International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V71I2P241

Volume 71 Issue 2, 399-407, February 2023
© 2023 Seventh Sense Research Group®

Original Article

Blockchain with Mayfly Optimization-based Chaotic Encryption Model for Smart and Secured Question Paper Sharing

B. Nagarajan[1], C. Ananth[2], N. Mohananthini[3]

[1,2]*Department of Computer and Information Science, Annamalai University, Annamalainagar, India.*
[3]*Department of Electrical and Electronics Engineering, Muthayammal Engineering College, Rasipuram, India*

[2]*Corresponding Author : ananth.prog@gmail.com*

Received: 20 September 2022 Revised: 09 February 2023 Accepted: 18 February 2023 Published: 25 February 2023

Abstract *- Recently, Blockchain (BC) has gained significant interest in several application areas of finance, entertainment, healthcare, education, etc. Examination plays a vital role in the education system. But there is a risk called question paper leaking (QPL), which can result in unfairness problems at the time of examinations. QPL can lead to some major challenges, like compromising education quality and loss of ethical standards. So, a smart and secure education system using BC can be developed for sharing question papers safely. With this motivation, this study develops a Blockchain with Mayfly Optimization-based Chaotic Encryption Model for Smart and Secured Question Sharing (BMFOCE-SSQS) technique. The proposed BMFOCE-SSQS technique aims to accomplish a secure question paper-sharing process. The presented BMFOCE-SSQS technique provides two levels of security using secret sharing and encryption processes. Firstly, the BMFOCE-SSQS technique executes multiple share creation (MSC) schemes, producing twelve different shares of each QP. Next, all the generated shares are tiled up to form an image. For the image encryption process, the MFOCE technique is employed in this study, where the MFO algorithm is used for the optimal key generation process. In addition, BC technology is used for the secure transmission of encrypted QPs. On the receiver side, the reversible process of decryption, unmerging of images, and share reconstruction take place. The experimental outcomes indicated that the BMFOCE-SSQS algorithms significantly improve the secure QP sharing process. A comparative analysis reported the better performance of the BMFOCE-SSQS technique over other existing models.*

Keywords *- Examination system, Education, Blockchain, Security, Question Paper Sharing, Encryption.*

1. Introduction

Blockchain (BC) has brought a revolution in the realm of technology and grabbed the stakeholders' interest in a wide range of industries involving healthcare, digital content distribution, and finance [1]. In BC, once a transaction occurs in the network, it experiences a validation named consensus mechanism, a process where some participant reaches a mutual agreement in allowing that transaction [2].

All the blocks contain the preceding block's hash, accordingly named a BC. In the BC, the study adopted asymmetric cryptography to issue transactions [22]. The Internet of Things (IoT) has brought an additional revolution in the realm of technology [3]. In recent times, IoT has established its mark in the education field. Educational examination and testing include the mass of information distributed for sharing aptitude tests, question papers, answer sheets, and quizzes for new admission. It is an important part of the e-learning system to calculate students' grades [4].

In contrast, malicious students might include fraudulent activity to illegally subvert the study materials involving answer sheets and question papers. A prominent place where illegal credential sharing takes place is online education [5]. With the present learning management system (LMS), students can cheat easily on tests by providing their passwords to others who can take the test on their behalf. Security is relatively important to guarantee reliable data exchange and confidentiality of data from the repository to students [6]. It alleviates fraudulent and cheating activities through the malicious student. Fig. 1 represents the architecture of BC.

Question paper leaking (QPL) causes an unfairness problem during examination [7]. QPL has become a major global challenge from university entrance exams to public examinations, and these situations worsen in developing nations. QPL might result in severe outcomes, like erosion of ethical standards and compromised quality of education [8].

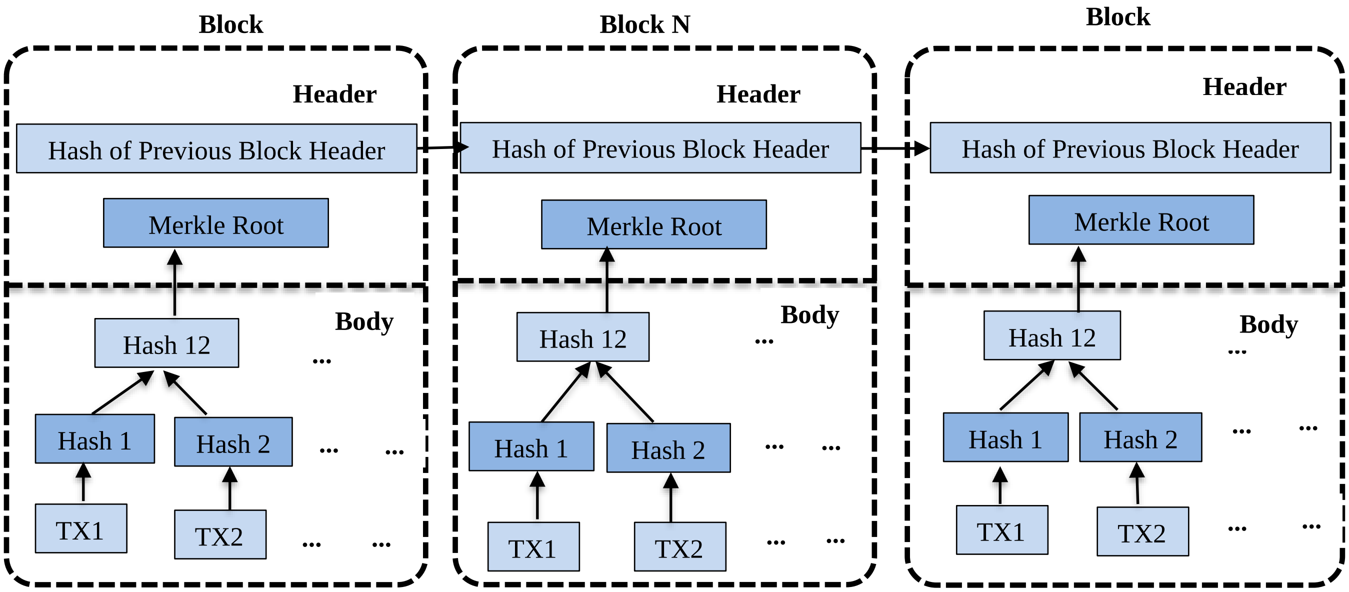


Fig. 1 Structure of Blockchain

In the QPL incident, teachers are involved with the authorities and students. Thus, smart examination systems need to be advanced that could securely share examination papers without considering QPL [9].

