complying with regulations, maintaining trust in healthcare providers, preventing data breaches, ensuring accurate patient care, and safeguarding research data. By implementing robust security measures and best practices for the storage, transmission, and access of medical reports, healthcare providers can mitigate risks, safeguard patient information, and uphold the highest standards of privacy and confidentiality in healthcare delivery [32], [33], [34].

Information security is ensured by using a variety of encryption techniques. Several encryption algorithms are used to hide the information or secure the data that is transmitted over the unsecured network. Consequently, PRNG is a fundamental component of a cryptosystem that guarantees data security across an insecure network channel. Therefore, the security strength in cryptography is determined by the PRNG [7], [8], [11].

Due to ease of hardware implementation, the Linear Feedback Shift Register (LFSR) and the Linear Congruential Generator (LCG) are the most widely used pseudo-random bit generators (PRBGs) [35], [36], [37]. However, because of their linear form, they are less likely to weaken in statistical tests for randomness. To overcome these drawbacks, a great deal of work has been done on PRNGs based on LFSRs, chaotic maps, and congruential generators. Although the Blum Blum Shub (BBS) PRBG is thought to be very secure, factorizing big prime numbers and the computing demands of the design present serious difficulties when implementing it in hardware [38], [39].

Using LCG-based techniques has been the main emphasis of PRNG designs to get low hardware complexity. A potentially useful method is to couple two LCGs, which improves security over single LCGs by producing pseudo-random bit sequences[38]. A two-CLCG block coupling was suggested to increase randomness even further, showing better security than earlier approaches [39]. In response, a redesigned architecture was presented that improved hardware speed and statistical features by using XOR gates in place of inequality conditions and left-shifting operations in place of multiplication operations in each LCG block. In addition, efforts to enhance randomization resulted in the development of the Coupled Variable-Input LCG (CVLCG), which resolves a few of the issues with current systems [36], [37]. Even with these

improvements, still have issues related to hardware performance and/or statistical properties, which makes them unsuitable for some applications.

Textual data encryption can be accomplished with the majority of encryption methods, including Rivest Cipher 6 (RC6), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and other symmetric encryption approaches [40]. As known images contain a significant quantity of redundant linked pixel data, image encryption is different from text encryption. The literature has a variety of image encryption algorithms [3][41] [42] [43]. When it comes to image encryption techniques, the S-box matrix is crucial for subbyte operation in image encryption methods. Therefore, a strong S-box matrix is required for secure encryption. Many S-box-based image encryption techniques have been presented in the past ten years [44][45] [46] [47].

A multilayer security approach for protecting medical data in telehealth applications using watermarking and chaotic encryption is proposed [1]. Watermarking can be employed to embed authentication information or patient-related data into medical images. In [3], investigated medical data security for healthcare applications using hybrid lightweight encryption and a swarm optimization algorithm. Data security and protection in cross-institutional electronic patient records is examined [48]. The exchange of electronic patient records between hospitals, clinics, laboratories, and other healthcare institutions introduces challenges related to confidentiality, access control, data integrity, and privacy protection. A multilayered encryption system for protecting medical images based on binary curves is proposed [22]. The use of multilayer encryption aims to provide additional protection for medical images by applying multiple security operations rather than relying on a single transformation. Rashmi et al. [23] explored an enhanced Lorenz-chaotic encryption method for partial medical image encryption and data hiding in big-data healthcare environments. A promising direction for future research is to integrate appropriate cryptographic and authentication mechanisms into a unified framework while rigorously evaluating its security, computational efficiency, and suitability for real-world healthcare applications.

In light of a secure and low-complexity encryption algorithm for hiding the information of QR codes and medical images, this paper introduces the image encryption algorithm using three PRNGs and S-boxes based on LCG and LFSR. The novelty of the proposed PRNG is four 16-bit LFSRs change the seed value of LCG blocks in every iteration independently. The remaining work is arranged as follows: Material and methods of PRNG is presented in Section 2. This section includes the proposed 32-bit PRNG circuit, the outcome and analysis of three different PRNGs, implementation on Virtex-5 (XC5VLX50T) and Virtex-7 (XCV5VLX220) FPGAs and design of three 16×16 substitution boxes (S-boxes). This section also discusses the image encryption algorithm which encrypts the images (QR code and medical images like ultrasounds and infected lungs). Section 3 demonstrates the result and discussion including the Security Strength Analysis of Encrypted Images in terms of the correlation coefficients, UACI, NPCR, information entropy, and quantitative image-quality metrics, including PSNR, MSE, and SSIM for five test images using the proposed encryption algorithms. Finally, Section IV concludes the work.

2. Materials and Methods

2.1. Proposed PRNG Circuits

This section discusses the design of three different PRNG circuits based on LCGs and LFSR. The proposed PRNG uses four 16-bit LFSR circuits to change the seed value of LCG blocks in every iteration independently [35]. The LCG recurrence equation is characterized by the following equations:

$$\boldsymbol{x_{i+1}} = \boldsymbol{[(r_1 \times x_i) + x_i + b_1] \bmod 2^n} \tag{1}$$

$$\boldsymbol{y_{i+1}} = \boldsymbol{[(r_2 \times y_i) + y_i + b_2] \bmod 2^n} \tag{2}$$

In a conventional LCG circuit, the value of b_1, b_2, r_1 and r_2 are fixed as given in Eqs. (1) and (2). In the proposed circuit, the value of b_1, b_2, r_1 and r_2 will be changed in every iteration by LFSR circuits [36]. Therefore, the proposed PRNGs improve the randomness of sequences that can be utilized in encryption algorithm. To achieve this, four LFSR circuits independently generate the random values that is used to change the value of b_1, b_2, r_1 and r_2 of LCG. Further the final random values of PRNG are captured either $X_i[31{:}0]$ or $Y_i[31{:}0]$ by 2:1 multiplexer in which LSB or MSB bit of X_i or Y_i act as a select line of the multiplexer. With these combinations, this section describes the three different PRNG circuits which is shown in Fig. 1 to Fig. 3.

The first proposed 32-bit PRNG circuit is shown in Fig. 1. The 32-bit seeds value b_1 and b_2, change accordingly by four 16-bit LFSRs as shown in the figure, where, $in_1[15:0]$, $in_1[31:16]$, $in_2[15:0]$ and $in_2[31:16]$ are 16-bit initial values corresponding four LFSR circuits. The value of r_1 and r_2 are also change in every iteration by $b_1[4:0]$ and $b_2[4:0]$ respectivly. The proposed PRNG circuit generates 32-bit random numbers $Z_i[31:0]$ in every iteration. To enhance the randomness, capture the value of $X_i[31:0]$ as a 32-bit random number when $X_i[31]$ equal to logic 0 while it is $Y_i[31:0]$ as a 32-bit random number when $X_i[31]$ equal to logic 1, which is shown in circuit.

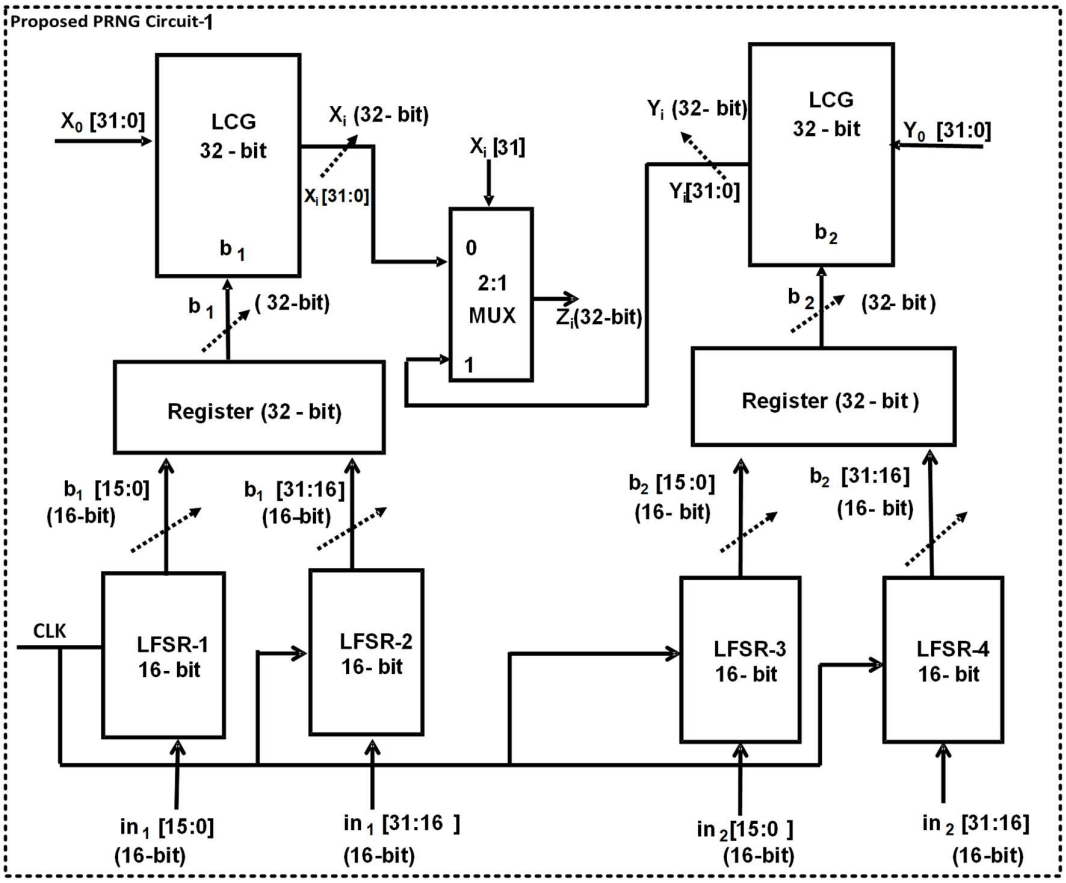


Fig.1. Proposed 32-bit PRNG Circuit-1 based on LCG and LFSR.

