Design of New Cryptosystem to Protect the Transmitted Data for Imam Hussein's Visitors or Protection Units

Prof.Faez Hassan Ali

(1).Dept. of Mathematics, College of Science, Mustansiriyah University.

Prof. Samira Naji Kadhim

. Dept. of Mathematics, College of Science for Women, Baghdad University.

Asst.Dr.Adnan Mohammed Ali

Computer Technology Engineering Department, Baghdad College of Economic Sciences University.

Abstract:

This paper presents the design of a new stream cipher cryptosystem (CS) with a new Key Generator (KG). Firstly, we presented the mathematical model of the new CS, which is based on Linear Feedback Shift Registers (LFSR) units with non-linear combined functions to increase the complexity of the design CS. This cryptosystem can be used to protect data transmitted (online or offline) during the Arbaeen pilgrimage commemorating Imam Hussein's martyrdom, peace be upon him, whether by pilgrims or/and military protection units affiliated with the army or police. To test the output key results, we apply Basic Efficiency Criteria (BEC) to the suggested KG. The results of using BEC demonstrate the robustness and efficiency of the new stream cipher CS.

Keywords: Cryptography, Cryptosystem, Stream cipher, Linear Feedback Shift Registers, Basic Efficiency Criteria, Multiplicative Cyclic Group.

Introduction

The issue of information protection has become one of the most important matters of concern to those interested, especially in light of the rapid development of information technology and its means of transmission and the development of methods of penetration of such information, especially information classified to a high degree of confidentiality, including Secret Information (SIs). (Shaker, Nasser, & Ali, 2023)

The basics of the problems that occur during the process of transferring SP's will be discussed, and then the means of addressing them through proposing and designing a CS for protecting those SIs.

implemented a new style based on the dynamic algorithm, which is based on the concept to alter the framework of the LFSRs with every modification in the initial keys to obtain a complex ciphering algorithm based on a bank of LFSRs stored in a file and selecting random 10 LFSR's. They use BEC on KG to validate the result, which passes all of the tests. (Salih, Al-Safi, & Ali, 2014) design a new robust and dynamic CS called Robust and Efficient Dynamic Stream Cipher Cryptosystem (RDSCC) using stream KG which has good random statistical properties. The RDSCC is constructed to be flexible to encrypt (decrypt) different types of data; like message text and image data efficiently. (Ghazi & Ali, 2018)

proposed (5) algorithms for CS: encryption, decryption, signature generation, key generation, and signature verification. The proposed CS construction is based on the quadratic residue, quadratic quotient, floor function, absolute value recording, Diffie-Hellman key exchange protocol, and probability theorem. (Hossain, 2019) The advantage of the proposed CS intensive technique is that the intended receiver receives only one PT value that distinguishes the CT from the PT by verifying the send-

er's signature. (Gad, Hagras, Soliman, & Hikal, 2021) present a novel fuzzy multi-modular chaotic map for images encryption (Chen, Xie, & Zhang, 2022) used a modified Henon Map to Combination Section Image Encryption algorithm. (Ali, Ali, Redha, & Abubakari, 2023) construct a novel efficient stream cipher cryptosystem (SCSC) to decrypt (encrypt) digital images. The new system achieves the efficiency criteria that were applied to both the encrypted images and the key which obtained from the KG. (Ali, Mahdi, Ali, & Abdulkareem, 2024), present an overview on the use of information technology for data security. The most common data protection technologies are introduced, including CG (and CS design) and information hiding. Additionally, they refer to the CA and Steganalysis approaches to demonstrate how we can attack data, particularly send data.

In section 2 we introduce some basics of cryptography and SCs. In section 3, we discuss some important Stream Cipher SC's. Section 4 introduces the BEC for CSCS. The problem statement is discussed in section 5. In section 6, we introduce the new proposed CS to protect the communication of pilgrims. Section 7 introduces the proposed KG for the suggested CS with implementation of BEC. In section 8 we will show the user interface of PHVCCS. Lastly, the conclusions and future works are introduced in section 9.