Furthermore, phishing, social engineering, and so on could loot any person's credentials to access data at any moment. Hence, the examination management system needs random question selection and more than user credentials [10]. Question sharing (QS) must be implemented using a powerful system where user credential is less significant.

This study develops a Blockchain with Mayfly Optimization-based Chaotic Encryption Model for Smart and Secured Question Sharing (BMFOCE-SSQS) technique. The presented BMFOCE-SSQS technique provides two levels of security using secret sharing and encryption processes. Firstly, the BMFOCE-SSQS technique executes multiple share creation (MSC) schemes, producing twelve different shares of each QP. Next, all the generated shares are tiled up to form an image. The MFOCE technique is employed in this study for the image encryption process, where the MFO algorithm is used for ideal key generation. In addition, BC technology is used for the secure transmission of encrypted QPs. The simulation values exhibited that the BMFOCE-SSQS algorithm significantly improves the secure QP sharing process.

2. Literature Review

Jain et al. [11] presented the Ethereum BC Platform in Education System. The study presents an application for Online-Examination with the help of BC Ethereum Platform using features of Smart Contract, which allow server runtime environments MongoDB and NodeJS database system. The BC-based system is highly secured when compared to other Cloud-based systems. Islam et al. [25] propose a novel system for smart education, based on the conception of BC, for QS. A two-stage encryption system for encrypting question papers (QSP) is developed.

Zhu et al. [13] present a BC-based online exam and biometric authentication schemes. The exam information is encrypted for storing in a distributed system that is attained in case the user fulfils a decryption policy. Also, the piece of evidence is noted down in a BC network that reliable institutions cooperatively develop. Sattar et al. [14] developed a BC architecture that protects the online exam scheme. The presented technique was utilized to secure a data management scheme connected to the present educational information. Institutions could easily compile the information history without needing a copy from the central server. The presented method eliminates any cheating between third-party institutions or users that access services and applications and enhances data security.

Kulkarni and Alfatmi [23] developed the modern treads in an online examination scheme and a novel technique developed for effectively carrying out online exams. This novel method depends on BC techniques, namely the smart contract. This keeps regress monitoring on the examinee, like control panel processes and posture analysis. Aishwarya et al. [16] developed dynamic face authentication based on the Viola-Jones algorithm and SVM to check the candidate's reliability during exams. Afterwards the exam, the system automatically assesses the student, and a valid score report is produced, viz., an E-certificate.

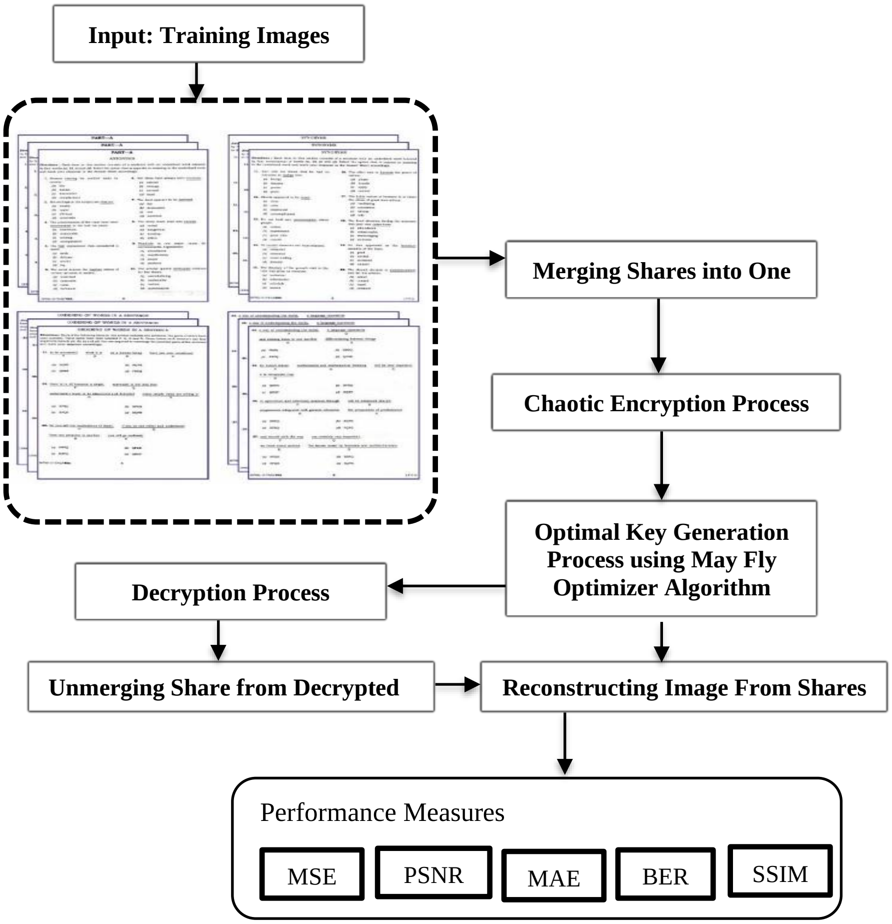

Input: Training Images
Merging Shares into One
Chaotic Encryption Process
Optimal Key Generation Process using May Fly Optimizer Algorithm
Decryption Process
Unmerging Share from Decrypted
Reconstructing Image From Shares
Performance Measures
MSE
PSNR
MAE
BER
SSIM

Fig. 2 Overall working procedure of BMFOCE-SSQS system

Santoso et al. [17] introduced an online exam security scheme in which minimalized system deficiency is utilized to abuse the examination. By adding the filter and executing the algorithm, the scheme enables differentiation between fake and real faces covered by the mask or using a photo image. The presented method stops displaying the question if there is fraud.