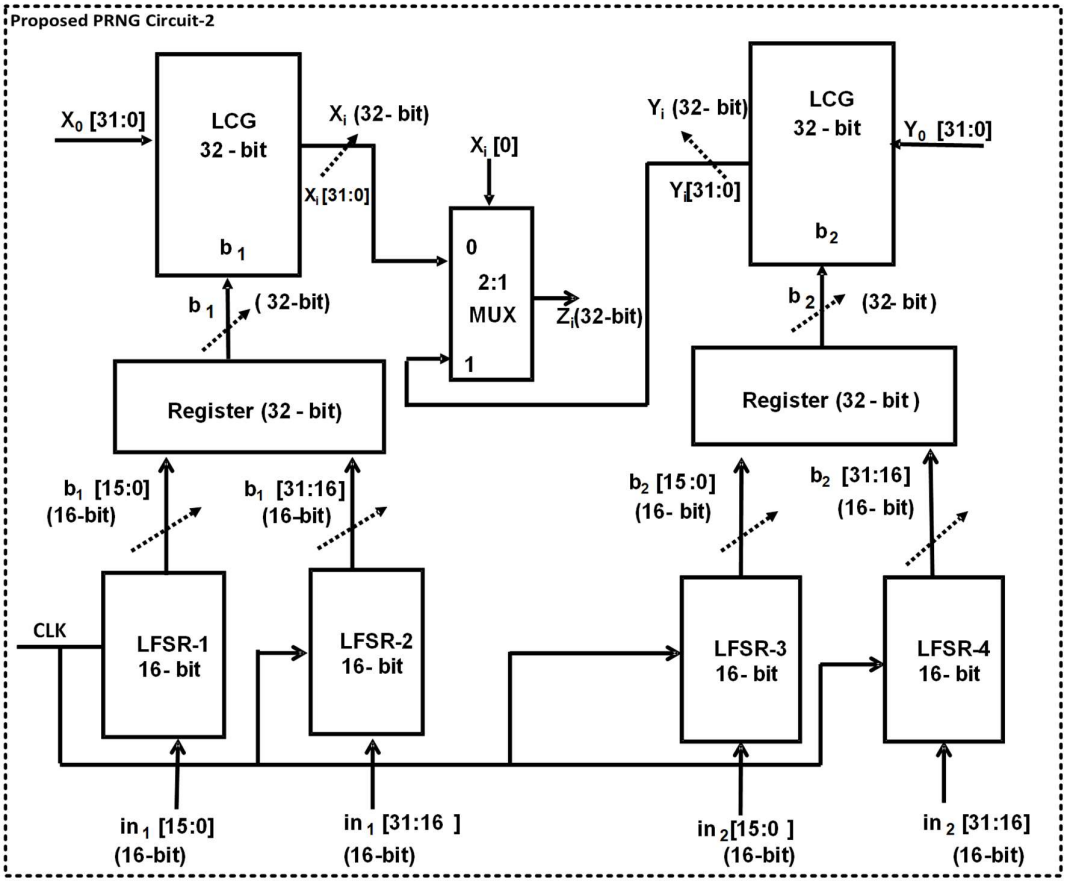


Fig.2. Proposed 32-bit PRNG Circuit-2 based on LCG and LFSR.

Similarly, proposed PRNG circuit-2 is shown in Fig.2. The 32-bit seeds value b_1 and b_2, change accordingly by four 16-bit LFSR as Circuit-1. The LSB bit of X_i i.e. X_i [0], when X_i [0] is 0 then it will pass the X_i value at Z_i, and similarly when X_i [0] is 1 then the Y_i value will get at Z_i. The Z_i is 32- a bit random value generated on every clock positive edge block. The value of r_1 and r_2 are also change in every iteration by $b_1[4:0]$ and $b_2[4:0]$ respectively. The proposed PRNG circuit generates 32-bit random numbers $Z_i[31:0]$ in every iteration. To enhance the randomness, capture the value of $X_i[31:0]$ as a 32-bit random number when $X_i[0]$ equal to logic 0 while it is $Y_i[31:0]$ as a 32-bit random number when $X_i[31]$ equal to logic 1, which is shown in circuit.

The proposed PRNG circuit-3 is shown in Fig. 3. The difference is that the LSB bit of Y_i i.e. Y_i [0], when Y_i [0] is 0 then it will pass the X_i value at Z_i and similarly when Y_i [0] will be 1 then Y_i value will get at Z_i. The value of r_1 and r_2 are also change in every iteration by $b_1[4:0]$ and $b_2[4:0]$ respectivly. The proposed PRNG circuit generates 32-bit random numbers $Z_i[31:0]$ in every iteration. To enhance the randomness, capture the value of $Y_i[31:0]$ as a 32-bit random number when $Y_i[0]$ equal to logic 0 while it is $Y_i[31:0]$ as a 32-bit random number when $Y_i[0]$ equal to logic 1, which is shown in circuit.

2.2. FPGA Implementation of PRNGs

Verilog hardware description language (HDL) is used in this work for the RTL coding of the proposed PRNGs. Synthesis of the proposed work has been done on commercially available FPGA: Virtex-5 (XC5VLX50T) and Virtex-7 (XC7VH290T). Xilinx ISE design suit is used in this work for the simulation and synthesis of proposed PRNG circuits.

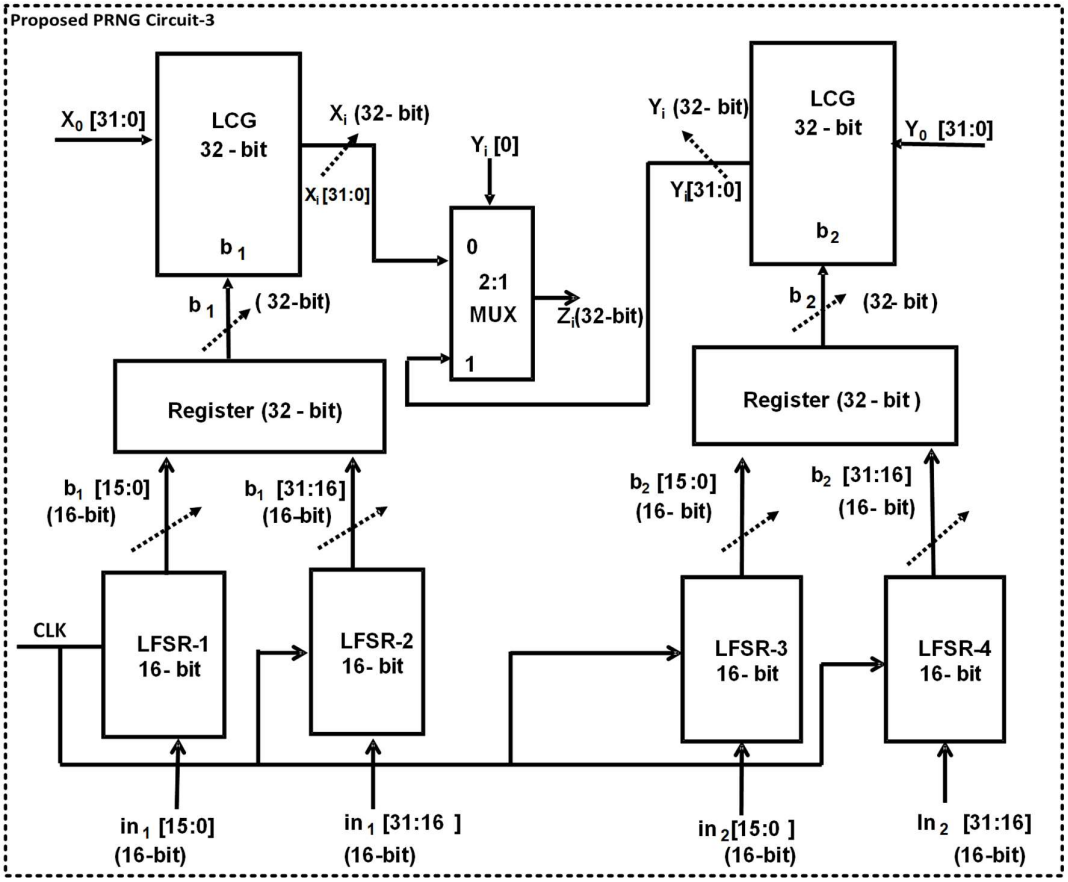


Fig.3. Proposed 32-bit PRNG Circuit-3 based on LCG and LFSR.

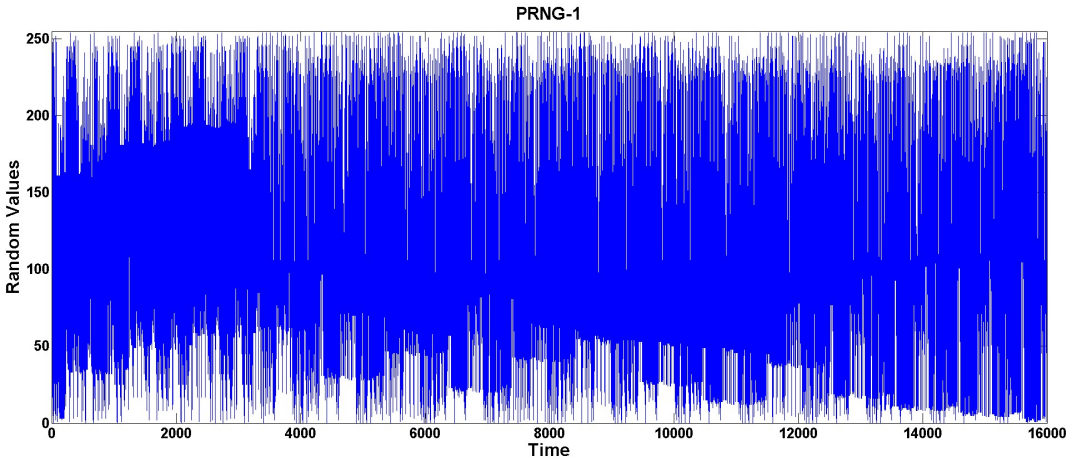


Fig. 4 Time vs Random Values graph of PRNG Circuit-1.

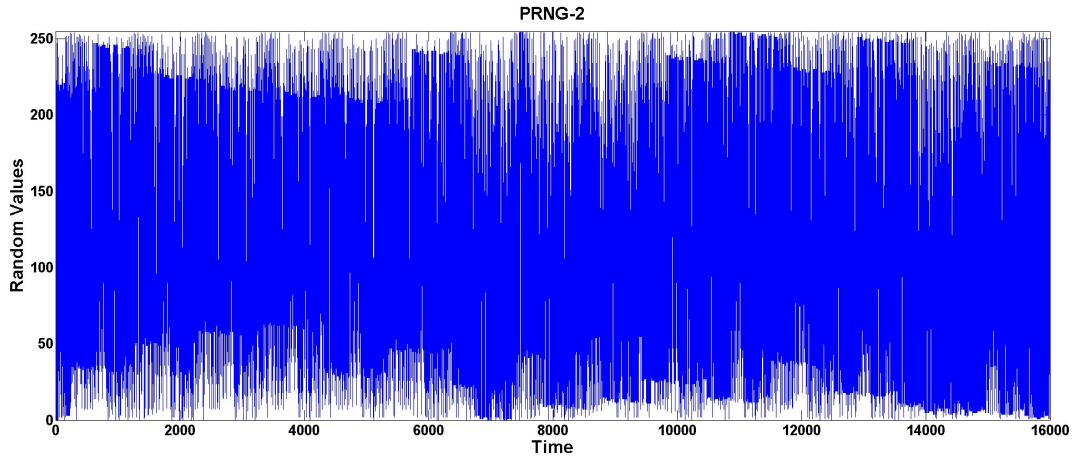


Fig. 5 Time vs Random Values graph of PRNG Circuit-2.