Cryptography and Cryptosystems

- Cryptography (CG) is the study of principles and techniques by which information or plaintext (PT) can be concealed in ciphertext (CT) and later revealed by legitimates users employing the secret key (SK), but in which it is either impossible or computationally infeasible for an unauthorized person to do so. Cryptanalysis (CA) is the scie**nce (and art) of** recovering

PT from CT without knowledge of the SK. Both terms are subordinate to the more general term Cryptology. The CG concerned in Encryption (EP) and Decryption processes (DP) [9] (Motwani & Raghavan, 1995).

Some encryption algorithms (E_k) use a SK, so that the CT depends on both the original PT and the SK value. Some-times the Encryption key (e_k) and the decryption key (d_k) are same. Other times e_k and d_k come in pairs. Then d_k, Inverts the e_k. A SK allows different encryptions of one PT just by changing the SK. Use of a SK provides additional security. If the E_k should fall into the interceptor's hands, future messages can still be kept secret because the interceptor will not know the SK value [1]

- The Cryptosystem (CS) : are the systems which use the EP and DP. The CS divided into Secret-Key CS (SKCS) and Public Key CS (PKCS). The SKCS consists of Classical CS (CCS) and Modern CS (MSC). The MSC divided into Block Cipher CS (BCSC) and Stream Cipher CS (SCSC), these CS's can be classified as in figure (1)

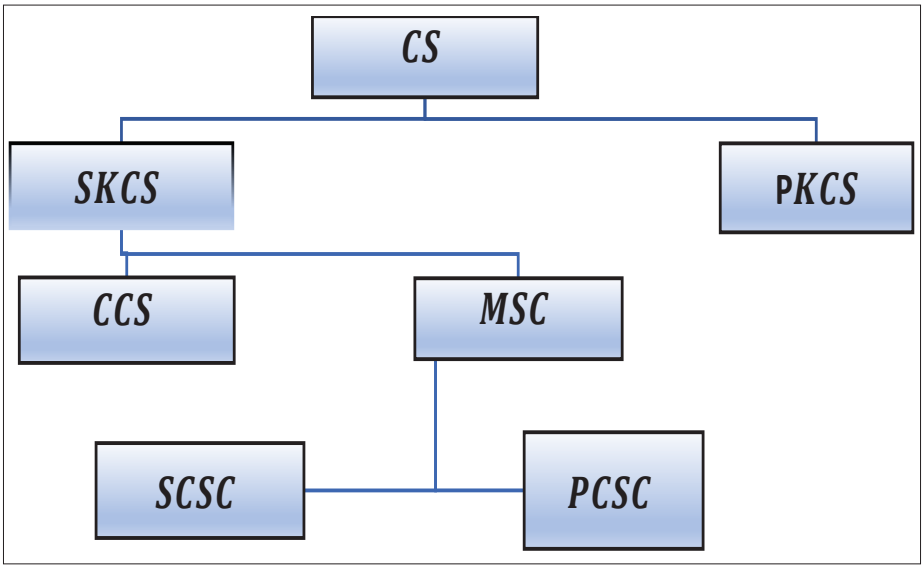

Figure (1) classification.

In a SKCS, the same SK will be used ($ek = d_k = k \epsilon K$), which is used in both EP and DP. It's also called symmetric cryptosystems.

The sender uses an invertible transformation, so produce the CT [10]:

$$C = (Ek\ (m)) \qquad ....(1)$$

where $m \epsilon M$ and $c \epsilon C$, and transmits it over the public insecure channel to the receiver. The *SK (k)* should also be transmitted to receiver by using a secure channel to decrypt c by function:

$$D_k\ (c) = D_k\ (E_k\ (m)) = m \qquad ....(2)$$

Where $c \epsilon C$ and $m \epsilon M$ and it's the PT.