3. The Proposed Model

In this study, we have developed a new BMFOCE-SSQS technique for a secure question paper-sharing process. The presented BMFOCE-SSQS technique provides two levels of security using secret sharing and encryption processes. At the initial stage, the BMFOCE-SSQS technique generates a collection of shares using the MSC scheme for each image, and they are merged together to generate an image. Then, the MFO algorithm with chaotic encryption is employed for the image encryption process, and the encrypted image is transmitted via BC technology. On the receiver side, the reversible process of decryption, unmerging of images, and share reconstruction take place. Fig. 2 depicts the working procedure of the BMFOCE-SSQS approach.

3.1. Share Creation Process

The pixel values of original images were filtered, and the RGB value is determined as Rm, Gm, and Bm matrixes, and it can be expressed as follows [24]:

$$Pixel = \sum R + G + B \tag{1}$$

Now, $pixel$ indicates the total quantity of Rm, Gm, and Bm. Each pixel present in the input images might take place using n converted manner named as shares. The R, G, and B share hinge on the state of the advanced pixel values in RGB images.

$$R_s = \int_1^k lim_{k\rightarrow 1ton} R_{ab} \tag{2}$$

$$G_s = \int_1^k lim_{k\rightarrow 1ton} G_{ab} \tag{3}$$

$$IB_s = \int_1^k lim_{k\rightarrow 1ton} B_{ab} \tag{4}$$

In the abovementioned equation, a and b represents the position of the matrix, $R_s, G_s\ and\ B_s$ specifies the share of RGB, $R_{ab}, G_{ab}\ and\ B_{ab}$ signifies the element of the image pixel. The pixel value of RGB can be accomplished using the unique images and taken as a certain matrix. After that, the shares were created based on image partition as different segments.

The SMSC technique focused on encrypting the image into a worthless share image. Prior to producing a share, the subsequent procedure is executed on XR1 and XR2 matrices, and the key matrix K$_{m}$ $_{is}$ made in a random fashion.

$$\begin{gathered} XR_1 = 128 - B_{M1} \\ XR_2 \ = \ B_{M2} \end{gathered} \tag{5}$$

The red band shares will be produced by the XOR operation of essential and elementary matrices, as given below.

$$\begin{gathered} Rs1 \ = \ XR_1 \oplus K_M \\ Rs2 \ = \ XR_2 \oplus XR_1 \\ Rs3 \ = \ XR_2 \oplus Rs_1 \\ Rs4 \ = \ Rs1 \ \oplus R \end{gathered} \tag{6}$$

3.2. Optimal Chaotic Encryption Process

In this study, the encryption of the merged shares is accomplished with the MFOCE approach. In the study, the Chen system in the chaotic state is chosen to make the presented method more robust and secure, and it is mathematically expressed in the following [12,19]:

$$\begin{cases} \dot{x} = 35(y - x) \\ \dot{y} = -7x - xz + 28y \\ \dot{z} = xy - 3z \end{cases} \tag{7}$$

The Chen system could iterate out three chaotic sequences in the chaotic state that are later employed in the design of decryption and encryption methods. The Chen system has a dynamic behavior and complicated topology, which provide wide-ranging application prospects in the field of confidential communication and data encryption. Based on this dynamic feature, the study used the Chen system in the encryption method. The presented method primarily comprises five steps given in the following, which is appropriate for images of any other sizes, recorded as $M \times N$.

Step 1. Read the image into the computer, and symbolize the image matrixes using P. When $M \neq N$, fill the images into a square matrix by means of initial $abs(M - N) \times \min(M, N)$ pixels of the image, in which abs represent the absolute value function and min indicates the minimal function. Lastly, consider $N_s = \max(M, N)$, whereby $\max(\cdot)$ indicates the maximal function.

Step 2. Produce a 128-bit secret key K using SHA-512 from P and split K into four groups that have 32 bits. Next, these four groups are transformed into 4 decimals $[k\_1]$ given below:

$$\begin{cases} k_1 = mod(K(1{:}16)/K(17{:}32), 1) \\ k_2 = mod(K(33{:}48)/K(49{:}64), 1) \\ \mathrm{k}_3 = mod(K(65{:}80)/K(81{:}96), 1) \\ \mathrm{k}_4 = mod(K(97{:}128), 1000) + 1000 \end{cases} \tag{8}$$

Step 3. Attain the $N_S \times N_S$ length chaotic sequence C_1, C_2, and C_3 using the Chen system with the key group $K' = [\mathrm{k}_1, \mathrm{k}_2, \mathrm{k}_3 \mathrm{k}_4]$, wherein $[\mathrm{k}_1, \mathrm{k}_2, \mathrm{k}_3]$ represents the primary variable of the Chen system and k_4 indicates the length of the sequence deleted to guarantee that the system enters the chaotic state.

Step 4. Choose the first matrix A_1, and iteratively produce FSM A_n of proper dimension. Attain the index matrixes S of the location of the sorted backup component in the original matrixes from C_1. Rearrange the pixel of the image matrixes P using the matrix A_n and S. The rearranged matrix is indicated as P'.

Step 5. Diffuse the re-segmented matrixes P' with chaotic sequence C_2 and C_3 using the presented global chaotic pixel diffusion technique. The diffused image matrix is represented as P

From the abovementioned steps, the ciphertext image is attained, while the key sequence comprised of K' and A_1 that are utilized for encrypting and decrypting the image. Because the FSM with iterative and irregular features are employed in the presented technique, the security and time complexity of the method is considerably enhanced. Here, the optimal keys involved in the encryption process are chosen by the MFO algorithm.

The early population can be classified into male and female mayflies (MFs) based on the MFO algorithm that is randomly produced [20]. The early population (candidates) is regarded as d-dimension space $X = [x_1, x_2, \dots x_d]^T$ that is arbitrarily located in the problem. The MFs have a velocity equivalent to $V = [v_1, v_2, \dots v_d]^T$, and the direction related to the individual and social flying experience. Next, the candidate tunes the location closer to the better location (p_{best}), and the better location of the other candidates (g_{best}). By assuming x_i as a current location of the candidate with step equivalent t, the upgraded location can be attained using the subsequent formula:

$$x_i(t+1) = x_i(t) + v_i(t+1), \tag{9}$$

Whereas $x_i(0)$ denoted limited between $x_{\min}$ and $x_{\max}$. The MFs movement on the top of the water to dance can be mathematically modelled in the following:

$$\begin{gathered} v_{ij}(t+1) = v_{ij}(t) + a_1 \times \exp(-\beta r_p^2) \times (pbest_{ij} - x_{ij}^t) \\ + a_2 \times \exp(-\beta r_g^2) \quad (10) \\ \times \left(gbest_j - x_{ij}^t\right), j = 1,2, \dots n \end{gathered}$$