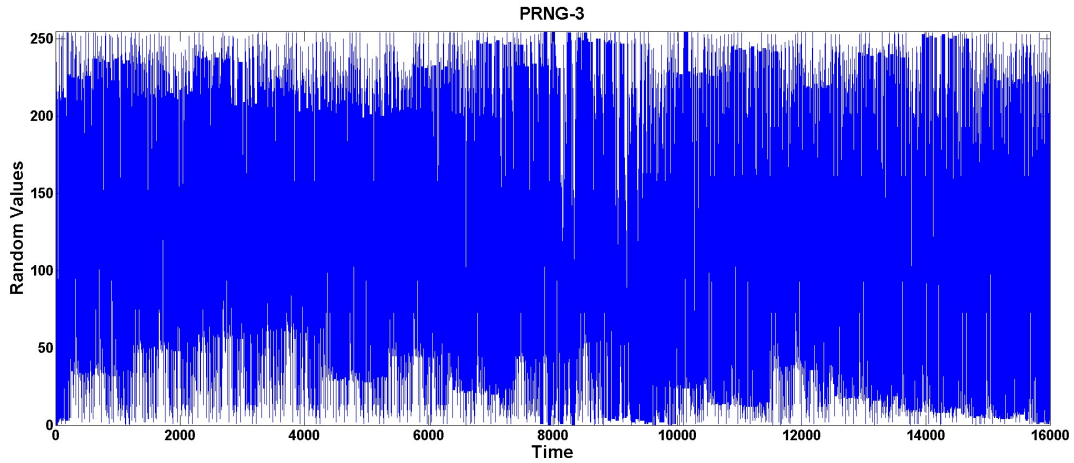
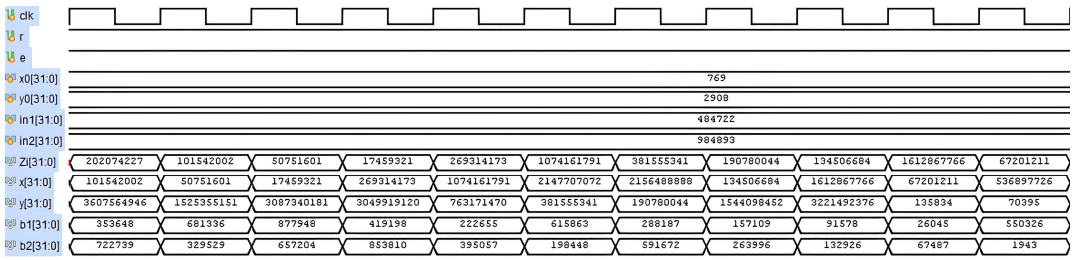


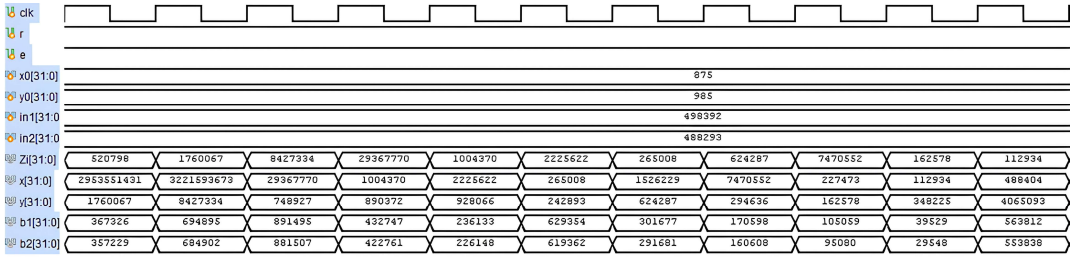
Fig. 6 Time vs Random Values graph of PRNG Circuit-3.

Fig. 4, 5, and 6 illustrate the generation of 8-bit random numbers over time using the three proposed Pseudo-Random Number Generators (PRNGs). These figures present the relationship between time and the corresponding random values generated at the outputs of the respective PRNG circuits. Specifically, Fig. 4 represents the output generated by Circuit 1, Fig. 5 illustrates the random number sequence produced by Circuit 2, and Fig. 6 depicts the output of Circuit 3. These results correspond to the three proposed circuit architectures presented in Fig. 1, 2, and 3, respectively. The output sequences obtained from these circuits serve as random keys that can potentially be used in cryptographic applications. The plotted waveforms demonstrate irregular variations in the generated 8-bit values over time, with no immediately apparent periodic patterns or repetitive sequences within the observed intervals. The seemingly erratic and non-uniform distribution of the output values indicates that the proposed PRNG circuits exhibit irregular temporal behaviour.

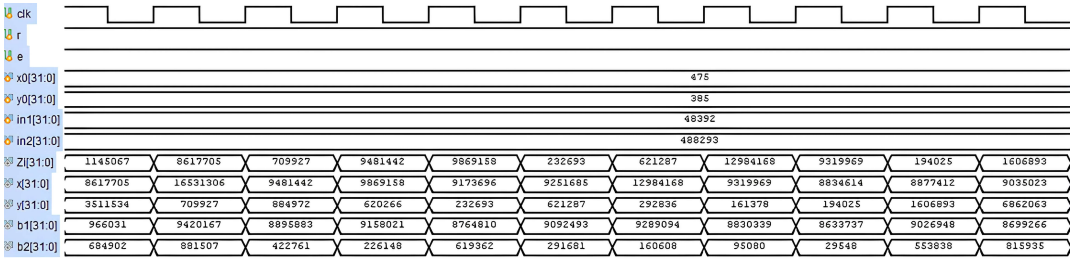
Table 1 lists the utilized area (in terms of Slices, LUTs, and FFs) and timing performance of the proposed PRNGs circuit and also compares with existing literature on PRNGs [36], [38], [44]. The simulation waveform of the proposed 32-bit PRNG is shown in Fig. 7(a), 7(b), and 7(c) corresponding PRNG circuit-1, -2, and -3.



(a)



(b)



(c)

Fig. 7 Simulation waveforms of proposed 32-bit PRNG using: (a) Circuit-1; (b) Circuit-2 and (c) Circuit-3.

Fig. 7(a) presents the simulation of the waveform of the 32-bit proposed PRBG circuit. For this simulation, set the value of $r_1[4:0] = b_1[4:0]$, $r_2[4:0] = b_2[4:0]$, $X_0[31:0] = 769$, $Y_0[31:0] = 2908$, $in_1[31:0] = 484722$, $in_2[31:0] = 984893$. The value of X_i and Y_i changed with a positive clock pulse cycle. The random value Z_i is equal to $Y_i[31:0]$ when $X_i[31]$=1 otherwise if $X_i[31]$=0 then output Z_i will be equal to $X_i[31:0]$.

Fig. 7(b) presents the simulation of the waveform of the 32-bit proposed PRNG circuit-2. For this simulation, set the values of $r_1[4:0] = b_1[4:0]$, $r_2[4:0] = b_2[4:0]$, $X_o[31:0]$=875, $Y_0[31:0]$=985, $in_1[31:0]$=498393, $in_2[31:0]$=488293. The random value Z_i is equal to $X_i[31:0]$ when $X_i[0]$=1 otherwise if $X_i[0]$=0 then output Z_i will be equal to $Y_i[31:0]$.

Similarly, Fig. 7(c) presents the simulation waveform of the 32-bit proposed PRNG circuit-3. For this simulation, set the variables value: $r_1[4:0] = b_1[4:0]$, $r_2[4:0] = b_2[4:0]$, $X_O[31:0]$=475, $Y_O[31:0]$=385, $in_1[31:0]$=48392, $in_2[31:0]$=488293. The random value Z_i is equal to $X_i[31:0]$ when $Y_i[0]$=1 otherwise if $Y_i[0]$=0 then output Z_i will be equal to $Y_i[31:0]$.

Table 1 Synthesis result of existing and proposed architecture of PRNGs.

Method	**Size (bits)**	**FPGA**	**Number of Slice Registers**	**Number of Slice LUTs**	**Maximum Frequency (MHz)**	**Delay (ns)**
Proposed PRNG Circit-1	**32**	**Virtex-5 (XC5VLX50T)**	161	390	289.956	3.449
		Virtex-7 (XC7VH290T)	160	445	305.027	3.278
Proposed PRNG Circit-2	**32**	**Virtex-5 (XC5VLX50T)**	161	390	289.956	3.449
		Virtex-7 (XC7VH290T)	160	445	305.027	3.278
Proposed PRNG Circit-3	**32**	**Virtex-5 (XC5VLX50T)**	161	390	289.956	3.449
		Virtex-7 (XC7VH290T)	160	445	305.027	3.278
PRNG *[44]*	**32**	**Virtex-5 (XC5VLX50T)**	128	679	73.307	-
	32	**Virtex-5**	-	480	219.35	4.559

PRNG ***[38]***		**Virtex-7**	-	440	282.64	3.54
PRNG [36]	**32**	**Virtex-5 (XC5VLX110T)**	177	403	342.190	2.922
		Virtex-7 (XC7VX330T)	177	305	427.068	2.342

2.3. S-Box Design

The S-box matrix is used in the image encryption process for subyte operation. It decides the security strength of encrypted data [7] [9], [44], [49]. The primary purpose of an S-box is to introduce non-linearity into the encryption algorithm, making the relationship between plaintext, ciphertext, and the encryption key more difficult for an attacker to analyze. In this section, three new 16×16 S-boxed are designed using three proposed PRNG circuits for subbyte operation in the proposed encryption algorithm. To design S-boxes, 256 unique 8-bit decimal values are arranged serially as random sequences generated by PRNG circuits. In this manner, it generates the S-box structure, which has 256 unique random decimal values. The same procedure is repeated independently for PRNG circuits 1, 2, and 3, producing three corresponding S-box matrices. The S-box matrix corresponding proposed PRNG circuit-1, -2, and -3 are shown in Tables 2, 3, and 4. Each table contain 256 entries, arranged as 16 rows by 16 columns. The values in the three tables may differ because their generating circuits produce different sequences. The resulting matrices serve as lookup tables for byte substitution in the proposed encryption algorithm.