There are many different types of , like monographic (character) ciphers, polygraphic (block) ciphers, exponentiation ciphers and (bit) ciphers [10] (Yan, 2000).in which we will focus.

Some Important SCSC

In this part we will introduce two important units which are very suitable to be used in CSCS because of their mathematical background, high complexity, high periodicity, randomness, speed when they be design software or hardware.

1.Linear Feedback Shift Register Systems

Linear Feedback Shift Register (LFSR) systems are used widely in SCSC field. A LFSR System consists of two main basic units. First, is a LFSR function and initial state values (Schneier, 1995). The second one is, the Combining Function (CF), which is a boolean function which is combined the output (x_i) of each LFSR s.t. CF=F($x_1, x_2, ..., x_n$). Most of SCSC are depend on these two basic units (Whitesitt, 1995).

2. Multiplicative Cyclic Group [13]

The Multiplicative Cyclic Group (MCG) unit generates the sequence S is a function of five variables which are not related to each other s.t. S=MCGU(q,a_t,a_r,γ,m), where $1 \le \gamma \le q-1$ is any start integer point. These variables are as follows:

- q is prime number.
- $a_t \neq a_r$ are two different generators.
- m is the digit value of the sequence which generated from the (for binary sequences we use $m = 2$).
- γ is the start point where $1 \le \gamma \le q-1$.

The MCG is very suitable to be used in . The algorithm steps can be found in [13]·(Ali, 2006).

Basic Efficiency Criteria for SCSC

Efficiency metrics are one of the most basic methods for measuring algorithm performance.We will now present some properties for *SCSC's* Basic Efficiency Criteria (*BEC*).

1. Randomness Tests (RTs)

When the *KG* designed to encrypt/decrypt one character or byte from PT, so we have to depend on the *RTs* to test the sequences *S* which belong to the filed $GF(2^8)$. The used *RTs* is 256-Digital Tests (*256DT*) which consists of (Ali, Ali, & Redha, 2023):

- **Digital Frequency Test (DFT):** Let's the expected number (*EN*) of digit *i* is $E^F = 0.0039L$, while n_i be the observed number (*ON*) of digit *i* in *S* , (*i* =0,1,…,255), then the statistic value T^F of *DFT* is:

$$T^F = \frac{256}{L}\sum_{i=0}^{255}(n_i - 0.0039L)^2 \qquad \text{.....(3)}$$

With freedom degree υ=255.

• **Digital Run Test (DRT):** Let E_j^R be the *EN* of runs with length *j*, and the ON of runs is R_{ij} with type *i* runs with length *j*, then, the T_i^R of *DRT* is:

$$T^R = \sum_{i=0}^{255}\sum_{j=0}^{M_i}\frac{\left(R_{ij}-E_j^R\right)^2}{E_j^R} = \sum_{j=0}^{M_i}\frac{\left(R_{ij}-65025L/256\right.}{65025L/256^{j+}} \quad .....(4)$$

With $\upsilon_i = 256\ (M_i\text{-}1)$,where M_i is maximum length of run *i*.

• **Digital Auto-Correlation Test (DA-CT):** The *ON* of similar and distinct digits are $n_0(\tau)$ and $n_1(\tau)$ after shifting *S* by τ respectively, where τ =1,2,…,L-1, while the *EN* of similarity and difference respectively are: $E_0^A(\tau)=0.004(L-\tau)$ and $E_1^A(\tau)=0.996(L-\tau)$ ….(5)

and

$$T^A(\tau) = \sum_{i=0}^{1}\frac{\left(n_i(\tau)-E_i^A(\tau)\right)^2}{E_i^A(\tau)} \quad ....(6)$$

with υ =1.

The Randomness of *LFSR's* system proven in [3].

2.Key Space Analysis

In order to remain secure via the exhaustive search attacks, it must make the method's key space as big as possible. A safeguard key space ought to exceed 2^{128}(Alvarez & Li, 2006).