In Eq. (10), β defines the visibility coefficient exploited to restrain MF visibility to others; $pbest_i$ denotes the i^{th} better candidate location had ever visited; r_p and r_g define the Cartesian distance amongst x_i and $pbest_i$ and x_i and

$gbest$; x_{ij}^{t} and $v_{ij}(t)$ embody the location and the velocity of i^{th} candidates in $j\text{-}th$ dimensions, correspondingly; a_1 and a_2 indicate the constant for positive attraction scaling the participation of the social and cognitive components correspondingly. The better location for personally following in the time step $t + 1$ is given below:

$$pbest_i = \begin{cases} x_i(t+1), if\ f(x_i(t+1)) < f(pbest_i) \\ is\ kept\ the\ same, O.W., \end{cases} \quad (11)$$

In Eq. (11), $f(.)$ defines the objective function to describe the solution quality. Next, the global better location $(gbest_j)$ can be accomplished by:

$$gbest = \min\{f(pbest_1), f(pbest_2), \cdots, f(pbest_N)\}, \quad (12)$$

In Eq. (12), N defines the overall amount of male candidates in the swarm. The Norm 2 formula was exploited to define the r_p and r_g in the following:

$$r_p = \sqrt{\sum_{j=1}^{n} (x_{ij} - pbest_i)} \quad (13)$$

$$r_g = \sqrt{\sum_{j=1}^{n} (x_{ij} - gbest)}$$

In Eq. (13), x_{ij} defines the j^{th} components of the $i\text{-}th$ candidate. In order to retain the algorithm with the better candidate, the better MFs keep dancing and upgrade the velocity by the subsequent formula:

$$v_{ij}(t+1) = v_{ij}(t) + n_d \times \delta, \quad (14)$$

In Eq. (14), n_d denotes the nuptial dance co-efficient, and δ defines random number within [−1, 1]. But, every male MF belongs to a special swarm; the female does not belong to that group. They fly around the male for breeding. By considering $y_i(t)$ as the i^{th} female candidate path, in the solution space, the location was upgraded as follows:

$$y_i(t+1) = y_i(t) + v_i(t+1). \quad (15)$$

The better male breed with the better female, the second-better male with the second-better female, and so on. Thus, the velocity was taken into account in the following:

$$v_{ij}(t+1) = \begin{cases} v_{ij}(t) + a_2 \times \exp\left(-\beta r_{mf}^2\right) \times \left(x_{ij}^t - y_{ij}^t\right), if\ f(y_i) > f(x_i), \\ v_{ij}^t(t) + r_w \times r, f(y_i) \leq f(x_i), \end{cases} \quad (16)$$

In Eq. (16), β describes a fixed visibility coefficient, a_2 represents a positive attraction constant, r_{mf} defines the Cartesian distance between male and female candidates, y_{ij}^t and $v_{ij}^t(t)$ denotes the i^{th} female candidate location and velocity in $j\text{-}th$ dimensions at time step t, and r_w describes a random walk coefficient, and r indicates a random number within [−1, 1]. The MFO approach uses crossover as the mating approach among the male and female candidates so that two candidates are initially chosen as male and female. The way of choosing the parent is the same as the technique of female attraction to a male. The novel generation of the crossover technique was accomplished by the subsequent formula:

$$offspring_1 = \zeta \times male + (1-\gamma) \times female, \quad (17)$$

$$offspring_2 = \zeta \times \text{female} + (1-\gamma) \times \text{male},$$

Here, in the MFO approach, the ideal key set is chosen by regarding 'fitness function' as max key with PSNR for unscrambling and scrambling the dataset from the image.

$$Fitness = MAX\{PSNR\} \quad (18)$$

3.3. BC Technology

Once the encryption of merged shares is completed, they are transmitted to the receiver via BC technology. BC is a transactional dataset technique and is a decentralized method for managing validation, and the tamper-resistant transaction includes consistency through a considerable amount of participants, termed nodes [21]. BC is categorized into a kind of distributed ledger that gives users confidence that stored data, namely certificates, is not tampered with. Different research demonstrated that BC could reduce dubiousness, transactional obscurity, and unconfident states by providing comprehensive disclosure of transactions and supplementing homogenous and verified facts across each participant from the network. Furthermore, the BC technique is estimated to greatly renovate the economy and social order via decreased transaction costs and the necessity for trustworthy and well-known third parties. Furthermore, a study shows that these technologies are deployed for concluding binding agreements, recording transactional details, validating payments with the use of a supply chain, storing medical records, tracking the attribution of artworks, storing individual records of credit, keeping a record of good movement, etc.

3.4. Decryption and Reconstruction Process

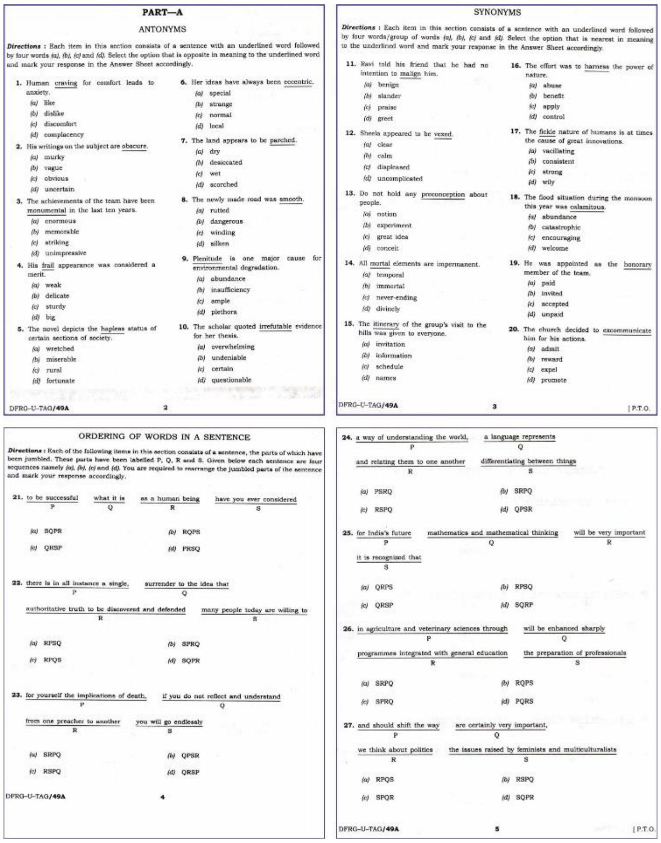
The presented BMFOCE-SSQS technique follows a symmetric process, i.e. images can be constructed in a reversible order. At the receiving end, the encrypted QP image is received, which is initially decrypted using a chaotic encryption technique. Next, the decrypted QP image is unmerged to form a collection of 12 original shares. Finally, the shares are reconstructed and formed the input QP image using Eq. (19):