Table 2 S-Box-1 matrix based on proposed PRBG circuit-1.

53	161	245	0	25	252	90	248	74	52	45	124	48	32	17	162
241	128	137	216	16	5	236	1	250	184	75	204	96	81	208	8
57	232	194	125	212	50	26	200	14	196	6	41	228	66	2	92
180	47	176	34	113	130	88	18	108	120	23	140	98	80	10	104
195	84	51	76	27	72	15	68	7	100	67	117	3	9	192	43
164	160	11	35	24	178	172	4	36	163	156	170	168	190	157	210
173	186	144	149	174	136	181	166	226	154	188	152	119	145	132	19
133	131	129	122	187	73	99	209	185	61	83	237	59	217	39	233
207	235	49	193	203	177	37	33	242	169	254	97	221	213	165	225
218	118	224	65	197	215	249	227	82	58	46	38	42	189	109	89
105	79	64	107	44	56	28	114	40	60	143	171	139	126	93	85
201	69	219	91	121	253	153	179	62	29	211	21	175	167	123	77
183	151	12	182	214	55	198	54	22	230	206	246	135	244	63	115
229	205	134	146	243	20	147	116	142	199	191	231	247	150	251	240
112	138	95	202	111	71	110	106	70	158	155	87	101	86	148	103
102	220	31	234	13	222	94	30	239	255	223	141	238	159	127	78

Table 3 S-Box-1 matrix based on proposed PRBG circuit-2.

61	77	72	0	135	215	88	16	44	192	38	26	124	1	199	247
96	9	236	6	228	152	29	207	80	3	250	221	30	49	220	58
146	136	2	62	132	217	238	157	57	45	76	130	21	90	42	118
170	216	54	137	98	153	183	142	128	63	181	18	160	17	109	36
111	102	123	145	33	94	224	115	35	209	239	185	147	204	131	218
120	99	25	184	64	173	32	164	112	119	251	91	10	227	240	4
56	252	144	159	200	248	235	108	140	5	92	232	189	7	214	166
71	246	134	24	206	208	122	156	11	186	8	254	223	43	12	37
194	104	253	230	201	198	39	241	219	14	93	177	237	161	213	234
129	78	95	117	210	143	121	225	41	163	82	34	107	75	245	205
126	171	66	40	125	73	70	229	222	190	133	202	110	46	27	148
203	79	28	249	113	149	182	154	53	48	13	176	60	178	162	85
106	97	244	65	22	226	51	138	47	141	59	31	89	50	158	67
15	179	20	116	52	55	243	193	231	19	87	74	242	105	103	81
114	212	191	83	195	139	211	167	101	255	197	233	84	188	23	180
165	187	155	168	86	196	175	69	68	169	150	172	151	100	127	174

Table 4 S-Box-1 matrix based on proposed PRBG circuit-3.

66	179	136	2	90	93	152	0	14	51	212	37	235	156	3	24
125	160	56	216	132	11	215	164	98	19	180	1	162	211	188	27
36	12	72	7	4	10	105	140	18	45	210	236	13	253	165	131
41	220	94	77	26	53	204	126	8	198	6	5	228	245	33	252
28	106	108	254	92	194	181	218	95	99	84	76	127	32	9	70
100	67	117	124	147	139	200	135	88	138	107	197	227	44	141	255
171	31	217	75	222	142	29	163	234	97	246	68	226	52	34	60
65	130	50	48	43	47	143	175	35	242	83	159	225	129	206	229
157	161	203	214	63	49	237	111	101	233	57	96	39	205	193	64
42	224	118	196	176	40	178	133	114	85	78	184	189	20	146	240
134	86	21	213	151	239	232	173	169	223	128	62	38	109	150	58
69	231	238	172	166	251	149	230	241	153	59	79	81	250	145	74
177	73	55	113	80	158	54	102	243	221	110	144	112	219	89	137
23	244	87	115	155	187	22	167	185	61	186	154	121	201	25	209
71	207	120	208	82	122	16	15	123	91	191	46	182	190	103	119
170	30	247	202	17	168	174	248	192	199	104	249	116	148	183	195

2.4. Proposed Image Encryption and Decryption Algorithm

This section presents an image encryption algorithm to hide the information of QR codes and medical data of patients. This algorithm is based on three times encryption using three different S-boxes and Proposed PRNGs. The proposed three-times encryption using S-box-1, S-box-2, and S-box-3 is shown in Fig. 8. The original image (pixel size: 128 x 128) will be encrypted three times with three different PRNG used each time. The sub-byte operations and bitwise XOR are performed in each encryption step.

As illustrated in Fig. 8, the encryption process begins by applying a bitwise XOR operation to the bit-transformed input image using binary random values. The resulting matrix is denoted as $I_{XOR1}(x,y)_{M\times N}$. A 16 × 16 S-box, $S_1(m,n)$, generated using the proposed PRNG-1, is then employed for the SubByte transformation. In this step, each pixel in the XORed matrix is substituted with an entry from the S-box, determined by its 4-bit MSB and 4-bit LSB components: $I_{S1}(i,j)_{mxn}$= S_1(4-bit MSB (I_{XOR1}(x, y), 4-bit LSB I_{XOR1}(x, y)). This produces the first encrypted image $I_{E1}(i,j)_{M\times N}$.

The second stage, indicated by the dotted block in Fig. 8, follows a similar approach. The intermediate image $I_{E1}(i,j)_{M\times N}$is first XORed with another set of pseudo-random binary values, yielding $I_{XOR2}(x,y)_{M\times N}$. A second 16 × 16 S-box, $S_2(m,n)$, is then applied for pixel substitution based on MSB and LSB values: I$S_2(i,j)_{mxn}$= S_2(4-bit MSB (I_{XOR2}(x, y), 4-bit LSB I_{XOR2}(x, y)). The output of this stage is the second encrypted image $I_{E2}(i,j)_{m\times n}$.

In the final stage, the same sequence of operations is repeated. The image $I_{E2}(i,j)_{M\times N}$undergoes a bitwise XOR operation using random numbers generated by PRNG-3, producing $I_{XOR3}(x,y)_{M\times N}$. Subsequently, a third 16 × 16 S-box, $S_3(m,n)$, is used for the SubByte transformation, where each pixel is replaced according to its corresponding MSB and LSB indices within the S-box: $I_{S3}(i,j)_{M\times N}$ (4-bit MSB (I_{XOR3}(x, y), 4-bit LSB (I_{XOR3}(x, y)). The resulting matrix $I_{E3}(i,j)_{M\times N}$represents the final encrypted image, providing a high level of security.

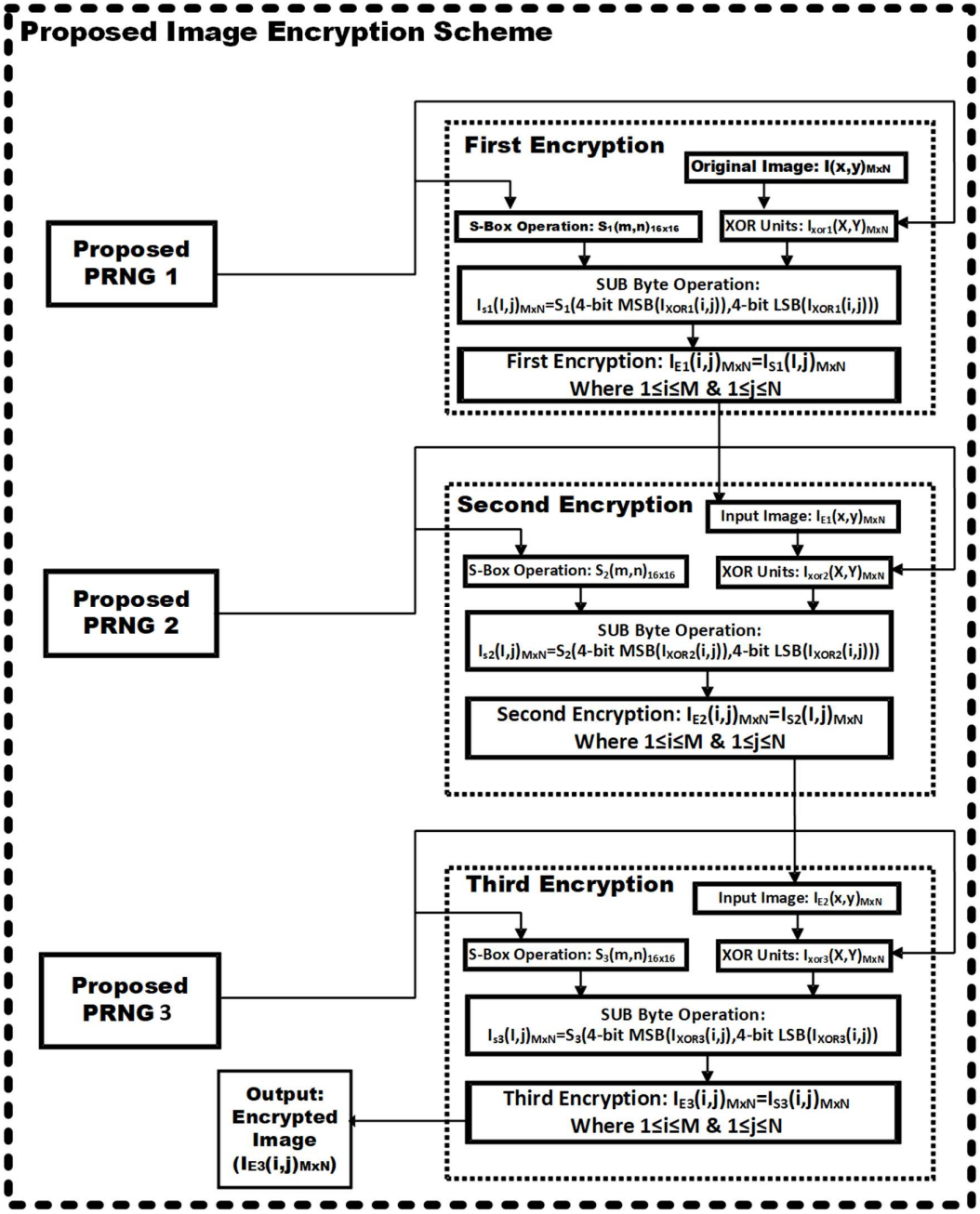


Fig. 8 Flowchart of the Proposed multistage image encryption algorithm using proposed LCG-LFSR-based PRNGs and S-boxes.