3.4.3 Efficiency Criteria Calculations of MCGU

1. The following cases described the good efficient sequences which is generated from the [16] (Ali, 2009):

• **Linear Complexity (LC):** the LC is secure when the MCGU has high non-linearity.

• **Periodicity (P(S)):** Every generated S has a period of q-1. So, if we have two distinct generators so we have $P_2^{(g(q))}$ generators. Lastly, the *MCGU* period is:

Semi-Annual Scientific Journal www.arbnj.com Ramadan 1447 A.H, March 2026 A.D

$P(S)=P_2^{(g(q))}*(q-1)$ ….(7)

Where $g(q) = \varphi(q-1)$.

- **Randomness (R(S))** : The randomization of *MCGU* is proved in [13].
- **General Complexity (GC(S))** : Suppose we have Nq primes (q), so we obtain g(q) different ways to select a to get the set A(q).$P_2^{(g(q)}$ choices to take two different generators in A(q), and q-1 choices to obtain γ so the general complexity can be calculated as follows:

$GC(S)=Nq*\phi(q-1)* *(q-1)$ ....(8)

Problem Statement

The Arbaeen pilgrimage commemorating the martyrdom of Imam Hussein (peace be upon him) is one of the most important and sacred religious rituals for all Muslims, particularly in Iraq and some neighboring countries. Terrorists or terrorist organizations may exploit the gathering of Muslims to perform this important ritual to carry out terrorist acts. It is certain that these terrorists are fully aware of all SI and calls that may occur between pilgrims or between the security agencies responsible for their safety. Consequently, the terrorists attempt to exploit every possible loophole or identify security weaknesses that exist at certain pilgrim protection sites.

Therefore, we deemed it appropriate to protect communications between pilgrims and the security agencies responsible for their safety, to prevent terrorists from exploiting the Arbaeen pilgrimage. This was achieved by implementing a new *CS* to protect important messages and calls, particularly those with a high level of confidentiality. The proposed *CS* can be installed on communications devices between security agencies, as well as on pilgrims' mobile phones to protect their communications with other pilgrims.

The Proposed to Protect the Communication of Pilgrims and security agencies

The proposed CS to protect Pilgrims and Security Agencies' (PA) communications is a software or hardware-based encryption/decryption algorithm that can be installed on security agencies' communications devices as well as on pilgrims' mobile devices to ensure secure information transmission. The proposed SC is called Protect Hussein's PA' Communications CS (PHPACCS). PHPACCS relies on a highly efficient KG that must pass internationally tests quality control standards.

The PHPACCS consists of two parts. The first part of PHPACCS is specialized for Encryption Process (PHPACCS-EP), it is a system dedicated to protecting the message. The other PHPACCS is specialized for Decryption Process (PHPACCS-DP). It is designed to remove protection from the message.

One of the most important requirements for proposed PHAPCCS is the Key Management System (KMS), this KMS is responsible for the encryption/decryption processes. The PHAPCCS depends on KG based on stream cipher which it depends on combination MCGU's. The output key of the proposed KG must pass all basic criteria efficiency tests (BCET), like linear complexity, periodicity, correlation immunity, randomness, …, etc. Figure (2) shows the basic and general scheme of the PHPACCS.

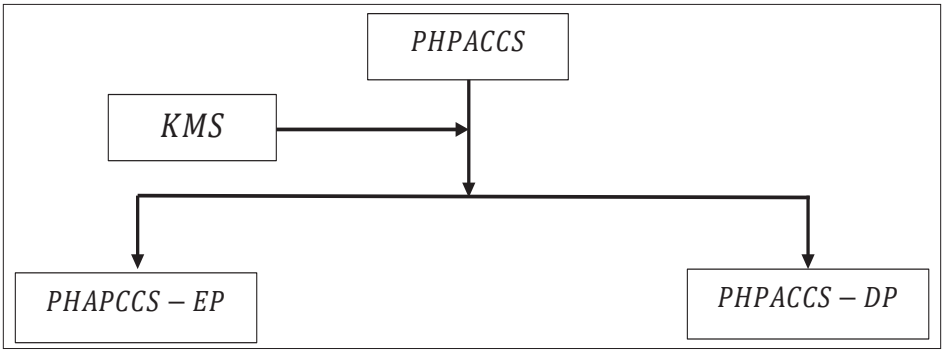

Figure (2): The general block diagram of the .