$$R = Rs1 \oplus Rs2 \oplus Rs3 \oplus Rs4 \oplus Rs4 \oplus K_M$$
$$G = Gs1 \oplus Gs2 \oplus Gs3 \oplus Gs4 \oplus Gs4 \oplus K_M \qquad (19)$$
$$B = Bs1 \oplus Bs2 \oplus Bs3 \oplus Bs4 \oplus Bs4 \oplus K_M$$

Through this process, the QPs get shared in a secure and effective way.

4. Results and Discussion

The presented BMFOCE-SSQS approach was simulated utilizing a Python tool. The results are examined on a set of ten QPs collected on our own. The results are examined under different measures on the applied ten test images. Fig. 3 demonstrates some sample images.



PART—A

ANTONYMS

Directions : Each item in this section consists of a sentence with an underlined word followed by four words *(a)*, *(b)*, *(c)* and *(d)*. Select the option that is opposite in meaning to the underlined word and mark your response in the Answer Sheet accordingly.

1. Human craving for comfort leads to anxiety.
   (a) like
   (b) dislike
   (c) discomfort
   (d) complacency

2. His writings on the subject are obscure.
   (a) murky
   (b) vague
   (c) obvious
   (d) uncertain

3. The achievements of the team have been monumental in the last ten years.
   (a) enormous
   (b) memorable
   (c) striking
   (d) unimpressive

4. His frail appearance was considered a merit.
   (a) weak
   (b) delicate
   (c) sturdy
   (d) big

5. The novel depicts the hapless status of certain sections of society.
   (a) wretched
   (b) miserable
   (c) rural
   (d) fortunate

6. Her ideas have always been eccentric.
   (a) special
   (b) strange
   (c) normal
   (d) local

7. The land appears to be parched.
   (a) dry
   (b) desiccated
   (c) wet
   (d) scorched

8. The newly made road was smooth.
   (a) rutted
   (b) dangerous
   (c) winding
   (d) silken

9. Plenitude is one major cause for environmental degradation.
   (a) abundance
   (b) insufficiency
   (c) ample
   (d) plethora

10. The scholar quoted irrefutable evidence for her thesis.
   (a) overwhelming
   (b) undeniable
   (c) certain
   (d) questionable

DFRG-U-TAG/**49A** 2

SYNONYMS

Directions : Each item in this section consists of a sentence with an underlined word followed by four words/group of words *(a)*, *(b)*, *(c)* and *(d)*. Select the option that is nearest in meaning to the underlined word and mark your response in the Answer Sheet accordingly.

11. Ravi told his friend that he had no intention to malign him.
   (a) benign
   (b) slander
   (c) praise
   (d) greet

12. Sheela appeared to be vexed.
   (a) clear
   (b) calm
   (c) displeased
   (d) uncomplicated

13. Do not hold any preconception about people.
   (a) notion
   (b) experiment
   (c) great idea
   (d) conceit

14. All mortal elements are impermanent.
   (a) temporal
   (b) immortal
   (c) never-ending
   (d) divinely

15. The itinerary of the group's visit to the hills was given to everyone.
   (a) invitation
   (b) information
   (c) schedule
   (d) names

16. The effort was to harness the power of nature.
   (a) abuse
   (b) benefit
   (c) apply
   (d) control

17. The fickle nature of humans is at times the cause of great innovations.
   (a) vacillating
   (b) consistent
   (c) strong
   (d) wily

18. The flood situation during the monsoon this year was calamitous.
   (a) abundance
   (b) catastrophic
   (c) encouraging
   (d) welcome

19. He was appointed as the honorary member of the team.
   (a) paid
   (b) invited
   (c) accepted
   (d) unpaid

20. The church decided to excommunicate him for his actions.
   (a) admit
   (b) reward
   (c) expel
   (d) promote

DFRG-U-TAG/**49A** 3 | P.T.O.

ORDERING OF WORDS IN A SENTENCE

Directions : Each of the following items in this section consists of a sentence, the parts of which have been jumbled. These parts have been labelled P, Q, R and S. Given below each sentence are four sequences namely *(a)*, *(b)*, *(c)* and *(d)*. You are required to rearrange the jumbled parts of the sentence and mark your response accordingly.

21. to be successful (P) what it is (Q) as a human being (R) have you ever considered (S)
   (a) SQPR *(b)* RQPS
   (c) QRSP *(d)* PRSQ

22. there is in all instance a single, (P) surrender to the idea that (Q)
   authoritative truth to be discovered and defended (R) many people today are willing to (S)
   (a) RPSQ *(b)* SPRQ
   (c) RPQS *(d)* SQPR

23. for yourself the implications of death, (P) if you do not reflect and understand (Q)
   from one preacher to another (R) you will go endlessly (S)
   (a) SRPQ *(b)* QPSR
   (c) RSPQ *(d)* QRSP

DFRG-U-TAG/**49A** 4

24. a way of understanding the world, (P) a language represents (Q)
   and relating them to one another (R) differentiating between things (S)
   (a) PSRQ *(b)* SRPQ
   (c) RSPQ *(d)* QPSR

25. for India's future (P) mathematics and mathematical thinking (Q) will be very important (R)
   it is recognized that (S)
   (a) QRPS *(b)* RPSQ
   (c) QRSP *(d)* SQRP

26. in agriculture and veterinary sciences through (P) will be enhanced sharply (Q)
   programmes integrated with general education (R) the preparation of professionals (S)
   (a) SRPQ *(b)* RQPS
   (c) SPRQ *(d)* PQRS