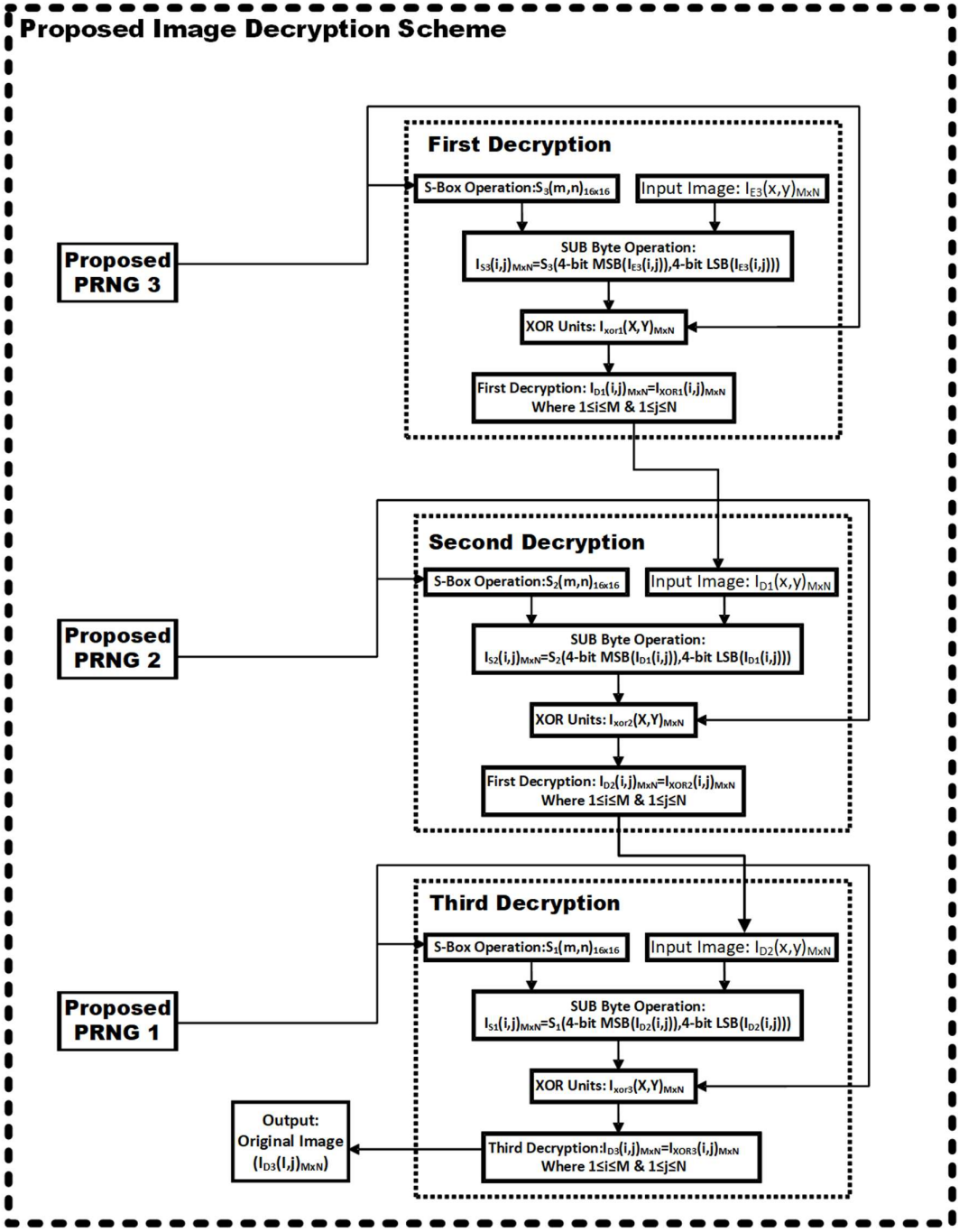


Fig. 9 Flowchart of the Proposed multistage image decryption algorithm using proposed LCG-LFSR-based PRNGs and S-boxes.

The decryption stage reconstructs the original image from its encrypted form. The overall procedure is illustrated in Fig. 9. The method applies SubByte transformations and bitwise XOR operations in three successive rounds, each using a distinct S-box and a unique random key generated by separate PRNGs. In the first stage, a 16 × 16 S-box denoted as $S_3(m,n)$is applied to the bit-transformed encrypted image $I_{E3}(i,j)_{m\times n}$. During the SubByte operation, each pixel value is substituted using the S-box based on its 4-bit most significant bits (MSB) and 4-bit least significant bits (LSB), expressed as: $I_{S3}(i,j)_{mxn}$=S_2(4-bit MSB $I_{E3}(X,Y)$, 4-bit LSB $I_{E3}(X,Y)$). The resulting matrix is then XORed with random values generated by PRNG-3, producing the intermediate image $I_{D1}(i,j)_{m\times n}$.

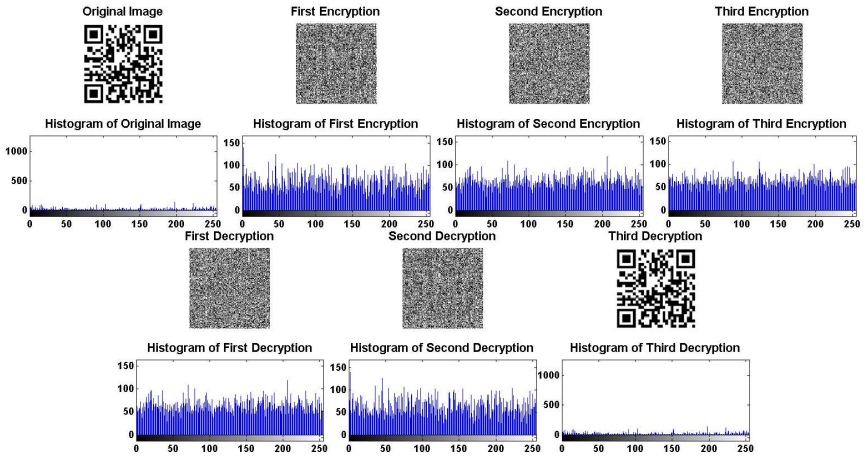
In the second stage, another 16 × 16 S-box, $S_2(m,n)$, is used to process $I_{D1}(i,j)_{m\times n}$. Similar to the previous step, pixel substitution is carried out by mapping MSB and LSB values to the corresponding S-box entries:

$I_{S2}(i,j)_{mxn}$=S_2(4-bit MSB $I_{D1}(X,Y)$, 4-bit LSB $I_{D1}(X,Y)$). This operation yields the second intermediate image $I_{D2}(i,j)_{m\times n}$.
Finally, the third stage (as shown in the dotted block of Fig. 9) employs the S-box $S_1(m,n)$on $I_{D2}(i,j)_{m\times n}$. Each pixel is again substituted using the corresponding row and column indices derived from its MSB and LSB values: $I_{S1}(i,j)_{mxn}$=S_1(4-bit MSB $I_{D2}(X,Y)$, 4-bit LSB $I_{D2}(X,Y)$). The output of this stage, $I_{D3}(i,j)_{m\times n}$, represents the fully decrypted image, which matches the original input image.

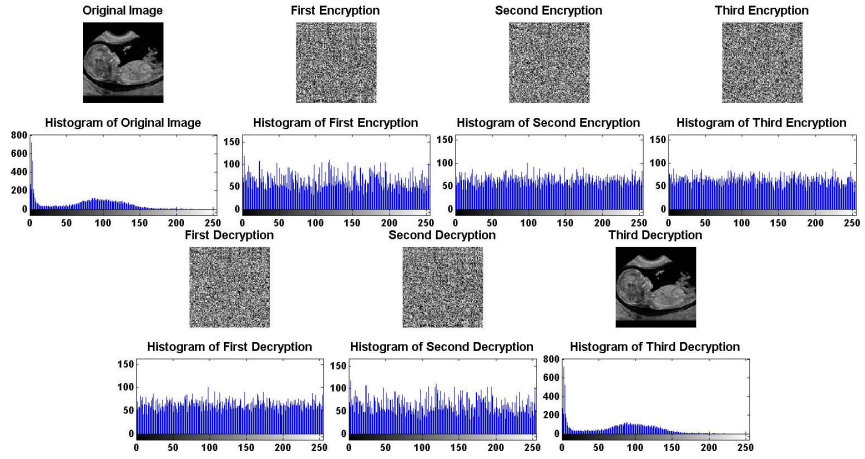
3. Result and Discussion

3.1. Security Strength Analysis of Encrypted Images

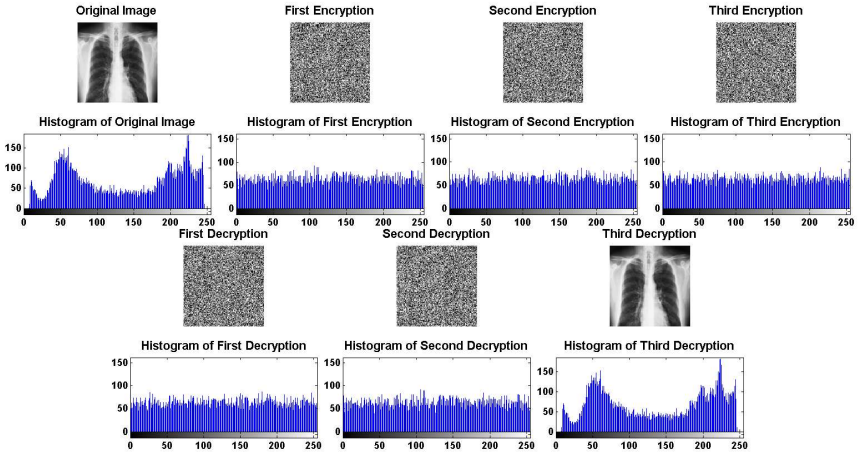
To evaluate the security strength of encrypted images, the following tests are performed: correlation coefficients, UACI, NPCR, information entropy, and quantitative image-quality metrics, including PSNR, MSE, and SSIM [11], [34], [44]. For this analysis, five 128×128 grayscale images: "Quick Response (QR) Code, Ultrasound, Infected Lungs, Baboon, and Peppers" are taken into consideration. The medical images used in this study including Ultrasound and Infected Lungs images were obtained from publicly available datasets on Kaggle. The standard test images including Baboon and Pepper were obtained from publicly available on MATLAB.