The Proposed KG for PHPACCS with BCET

In this section we proposed new stream cipher KG to be used in PHPACCS, to protect the SI. As known, the proposed stream cipher KG (which is very suitable to be used in high-speed information transmission) must have high complexity, good randomness, high periodicity, high correlation immunity and high speed.

1. Desing of New KG for PHPACCS

The proposed KG for PHPACCS depends on the LFSR and MCGU, so it's called **PHPACKG.**

A. Key Management of PHPACKG

The input key for PHPACKG depending in two subkeys, which are as follows:

- **Initial Key Bits (IKB):** This key consists of two parts:
  - **Basic key (BK):** This key is changed daily requires essential secret key consists of (16) ASCII CODE (8 bits) characters.
  - **Message key (MK):** This key is changed with each message requires public key consists of (10) ASCII CODE characters.

- **MCGU Key (MCGK):** To implement this unit, we will use prime number (q), two generators (α_1 and α_2) with start point γ. This subkey changed every day.

The *BK* and *MCGK* are secret must be sent over a secure channel physically and it can be stored with protection in the same environment of the *PHPACCS*

B. PHPACKG Components

The main components of PHVCKG are as follows:

- **LFSR'S unit (LFSRU):** It's a system consist of 2 LFSR's:
  - LFSR1: depends on the characteristic polynomial x^53+x^2+1ϵ GF(2).
  - LFSR2: depends on the characteristic polynomial x^71+x^3+1ϵ GF(2).

$$\text{Per}(LFSRU) = \text{lcm}(L_1, L_2) = \Pi^2_{(i=1)} L_i \quad \ldots.(9)$$

- **RAM Unit (RAMU):** Consists of 256 random and different bytes.
- **MCGU:** depends on (q, α_1,α_2) and start point *s*.

C. PHPACKG Initialization

1. Converts the two keys (*BK* and *MK*) to binary from to obtain sequence of *IK* consists from 128 (16×8) bits.
2. The two *LFSR's* is are filled by *IK* and fill the last stage from each *LFSR* by 1.
3. Use the chosen (q, α_1,α_2, s) for *MCGU.*

D. PHPACKG Moving

1. Filling the *LFSRU* by combining *BK* and *MK.*
2. Moving *LFSRU* to fill the *RAMU* with random and different bytes.
3. Each time the LFSRU produces (8) bits that form an address (*AD*), from each LFSR four bits.

4. The *AD* is considered as an input to the *RAMU* to obtain a Variable Byte called *V-byte (VB)*.

5. The *MCGU* moves to generate four bytes called MCG-Byte (*MCGB*) which is xored with *VB* to obtain *KB s.t.*

   KB=VB XOR MCGB ....(10)

6. The KB is xored with one plain byte (*PB*) to obtain cipher byte (*CB*).

   CB=PB XOR ....(11)

figure (3) shows the main diagram of PHVCKG.