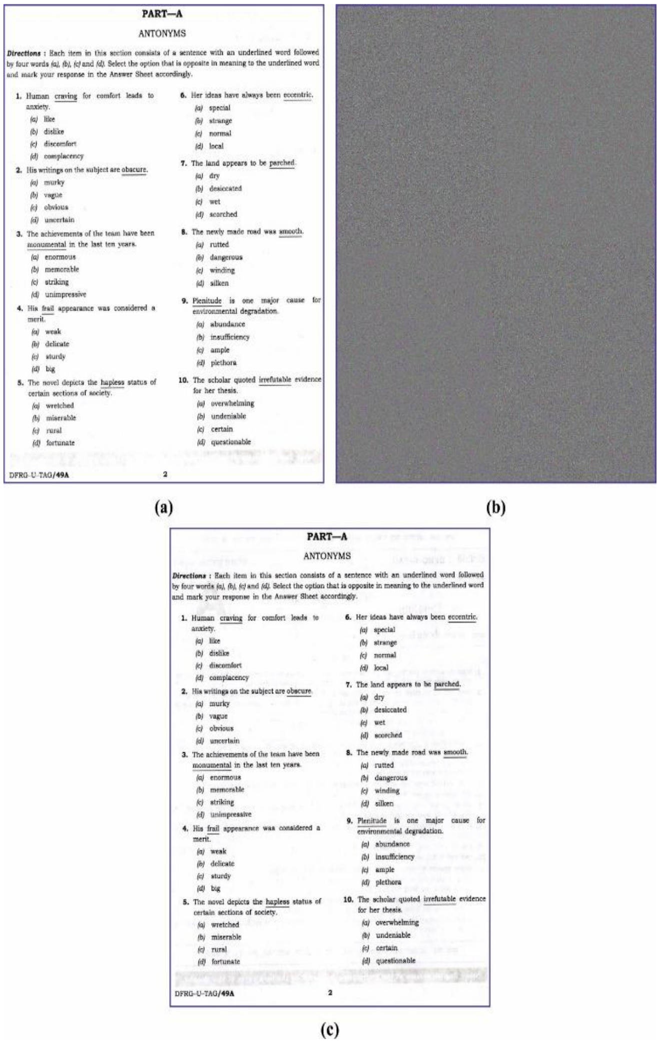
27. and should shift the way (P) are certainly very important, (Q)
   we think about politics (R) the issues raised by feminists and multiculturalists (S)
   (a) RPQS *(b)* RSPQ
   (c) SPQR *(d)* SQPR

DFRG-U-TAG/**49A** 5 | P.T.O.

Fig. 3 Sample Images

Fig. 4 visualizes the sample outcomes of the BMFOCE-SSQS approach on the secure QP sharing process. Fig. 4a shows the original QP image, which needs to be shared. Next, Fig. 4b indicates the encrypted version of the QP using the MFOCE technique. Finally, the reconstructed form of QP is depicted in Fig. 4c. From these figures; it is affirmed that the BMFOCE-SSQS model has securely shared the QPs and reconstructed without any loss.

Fig. 5 provides an overall result analysis of the BMFOCE-SSQS model. The experimental values implied that the BMFOCE-SSQS model had reached improved results under all measures. Based on MSE, the BMFOCE-SSQS model has attained a minimal MSE of 0.96. At the same time, it is observed that the BMFOCE-SSQS model has gained a maximum PSNR of 48.52dB. Likewise, the BMFOCE-SSQS model has reached a lower MAE of 36.22. Finally, the BMFOCE-SSQS model has accomplished the least BER of 0.37.



PART—A

ANTONYMS

Directions : Each item in this section consists of a sentence with an underlined word followed by four words *(a)*, *(b)*, *(c)* and *(d)*. Select the option that is opposite in meaning to the underlined word and mark your response in the Answer Sheet accordingly.

1. Human craving for comfort leads to anxiety. *(a)* like *(b)* dislike *(c)* discomfort *(d)* complacency
2. His writings on the subject are obscure. *(a)* murky *(b)* vague *(c)* obvious *(d)* uncertain
3. The achievements of the team have been monumental in the last ten years. *(a)* enormous *(b)* memorable *(c)* striking *(d)* unimpressive
4. His frail appearance was considered a merit. *(a)* weak *(b)* delicate *(c)* sturdy *(d)* big
5. The novel depicts the hapless status of certain sections of society. *(a)* wretched *(b)* miserable *(c)* rural *(d)* fortunate
6. Her ideas have always been eccentric. *(a)* special *(b)* strange *(c)* normal *(d)* local
7. The land appears to be parched. *(a)* dry *(b)* desiccated *(c)* wet *(d)* scorched
8. The newly made road was smooth. *(a)* rutted *(b)* dangerous *(c)* winding *(d)* silken
9. Plenitude is one major cause for environmental degradation. *(a)* abundance *(b)* insufficiency *(c)* ample *(d)* plethora
10. The scholar quoted irrefutable evidence for her thesis. *(a)* overwhelming *(b)* undeniable *(c)* certain *(d)* questionable