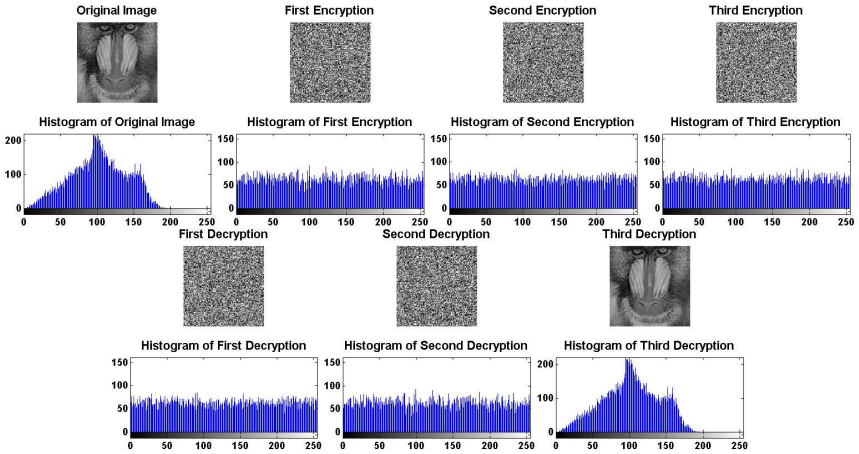
(a)



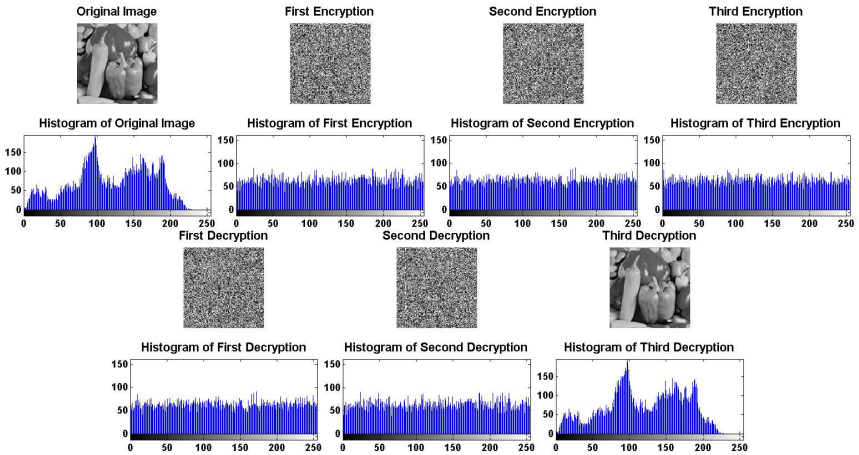
(b)



(c)



(d)

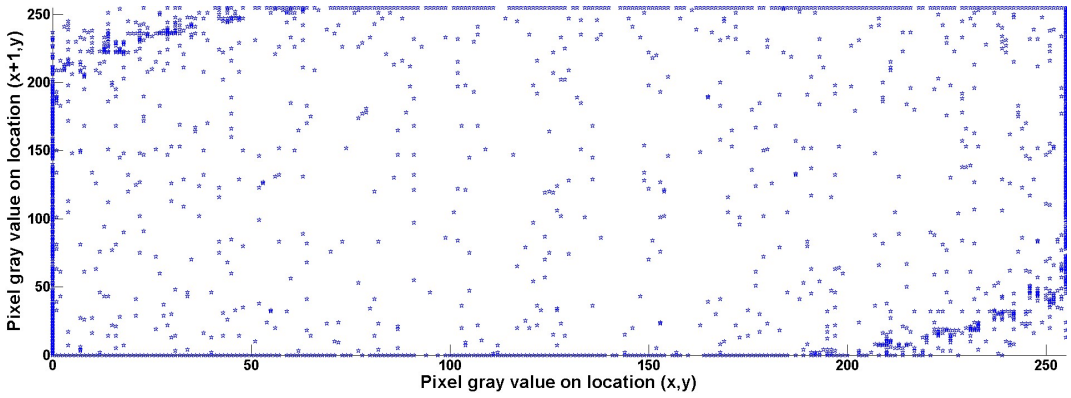


(e)

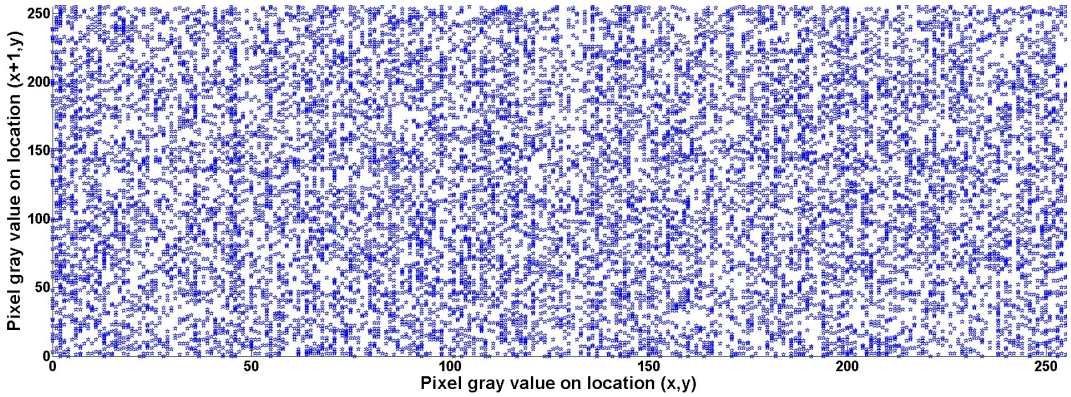
Fig. 10 Original, Encrypted, Decrypted images and their histogram plot corresponding: (a) QR Code; (b) Ultrasound; (c) Infected Lungs; (d) Baboon and (e) Peppers.

The correlation analysis is performed in this work to look at the relationship between pixels. This is important to consider because close pixels in digital photographs have a high association with each other in

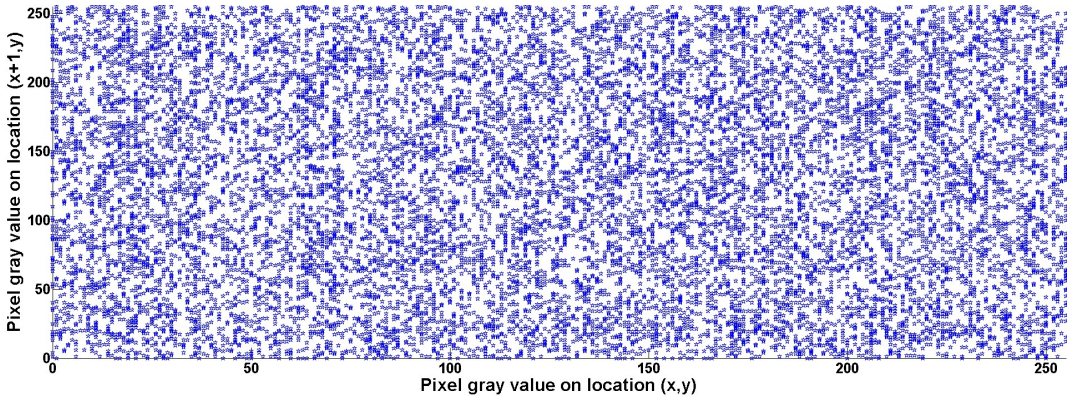
all directions. Thus, to withstand statistical attacks, encrypted images should require minimal correlation between adjacent pixels. All image encryption schemes require that the encrypted image differs greatly from the original image to prevent differential attacks. The NPCR can be measured to test for this kind of change. The NPCR calculates the number of pixels that differ between the original and encrypted image. The structural difference between the two images is reflected by a value that is close to one. Table 5 includes the correlation analysis and NPCR results of five different 128×128 grayscale images (QR Code, Ultrasound, Infected Lungs, Baboon, and Peppers). These two parameters are evaluated for three different steps of encryption.



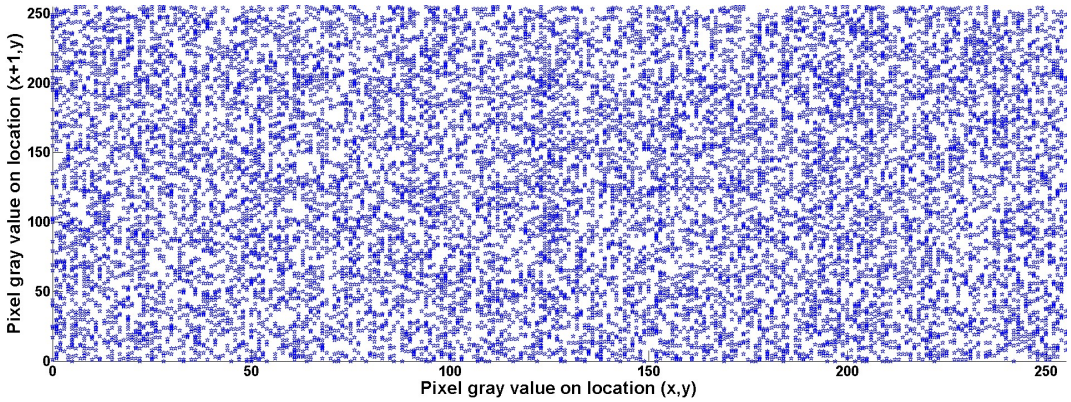
(a)



(b)



(c)



(d)

Fig. 11 Correlation analysis between pixels of: (a) Original image of QR Code; (b) First Encrypted image of QR Code; (c) Second Encrypted image of QR Code; and (d) Third Encrypted image of QR Code.

The histogram of Original, Encrypted, and Decrypted Images are shown in Fig. 10 corresponding QR Code, Ultrasound, Infected Lungs, Baboon, and Peppers images. The histogram of original, encrypted, and decrypted QR Code images are shown in Fig. 10(a). The same for ultrasound, infected lung, baboon, and pepper images are shown in Figs. 10(b), (c), (d), and 10(e). It is observed that the histogram of encrypted images is almost flat therefore it indicates quality encryption. Fig. 11 shows the correlation distributions of encrypted images corresponding to QR code. The correlation distributions corresponding to the original, first-encrypted, second-encrypted, and third-encrypted QR Code images are shown in Fig. 11(a), (b), (c), and (d).

Table 5 presents the key space, correlation coefficients, UACI, NPCR, information entropy, and quantitative image-quality metrics, including PSNR, MSE, and SSIM, obtained for four 128 × 128 grayscale test images using the proposed encryption algorithms. The performance of the proposed algorithms is evaluated at three different levels of encryption.