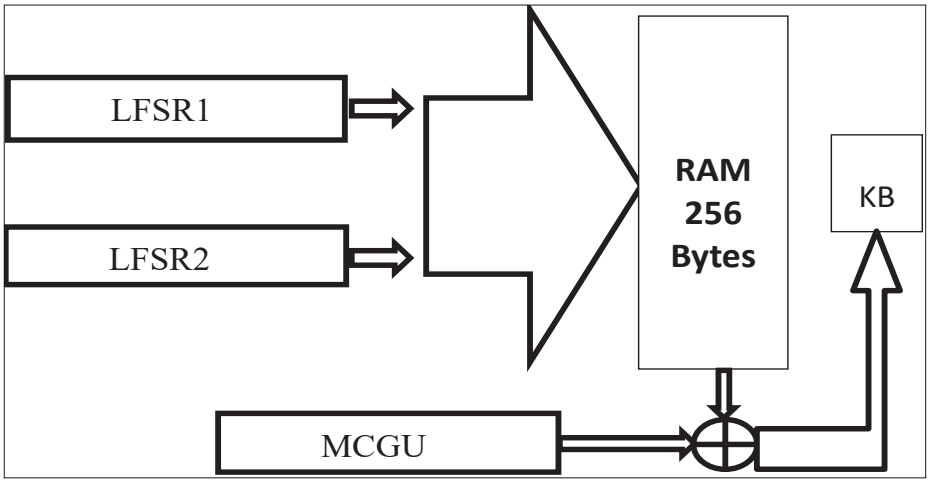

figure (3) shows the main diagram of .

2. Implementation of on

A. Standard using

In this subsection, the *256DT* will applied to check the results of key sequences generated from PHPACKG for three various examples with different lengths (in bytes) with different initial keys (*IK*). This information shown in table (1).

Table (1): Various examples with different lengths and inputs.

Example	Length of Key file ($\times 10^3$ bytes)	*IK* for *LFSRU*	*MCGU* q =10103
1	15	69 54 145 164 107 153 242 21 27 37 43 59 147 14 238 186	
2	30	22 160 169 87 228 251 197 149 237 148 105 31 220 124 216 54	
3	50	93 13 125 58 32 53 38 49 11 162 72 38 178 128 137 134	

For DFT and DRT, T value compared with υ and T_0,(using relations (3) and (4)) finally the randomness decision, all these results are shown in table (2).

Table (2): Results of *DFT* and *DRT*

Test	Example	T	υ	T_0	Decision
DFT	1	271.1	255	288.016	Pass
	2	211.3			Pass
	3	239.8			Pass
DRT	1	516.1	512	559.408	Pass
	2	543.9			Pass
	3	551.3			Pass

For DA-CT, firstly, shifting (τ =1,2,…,100) for the generated sequence S, the ratio of pass (rp) with maximum, mean and minimum of differences (mxd,md,mnd) between T value and T0=3.841 with υ =1 (using relations (5) and (6)). All these results are shownin table (3).

Table (3): Results ofτ

Issue	*rp*	*mxd*	*md*	*mnd*
1	98٪	3.48	2.42	1.86
2	97٪	2.94	2.25	0.311
3	95٪	3.78	1.76	1.19

B. Periodicity of PHPACKG

Since we have (2) *LFSRs* in *PHPACKG* with *MCGU* (see section (4.3)), then the periodicity of *PVHCKG:*

Per (S) = Per(LFSRs) Per(MCGU)*, then:

$$Per(S) = L.C.M = (2^{L1} - 1, 2^{L2} - 1) * P_2^{g(q)} * (q-1) \quad \ldots(12)$$

Since the period of the two combined LFSRs are coprime (see relation (9)), then:

For instance, if q =2021 then:

$$Per(S) = 2^{165} * 2^{23} = 2^{188}$$

C. Key Space (KS) of PHPACKG

The size *KS* which considered *GC* for cryptosystem which can be calculated by:

For *MCGU*, we have: $GC(MCGU) = \phi(q-1) * P_2^{\phi(q-1)} * (q-1)$, (see relation (8) and set Nq =1).

So the *GC* for *PHVCKG* can be calculated by relation (11):

$$GC(S) = 2^{128} * \phi(q-1) * P_2 P_2^{\phi(q-1)} * (q-1) \quad \ldots.(11)$$

Remark (1): For the performance metrics of PHPACCS, since the PHPACKG consists of just two LFSR's and one MCGU we sure that it has low execution time and need no much memory to be execute.

User Interface of PHPACCS

Figure (4) shows the main interface of PHPACCS after execute the application of PHPACCS. As seen the interface consists of Encryption/ Decryption buttons and two editors for entering plain/Cipher text.