DFRG-U-TAG/**49A** 2

Fig. 4 a) Original Image b) Encrypted Image c) Reconstructed Image

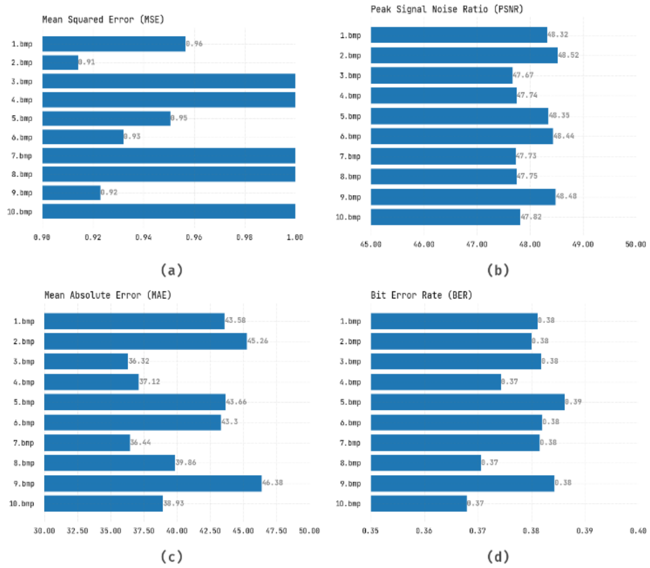


Fig. 5 Result analysis of BMFOCE-SSQS model a) MSE b) PSNR c) MAE d) BER

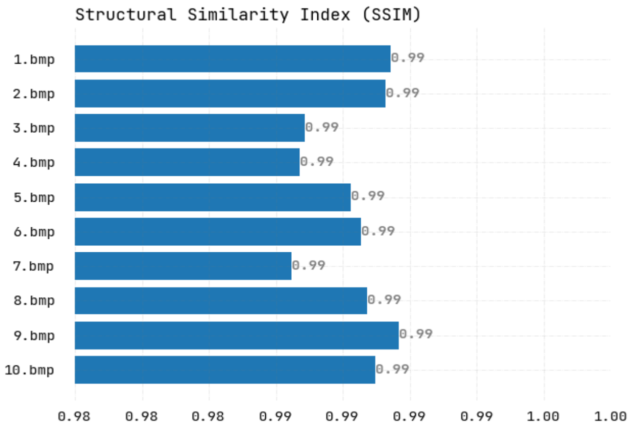


Fig. 6 SSIM analysis of BMFOCE-SSQS system with distinct images

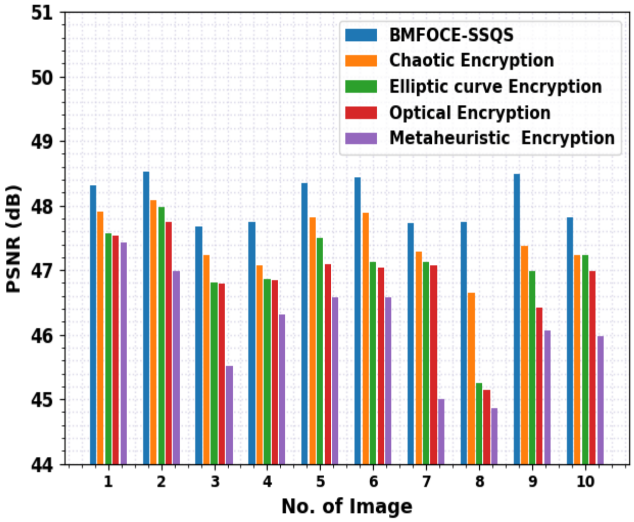


Fig. 7 PSNR analysis of BMFOCE-SSQS system with recent approaches

A brief SSIM examination of the BMFOCE-SSQS model is shown in Fig. 6. The results indicated that the BMFOCE-SSQS model had achieved enhanced performance with maximum SSIM values. It is noticed that the BMFOCE-SSQS model has gained at least 0.99 SSIM values under all images.

The experimental results of the BMFOCE-SSQS model are compared with recent models in terms of PSNR in Table 1 and Fig. 7. The outcomes pointed out that the BMFOCE-SSQS approach has assured higher PSNR values under all images. For sample, in image 1, the BMFOCE-SSQS system has achieved a maximal PSNR of 48.32dB, whereas the CE, ECC, OC, and ME algorithms have resulted in decreased PSNR of 47.9dB, 47.57dB, 47.54dB, and 47.42dB respectively.

Table 1. PSNR analysis of BMFOCE-SSQS system with recent approaches

PSNR (dB)					
No. of Image	**BMFOCE-SSQS**	**Chaotic Encryption**	**Elliptic curve Encryption**	**Optical Encryption**	**Metaheuristic Encryption**
1.bmp	48.32	47.9	47.57	47.54	47.42
2.bmp	48.52	48.09	47.97	47.74	46.98
3.bmp	47.67	47.24	46.81	46.79	45.52
4.bmp	47.74	47.07	46.86	46.85	46.32
5.bmp	48.35	47.82	47.5	47.09	46.57
6.bmp	48.44	47.89	47.12	47.03	46.57
7.bmp	47.73	47.29	47.12	47.08	45.01
8.bmp	47.75	46.65	45.25	45.15	44.87
9.bmp	48.48	47.38	46.99	46.42	46.06
10.bmp	47.82	47.24	47.24	46.99	45.97

Also, in image 3, the BMFOCE-SSQS approach has gained a higher PSNR of 47.67dB, whereas the CE, ECC, OC, and ME techniques have resulted in lower PSNR of 47.24dB, 46.81dB, 46.79dB, and 45.52dB correspondingly. Moreover, in image 6, the BMFOCE-SSQS system has obtained an improved PSNR of 48.44dB, whereas the CE, ECC, OC, and ME algorithms have resulted in lesser PSNR of 47.89dB, 47.12dB, 47.03dB, and 46.57dB correspondingly.

Furthermore, in image 10, the BMFOCE-SSQS approach has accomplished an increased PSNR of 47.82dB, whereas the CE, ECC, OC, and ME methodologies have resulted in reduced PSNR of 47.24dB, 47.24dB, 46.99dB, and 45.97dB correspondingly. These results and discussion highlighted the improved security outcomes of the BMFOCE-SSQS model.

5. Conclusion

This study established a novel BMFOCE-SSQS technique for a secure question paper-sharing process. The presented BMFOCE-SSQS technique provides two levels of security using secret sharing and encryption processes. At the initial stage, the BMFOCE-SSQS technique generates a collection of shares using the MSC scheme for each image, and they are merged together to generate an image. Then, the MFO algorithm with chaotic encryption is employed for the image encryption process, and the encrypted image is transmitted via BC technology. On the receiver side, the reversible process of decryption, unmerging of images, and share reconstruction take place. The simulation outcomes stated that the BMFOCE-SSQS method significantly improves the secure QP sharing process. A comparative analysis reported the better performance of the BMFOCE-SSQS technique over other existing models.