This table summarizes the correlation coefficients in the horizontal, vertical, and diagonal directions for the original images (Barbara, Cameraman, Peppers, and Baboon) and their corresponding encrypted images. The results indicate that the encrypted images exhibit negligible correlation with their respective original images. This significant reduction in correlation demonstrates the effectiveness of the proposed encryption scheme in eliminating the statistical relationships present in the original images. Consequently, the proposed scheme provides enhanced resistance against statistical attacks as compared to existing literature [44], [50], [51].

The experimental results further demonstrate that the information entropy values of the encrypted images are close to the ideal value of 8, while the correlation coefficients approach zero. In addition, the encrypted images exhibit relatively high MSE values, low PSNR values (below 10 dB), and SSIM values close to zero. These characteristics indicate a substantial difference between the original and encrypted images and confirm the effectiveness of the encryption process in concealing the visual information.

Furthermore, the obtained NPCR values are greater than 0.995, while the UACI values are close to the ideal value of 30%. These results demonstrate that even a small change in the plaintext image can produce significant changes in the corresponding ciphertext image. Therefore, the proposed encryption algorithms exhibit strong sensitivity to plaintext variations and provide effective resistance against differential attacks.

Table 5 Comparison of security parameters.

		Gary Scale Image (128×128)	Original Image	Proposed			References	
				Encryption-1	Encryption-2	Encryption-3		
Information Entropy		**QR**	3.8026	7.9313	7.9660	7.9715		--
		Ultrasound	5.7349	7.9440	7.9814	7.9834		--
		Lung	7.7262	7.9836	7.9870	7.9879		--
		Baboon	7.2184	7.9821	7.9884	7.9877		7.9866
		Peppers	7.5681	7.9829	7.9887	7.9875		7.9894
Encryption Quality	**MSE**	**QR**	--	18118	18828	18721	[44]	--
		Ultrasound	--	13643	13996	13881		--
		Lung	--	10314	10776	10935		--
		Baboon	--	7385.9	7621.1	7551.8		6691.3
		Peppers	--	8134.4	8293.3	8167.9		8290.0
	PSNR	**QR**	--	5.5497	5.3828	5.4076		--

		Ultrasound	--	5.5388	5.4280	5.4637		--
		Lung	--	7.6843	7.4940	7.4305		--
		Baboon	--	7.0720	6.9358	6.9755		8.1478
		Peppers	--	8.0554	7.9714	8.0376		7.9731
	SSI	**QR**	--	0.4572	0.4556	0.4577		--
		Ultrasound	--	0.4216	0.4207	0.4181		--
		Lung	--	0.7206	0.7173	0.7117		--
		Baboon	--	0.7537	0.7494	0.7482		0.7824
		Peppers	--	0.7433	0.7416	0.7419		0.7385
Differential Attack	**UACI**	**QR**	--	44.5360	45.5778	45.3947		--
		Ultrasound	--	37.5887	38.1212	37.9969		--
		Lung	--	32.5222	33.2064	33.4836		--
		Baboon	--	28.0230	28.4153	28.3502		27.0424
		Peppers	--	29.2615	29.4087	29.2087		29.4536
	NPCR	**QR**	--	0.9959	0.9960	0.9969		--
		Ultrasound	--	0.9948	0.9957	0.9962		--
		Lung	--	0.9955	0.9955	0.9962	[50]	--
		Baboon	--	0.9968	0.9960	0.9949		0.9960
		Peppers	--	0.9968	0.9961	0.9957		0.9962
Correlation Analysis	**Horizon-tal**	**QR**	0.8393	0.0018	-0.0034	0.0080	[51]	--
	Vertical		0.8514	0.0809	0.0246	-0.0137		--
	Diagonal		0.7088	0.0029	-0.0041	0.0050		--
	Horizon-tal	**Ultrasound**	0.9547	0.0025	-0.0020	0.0052		--
	Vertical		0.9116	0.0458	0.0039	0.0072		--
	Diagonal		0.8938	-0.0091	0.0057	-0.0017		--
	Horizon-tal	**Lung**	0.9824	0.0120	0.0064	-0.0085		--
	Vertical		0.9926	0.0375	0.0084	0.0036		--
	Diagonal		0.9775	-0.0074	-0.0003	-0.0119		--
	Horizon-tal	**Baboon**	0.8630	0.0040	-0.0030	0.0002		−0.0017
	Vertical		0.8752	0.0154	0.0046	-0.0111		0.0020
	Diagonal		0.8128	-0.0084	-0.0120	0.0094		0.0133
	Horizon-tal	**Peppers**	0.9216	0.0121	0.0026	0.0069		−0.0128
	Vertical		0.9418	0.0223	0.0040	-0.0017		−0.0141
	Diagonal		0.8697	-0.0028	0.0030	0.0050		0.0073

4. Conclusion

This paper summarizes the encryption method to hide the information of QR code and privacy-related medical images ultrasound infected lungs, etc. The hardware-efficient PRNG based on LCG and LFSR is used in this encryption algorithm that enhances the security strength of encrypted data. Three different hardware-efficient PRNG based on LCG and LFSR are proposed. The novelty of the proposed PRNG uses four 16-bit LFSRs that change the seed value of LCG blocks in every iteration independently. The S-box, one of the key elements of image encryption methods, is employed in this technique. Three 16×16 substitution boxes (S-boxes) are designed using proposed PRNGs. The proposed image encryption algorithm is proposed in this work encrypts the images (QR code and medical images like ultrasounds and infected lungs) up to three times in succession, using three different PRNGs and S-boxes each time. This significant reduction in correlation demonstrates the effectiveness of the proposed encryption scheme in eliminating the statistical relationships present in the original images. Consequently, the proposed scheme provides enhanced resistance against statistical attacks. The experimental results further demonstrate that the information entropy values of the encrypted images are close to the ideal value of 8, while the correlation coefficients approach zero. In addition, the encrypted images exhibit relatively high MSE values, low PSNR values (below 10 dB), and SSIM values close to zero. These characteristics indicate a substantial difference between the original and encrypted images and confirm the effectiveness of the encryption process in concealing the visual information. Furthermore, the obtained NPCR values are greater than 0.995, while the UACI values are close to the ideal value of 30%. These results demonstrate that even a small change in the plaintext image can produce significant changes in the corresponding ciphertext image. Therefore, the proposed encryption algorithms exhibit strong sensitivity to plaintext variations and provide effective resistance against differential attacks. Therefore, the proposed encryption technique is safe to use for both medical image and QR Code encryption to hide the information. Consequently, in real-time applications

for secure communication, the proposed approach can be used to create an effective image crypto-processor that obtains both the device's integrity and confidentiality.

List of Abbreviations

QR	Quick Response
PRNG	Pseudo Random Number Generator
LCG	Linear Congruential Generator
LFSR	Linear Feedback Shift Register
FPGA	Field Programmable Gate Array
HDL	hardware description language
UACI	Unified Average Changing Intensity
NPCR	Number of Pixels Change Rate
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error
SSIM	Structural Similarity Index Measure
MRI	Magnetic Resonance Imaging
CT	Computed Tomography
RC6	Rivest Cipher 6
AES	Advanced Encryption Standard
IDEA	International Data Encryption Algorithm
LUT	Look Up Table
FF	Flip Flop
BBS	Blum Blum Shub
CLCG	Coupled Linear Congruential Generator
CVLCG	Coupled Variable-Input Linear Congruential Generator
IoMT	Internet of Medical Things
IoT	Internet of Things
ISE	Integrated Synthesis Environment
LSB	Least Significant Bit
MSB	Most Significant Bit
PRBG	Pseudo-Random Bit Generator
RTL	Register-Transfer Level
XOR	Exclusive OR

Author Contributions

Mangal Deep Gupta: Conceptualization, Methodology, Software, Validation, Formal analysis, Supervision, Project administration, Writing – original draft, Visualization , Writing – review & editing. Pratham Srivastava: Software, Investigation, Data curation, Writing – review & editing, Visualization. Both authors reviewed and approved the final version of the manuscript.

Declaration of Interests/Conflict of Interest

There is no conflict of interest.

Availability of Data and Materials

The medical images used in this study, including the ultrasound and infected-lung images, were obtained from publicly available datasets on Kaggle [X-Ray, Ultrasound]. The standard test images, including Baboon and Peppers, were obtained from publicly available sources [Baboon, Peppers]

AI Use Declaration

There is no any AI tool used in preparation of this manuscript.

Ethics committee approval and consent to participate

This study used anonymized medical images obtained from publicly available datasets. No human participants were recruited or directly involved in this study. Therefore, ethics committee approval and informed consent were not applicable to the image-processing analysis conducted in this work.

Human Rights Statement

This study used patient-derived images. All procedures involving human participants and their data were conducted in accordance with the ethical principles of the Declaration of Helsinki

Funding

Not Applicable

Acknowledgements

The research was supported by the University Seed Money Scheme, administered by the Research Project Development Committee, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India. The scheme provides initial financial assistance to newly appointed faculty members to support their research activities.

5. References

[1] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimed. Tools Appl.*, vol. 78, no. 3, pp. 3457–3470, 2019, doi: 10.1007/s11042-018-6263-3.

[2] C. Ilioudis and G. Pangalos, "A framework for an institutional high level security policy for the processing of medical data and their transmission through the Internet," *J. Med. Internet Res.*, vol. 3, no. 2, pp. 18–31, 2001, doi: 10.2196/jmir.3.2.e14.

[3] K. Tamilarasi and A. Jawahar, "Medical Data Security for Healthcare Applications Using Hybrid Lightweight Encryption and Swarm Optimization Algorithm," *Wirel. Pers. Commun.*, vol. 114, no. 3, pp. 1865–1886, 2020, doi: 10.1007/s11277-020-07229-x.

[4] M. D. Gupta and R. K. Chauhan, "Hardware Efficient Pseudo-Random Number Generator using Chen Chaotic System on FPGA," *Journal of Circuits, Systems and Computers*, vol. 31, no. 03, p. 2250043, 2022, doi: 10.1142/S0218126622500438.

[5] C. İnce, K. İnce, and D. Hanbay, "Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices," *Multimed. Tools Appl.*, vol. 83, no. 29, pp. 72789–72817, 2024, doi: 10.1007/s11042-024-18620-2.

[6] S. Pankaj and M. Dua, "Chaos based Medical Image Encryption Techniques: A Comprehensive Review and Analysis," *Information Security Journal: A Global Perspective*, vol. 33, no. 3, pp. 332–358, May 2024, doi: 10.1080/19393555.2024.2312975.

[7] M. Vijayakumar and A. Ahilan, "An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map," *Ain Shams Engineering Journal*, vol. 15, no. 4, p. 102620, 2024, doi: https://doi.org/10.1016/j.asej.2023.102620.