Figure (4): main interface of PHPACCS.

In the main interface, the pilgrims' or the pilgrims' protection officer will enter the PT of the message then press "Encryption" to protect the information, then obtain the CT to send it to the legal receiver. These details are shown in figure (5).

Figure (5): The and after Appling .

Conclusions and Future Work

1. In this paper, we proposed a protection system for s which possess from the pilgrims or between the security agencies responsible for their safety in the Arbaeen pilgrimage commemorating the martyrdom of Imam Hussein (peace be upon him).
2. The passes all the tests like randomness (frequency, run and autocorrelation tests), periodicity and general complexity, so it's now able to work effectively and practically.
3. The is considered a nonlinear system because of two reasons; first is the and which are hard to be analyzed.
4. The has a few requirements to be applied in any the suitable environment and its inexpensive and simple to operate, both software or hardware.
5. The is just a nucleus of an initial idea for a communications protection sys-

tem for pilgrimages and security forces, and it is subject to modification or development according to the requirements of solving the basic problem.

6. We call the official security agencies to take a benefit from the to keep their in save since its national, not commercial, encryption system.
7. We can generalize the using of to be suitable to encrypt the images and voice digital files, if that done, we may use the steganography to add to the to increase the security of the .

References

8. Ali, A. M., Ali, F. H., & Redha, S. M. (2023, June 1). Using statistical methods to increase the contrast level in digital images. Journal of Economics and Administrative Sciences (JEAS), 29(136), 49–59. https://doi.org/10.33095/jeas.v29i136.
9. Ali, A. M., Ali, F. H., Redha, S. M., & Abubakari, N. (2023). Image encryption using non-linear stream cipher cryptosystem. Al-Mustansiriyah Journal of Science, 34(2). http://doi.org/10.23851/mjs.v34i2.1294
10. Ali, F. H. (2006). Use the multiplicative cyclic group to generate pseudo random digital sequences. Al-Rafidain University College for Sciences, (20), 122–135.
11. Ali, F. H. (2009). High efficient sequences generate from developed MCG generator. Al-Rafidain University College, (25), 169–182.
12. Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(8), 2129–2151.
13. Chen, Y., Xie, S., & Zhang, J. (2022). A hybrid domain image encryption algorithm based on improved Henon map. Entropy (Basel), 24(2), 287.

14. Gad, M., Hagras, E., Soliman, H., & Hikal, A. (2021). A new parallel fuzzy multi modular chaotic logistic map for image encryption. The International Arab Journal of Information Technology, 18(2), 227–236.

15. Ghazi, A. A., & Ali, F. H. (2018). Design of new dynamic cryptosystem with high software protection. Iraqi Journal of Science, 59(4C), 2301–2309. https://doi.org/10.24996/ijs.2018.59.4C.17.

16. Hossain, S. (2019). Design a new cryptosystem. International Journal of Scientific and Research Publications (IJSRP). https://doi.org/10.29322/IJSRP.29.12.2019.

17. Motwani, R., & Raghavan, P. (1995). Randomized algorithms. Cambridge University Press.

18. Salih, M. M., Al-Safi, M. G. S., & Ali, F. H. (2014). [Article title not provided]. IOSR Journal of Computer Engineering (IOSR-JCE), 16(2, Ver. VIII), 72–78. Retrieved from http://www.iosrjournals.org.

19. Schneier, B. (1995). Applied cryptography. John Wiley & Sons.

20. Shaker, S. A., Nasser, A. G., & Ali, F. H. (2023). Constructing a digital certificate authentication system for classified documents. Iraqi Journal of Science, 64(3), 1391–1400. https://doi.org/10.24996/ijs.2023.64.3.31.

21. Whitesitt, J. E. (1995, April). Boolean algebra and its application. Dover Publications.

22. Yan, S. Y. (2000). Number theory for computing (2nd ed.). Springer-Verlag.