References

[1] Thilagavathi, M, “Blockchain-Based Framework for Online Entrance Examination and Score Card Verification System,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT*), vol. 12, no. 1S, pp. 388-398, 2021. *Crossref*, https://doi.org/10.17762/turcomat.v12i1S.1868

[2] Banupriya Sadayapillai, and Kottilingam Kottursamy., “A Blockchain-Based Framework for Transparent, Secure, and Verifiable Online Examination System,” *Journal of Uncertain Systems*, vol. 15, no. 3, 2022. *Crossref*, https://doi.org/10.1142/S1752890922410021

[3] Ashis Kumar Samanta, Bidyut Biman Sarkar, and Nabendu Chaki, “A Blockchain-Based Smart Contract towards Developing Secured University Examination System,” *Journal of Data, Information and Management*, vol. 3, no. 4, pp. 237-249, 2021. *Crossref*, https://doi.org/10.1007/s42488-021-00056-0

[4] Shixian Song, “Construction of University Online Examination System Based on Cloud Computing Technology,” *Scientific Programming*, vol. 2021. *Crossref*, https://doi.org/10.1155/2021/7849255

[5] Tsai et al., “Design and Development of a Blockchain-Based Secure Scoring Mechanism for Online Learning,” *Educational Technology & Society*, vol. 25, no. 3, pp. 105-121.

[6] Shoaib Farooq et al., “Blockchain Based Online Examination Assessment Models for Educational Institutes, A Systematic Literature Review,” *VFAST Transactions on Software Engineering*, vol. 9, no. 3, pp. 57-67, 2021. *Crossref*, http://dx.doi.org/10.21015/vtse.v9i3.707

[7] Qurotul Aini et al., “Digitalization Online Exam Cards in the Era of Disruption 5.0 Using the Devops Method,” *Journal of Educational Science and Technology (EST),* vol. 7, no. 1, pp.67-75, 2021. *Crossref*, http://dx.doi.org/10.26858/est.v7i1.18837

[8] Shuangquan Li et al., “Health Checkup Could Reveal Chronic Disorders with Support from Artificial Intelligence,” *International Journal of Engineering Trends and Technology*, vol. 67, no. 11, pp. 8-15, 2019. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V67I11P202

[9] Dilmurod Nabiev, and Khayit Turaev, "Study of Synthesis and Pigment Characteristics of the Composition of Copper Phthalocyanine with Terephthalic Acid," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 1-9, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I8P201

[10] Shwetambari Borade et al., "Deep Scattering Convolutional Network for Cosmetic Skin Classification," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 10-23, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I7P202

[11] Apoorv Jain et al., “Smart Contract Enabled Online Examination System Based in Blockchain Network,” *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1-7, 2021. *Crossref*, https://doi.org/10.1109/ICCCI50826.2021.9402420

[12] Jyoti Kansari, Avinash Dhole, and Yogesh Rathore, "A Survey on Block Cipher and Chaotic Based Encryption Techniques," *International Journal of Computer Trends and Technology*, vol. 69, no. 3, pp. 52-59, 2021. *Crossref*, https://doi.org/10.14445/22312803/IJCTT-V69I3P110

[13] Xiaoling Zhu, and Chenglong Cao, “Secure Online Examination with Biometric Authentication and Blockchain-Based Framework,” *Mathematical Problems in Engineering*, vol. 2021, pp. 1-12, 2021. *Crossref*, https://doi.org/10.1155/2021/5058780

[14] Md Rahat Ibne Sattar et al., “An Advanced and Secure Framework for Conducting Online Examination Using Blockchain Method,” *Cyber Security and Applications*, vol. 1, p.100005, 2023. *Crossref*, https://doi.org/10.1016/j.csa.2022.100005

[15] S. Sivasubramaniam, and S. P. Balamurugan, "Nature Inspired Optimization with Hybrid Machine Learning Model for Cardiovascular Disease Detection and Classification," *International Journal of Engineering Trends and Technology*, vol. 70, no. 12, pp. 127-137, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I12P214

[16] S. Aishwarya et al., “Detection of Impersonation in Online Examinations Using Blockchain,” *2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS*), *IEEE*, pp. 1-5, 2020. *Crossref*, https://doi.org/10.1109/ICPECTS49113.2020.9337001

[17] Handri Santoso et al., “Development of an Online Exam Security System Using Ensemble Method,” *2021 4th International Conference of Computer and Informatics Engineering (IC2IE)*, IEEE. pp. 272-276,

[18] Zebanaaz, Kauser Fatima, and C.Atheeq, "Performance Based Comparison Study of RSA and Chaotic Maps in MANET," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 4, no. 2, pp. 17-22, 2017. *Crossref*, https://doi.org/10.14445/23488379/IJEEE-V4I2P104

[19] Yongjin Xian, and Xingyuan Wang, “Fractal Sorting Matrix and Its Application on Chaotic Image Encryption,” *Information Sciences*, vol. 547, pp. 1154-1169, 2021. *Crossref*, https://doi.org/10.1016/j.ins.2020.09.055

[20] Konstantinos Zervoudakis, and Stelios Tsafarakis, “A Mayfly Optimization Algorithm,” *Computers & Industrial Engineering*, vol. 145, p.106559, 2020. *Crossref*, https://doi.org/10.1016/j.cie.2020.106559

[21] Beck, R., Müller-Bloch, C. and King, J.L, “Governance in the Blockchain Economy: A Framework and Research Agenda,” *Journal of the Association for Information Systems*, vol. 19, no. 10, p. 1, 2018.

[22] S.Jagadeesan et al., "High Level Secure Messages Based on Steganography and Cryptography," *International Journal of Engineering Trends and Technolog*y, vol. 68, no. 2, pp. 142-145, 2020. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V68I2P220S

[23] Mayuri Diwakar Kulkarni, and Khalid Alfatmi, “New Approach for Online Examination Conduction System Using Smart Contract,” *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 848-852, 2021. *Crossref*, https://doi.org/10.1109/CSNT51715.2021.9509683

[24] Duraisamy, M., and Balamurugan, S.P, “Multiple Share Creation Scheme with Optimal Key Generation for Secure Medical Image Transmission in the Internet of Things Environment,” *International Journal of Electronic Healthcare*, vol. 11, no. 4, pp. 307-330, 2021. *Crossref*, bhttps://doi.org/10.1504/IJEH.2021.117827

[25] Islam, Anik et al., “BSSSQS: A Blockchain Based Smart and Secured Scheme for Question Sharing in the Smart Education System,” *Journal of Information and Communication Convergence Engineering*, vol. 17, no. 3, pp. 174-184, 2019. *Crossref*, https://doi.org/10.6109/jicce.2019.17.3.174