[8] S. Adhikari, A. Panja, and S. Karforma, "ICSPRNG: Ikeda assisted Cryptographically Secure Pseudo Random Number Generator," *Multimed. Tools Appl.*, 2024, doi: 10.1007/s11042-024-19093-z.

[9] M. D. GUPTA, R. K. CHAUHAN, and V. K. UPADDHYAY, "Analyses of Reconfigurable Chaotic Systems and their Cryptographic S-box Design Applications," *Chaos Theory and Applications*, vol. 5, no. 3, pp. 219–232, 2023, doi: 10.51537/chaos.1285094.

[10] S. Krishnamoorthi, R. K. Dhanaraj, and S. K. Hafizul Islam, "CCM-PRNG: Pseudo-random bit generator based on cross-over chaotic map and its application in image encryption," *Multimed. Tools Appl.*, vol. 83, no. 34, pp. 80823–80846, 2024, doi: 10.1007/s11042-024-18668-0.

[11] R. Arshad, M. Jalil, W. Iqbal, and U. H. Chaudhry, "A Secure and Efficient Multi-Step Multi-Index Image Encryption Scheme Using Hybrid Combination of Substitution, Permutation and Hyper-chaotic Structure," *Arab. J. Sci. Eng.*, vol. 50, no. 2, pp. 1001–1024, 2025, doi: 10.1007/s13369-024-09099-y.

[12] M. Canadi, W. Höpken, and M. Fuchs, "Application of QR Codes in Online Travel Distribution," *Information and Communication Technologies in Tourism 2010*, pp. 137–148, 2010, doi: 10.1007/978-3-211-99407-8_12.

[13] P. Sutheebanjard, "Proceedings 2010 Eighth International Conference on ICT and Knowledge Engineering : November 24-25, 2010, Bangkok, Thailand.," pp. 89–92, 2010.

[14] P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," *IEEE Trans. Industr. Inform.*, vol. 12, no. 1, pp. 384–392, 2016, doi: 10.1109/TII.2015.2514097.

[15] ITSC, "Section 3: QR Code," *Synthesis Journal. Information Technology Standards Committee Singapore*, vol. 3, pp. 59–78, 2008.

[16] M. A. Gurdan durak, Emre Ozkeskin, "Uses of Smart Phones," *Turkish Online JOurnal of Distance Education*, vol. 17, no. April, pp. 42–58, 2016, [Online]. Available: https://dergipark.org.tr/en/download/article-file/222605

[17] S. Tiwari, "An introduction to QR code technology," *Proceedings - 2016 15th International Conference on Information Technology, ICIT 2016*, vol. 1, pp. 39–44, 2017, doi: 10.1109/ICIT.2016.38.

[18] A. Sankara Narayanan, "QR Codes and Security Solutions," *International Journal of Computer Science and Telecommunications*, vol. 3, no. 7, pp. 69–72, 2012, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.9840&rep=rep1&type=pdf

[19] Y. Lin, S. Member, Y. Chang, and J. Wu, "Appearance-Based QR Code Beauti fi er," vol. 15, no. 8, pp. 2198–2207, 2013.

[20] T. Yuan, Y. Wang, K. Xu, R. R. Martin, and S. M. Hu, "Two-Layer QR Codes," *IEEE Transactions on Image Processing*, vol. 28, no. 9, pp. 4413–4428, 2019, doi: 10.1109/TIP.2019.2908490.

[21] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, "QR code security: A survey of attacks and challenges for usable security," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8533 LNCS, pp. 79–90, 2014, doi: 10.1007/978-3-319-07620-1_8.

[22] N. Sasikaladevi, K. Geetha, and A. Revathi, "EMOTE – Multilayered encryption system for protecting medical images based on binary curve," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 3, pp. 676–686, 2022, doi: 10.1016/j.jksuci.2019.01.014.

[23] P. Rashmi, M. C. Supriya, and Q. Hua, "Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/9363377.

[24] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. Al-Tameemi, "Robust large image steganography using lsb algorithm and 5d hyper-chaotic system," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 689–698, 2021, doi: 10.11591/eei.v10i2.2747.

[25] J. Selvaraj, W. C. Lai, B. P. Kavin, K. C, and G. H. Seng, "Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security," *Electronics (Switzerland)*, vol. 12, no. 7, 2023, doi: 10.3390/electronics12071636.

[26] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020, doi: 10.1016/j.future.2020.02.029.

[27] J. Jain and A. Jain, "Securing E-Healthcare Images Using an Efficient Image Encryption Model," *Sci. Program.*, vol. 2022, 2022, doi: 10.1155/2022/6438331.

[28] H. M. Yuan, Y. Liu, T. Lin, T. Hu, and L. H. Gong, "A new parallel image cryptosystem based on 5D hyper-chaotic system," *Signal Process. Image Commun.*, vol. 52, pp. 87–96, 2017, doi: 10.1016/j.image.2017.01.002.

[29] Z. Lv and F. Piccialli, "The Security of Medical Data on Internet Based on Differential Privacy Technology," *ACM Trans. Internet Technol.*, vol. 21, no. 3, 2021, doi: 10.1145/3382769.

[30] M. K. Hasan *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi: 10.1109/ACCESS.2021.3061710.

[31] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/5978636.

[32] F. Masood *et al.*, "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," *Wirel. Pers. Commun.*, vol. 127, no. 2, pp. 1405–1432, 2022, doi: 10.1007/s11277-021-08584-z.

[33] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimed. Tools Appl.*, vol. 81, no. 5, pp. 7253–7270, 2022, doi: 10.1007/s11042-021-11812-0.

[34] W. El-Shafai, F. Khallaf, E. S. M. El-Rabaie, and F. E. A. El-Samie, "Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services," *J. Ambient Intell. Humaniz. Comput.*, 2022, doi: 10.1007/s12652-022-03832-x.

[35] M. D. Gupta and R. K. Chauhan, "Efficient Hardware Implementation of Pseudo-Random Bit Generator Using Dual-CLCG Method," *Journal of Circuits, Systems and Computers*, vol. 30, no. 10, pp. 1–6, 2021, doi: 10.1142/S0218126621501826.

[36] M. D. Gupta, R. K. Chauhan, and S. Gulia, "Hardware Efficient Hybrid Pseudo-Random Bit Generator Using Coupled-LCG and Multistage LFSR with Clock Gating Network," *Journal of Circuits, Systems and Computers*, vol. 32, no. 3, pp. 1–24, 2023, doi: 10.1142/S0218126623500391.

[37] M. D. Gupta and R. K. Chauhan, "Coupled variable-input LCG and clock divider-based large period pseudo-random bit generator on FPGA," *IET Comput. Digit. Tech.*, vol. 15, no. 5, pp. 349–361, 2021, doi: 10.1049/cdt2.12027.

[38] A. Kumar Panda and K. Chandra Ray, "A coupled variable input LCG method and its VLSI architecture for pseudorandom bit generation," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 4, pp. 1011–1019, 2020, doi: 10.1109/TIM.2019.2909248.

[39] A. K. Panda and K. C. Ray, "Modified dual-CLCG method and its VLSI architecture for pseudorandom bit generation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 3, pp. 989–1002, 2019, doi: 10.1109/TCSI.2018.2876787.

[40] A. Kadir, A. Hamdulla, and W. Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik (Stuttg).*, vol. 125, no. 5, pp. 1671–1675, 2014, doi: 10.1016/j.ijleo.2013.09.040.

[41] Sri Indah Desti and A. A. Hamdan, "Forgery Detection and Authentication of Medical Images using Adaptive Bit Substitution Watermarking," *IJACI : International Journal of Advanced Computing and Informatics*, vol. 2, no. 2, pp. 139–151, Feb. 2026, doi: 10.71129/ijaci.v2i2.pp139-151.

[42] W. Ilham and A. Ahmad, "A Comprehensive Review of ConvNeXt Architecture in Image Classification: Performance, Applications, and Prospects," *IJACI : International Journal of Advanced Computing and Informatics*, vol. 2, no. 2, pp. 108–114, Oct. 2025, doi: 10.71129/ijaci.v2i2.pp108-114.

[43] S. Ding *et al.*, "Design of a three-dimensional logistic map and its application to seafood image encryption," *J. Supercomput.*, vol. 82, no. 4, p. 225, 2026, doi: 10.1007/s11227-025-08196-5.

[44] M. D. Gupta and R. K. Chauhan, "Secure image encryption scheme using 4D-Hyperchaotic systems based reconfigurable pseudo-random number generator and S-Box," *Integration*, vol. 81, pp. 137–159, 2021, doi: 10.1016/j.vlsi.2021.07.002.

[45] S. B. LAKASEK and H. Elhadi, "A Robust Image Watermarking Technique Using NSST-HD-SVD," *IJACI : International Journal of Advanced Computing and Informatics*, vol. 2, no. 2, pp. 115–126, Feb. 2026, doi: 10.71129/ijaci.v2i2.pp115-126.

[46] S. Ding *et al.*, "SRA: A sine-based reconstruction approach to improve 2D chaotic map performance," *The European Physical Journal Plus*, vol. 141, no. 2, p. 182, 2026, doi: 10.1140/epjp/s13360-026-07421-1.

[47] S. Gao *et al.*, "A 3D Memristive Cubic Map With Dual Discrete Memristors: Design, Implementation, and Application in Image Encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 35, no. 8, pp. 7706–7718, 2025, doi: 10.1109/TCSVT.2025.3545868.

[48] M. Van Der Haak, A. C. Wolff, R. Brandner, P. Drings, M. Wannenmacher, and T. Wetter, "Data security and protection in cross-institutional electronic patient records," *Int. J. Med. Inform.*, vol. 70, no. 2–3, pp. 117–130, 2003, doi: 10.1016/S1386-5056(03)00033-9.

[49] S. Ullah, X. Liu, A. Waheed, and S. Zhang, "An efficient construction of S-box based on the fractional-order Rabinovich–Fabrikant chaotic system," *Integration*, vol. 94, p. 102099, 2024, doi: https://doi.org/10.1016/j.vlsi.2023.102099.

[50] Ü. Çavuşoğlu and S. Kaçar, "A novel parallel image encryption algorithm based on chaos," *Cluster Comput.*, vol. 22, no. 4, pp. 1211–1223, 2019, doi: 10.1007/s10586-018-02895-w.

[51] Sivaraman R, S. Rajagopalan, and R. Amirtharajan, “FPGA based generic RO TRNG architecture for image confusion,” *Multimed. Tools Appl.*, vol. 79, no. 19–20, pp. 13841–13868, 2020, doi: 10.1007/s11042-019-08592-z.