SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I4P113

Volume 10 Issue 4, 131-140, April 2023
© 2023 Seventh Sense Research Group®

Original Article

Artificial Bee Colony Optimization with Hybrid Image Encryption with Random Key Driven Share Creation Scheme for Blockchain-Assisted 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: 04 March 2023 Revised: 31 March 2023 Accepted: 18 April 2023 Published: 30 April 2023

Abstract *- Educational tests and examinations cover massive data sharing to distribute question papers, aptitude tests, answer sheets, and quizzes for new admissions. Question Paper Leaking (QPL) can cause an unreasonable issue during exams. Today, QPL was a severe problem worldwide, from university entrance exams to public exams, and the situation is getting worse in emerging countries. QPL can cause specific rigorous results such as erosion of ethical standards and the education quality being compromised. There is a need for the security of e-learning mechanisms through cryptographic techniques. Blockchain (BC) fulfilled educational valuations and personalized curricula with smart contracts over a public permission BC. It exhibits the potential of this developing technology to enhance various core learning experiences, such as learner privacy, assessments, and curriculum personalization. This study presents an Artificial Bee Colony Optimization with Hybrid Image Encryption with Random Key Driven Share Creation Scheme for Blockchain Assisted Question Paper Sharing (ABCHIE-RKDSC) technique. In the presented ABCHIE-RKDSC model, three main procedures are involved, called share creation, share encryption, and BC-enabled transmission. During the process of share creation, a set of four shares is created for every input image and the random key generation method is performed by a user input equation instead of a conventional random seed function. Next, the generated shares undergo encryption by hybrid Advanced Encryption Standard with the Elliptic Curve Cryptography (AES-ECC) method. Moreover, the key generation process of the AES-ECC method is performed by the use of the ABC algorithm. The proposed ABCHIE-RKDSC technique involves BC technology that enables secure transmission of encrypted QPs. Finally, the share reconstruction and image decryption process take place to retrieve the original QPs. The experimental validation of the ABCHIE-RKDSC algorithm is investigated, and the outputs are evaluated under varied measures. A comprehensive result investigation highlighted the advancement of the ABCHIE-RKDSC method over other methods.*

Keywords *– Blockchain, Question paper leakage, Image encryption, Optimal key generation, Share creation.*

1. Introduction

In an intelligent education system, papers and other documents can be securely shared in several ways [1]. One method uses an education-specific platform or learning management system (LMS) that involves collaboration features and secure file sharing [2]. Several LMS platforms let teachers share and upload documents with their students and set authorizations for those who can download, view, or edit the files. Such platforms commonly include security measures like access controls and encryption to protect the integrity and privacy of shared files. Another option was to use a decentralized file-sharing platform constructed on top of a blockchain (BC) [3]. Such platforms permit users to share and upload files in a decentralized and secure manner, ensuring that the files are saved in a distributed way and cannot be deleted or modified without the original author's permission [5]. At last, end-to-end encryption can be utilized when sharing files through other messaging platforms or email to safeguard that the documents are accessible to the intended recipients [6].

Image encryption refers to a method that can be utilized to secure the sharing of other documents or papers in a smart education mechanism. With image encryption, the document can be transformed into an image file, and the image file can be encoded through an encryption system [8]. The encoded image can be shared with intended recipients, who can decode the image through the proper decryption key [9]. There were many advantages to using image encryption for document sharing in smart education mechanisms. One benefit is that it can make it more problematic for unauthorized persons to access the file [10], as the file is encoded and can only be decoded by those who have the decryption key. Another benefit is that it can make it very hard for the file to be altered or modified, as any changes in the file lead to a different encoded image [11, 12]. Several software programs and tools can be utilized for decoding and encoding image files [13, 14]. A few instances are AxCrypt, GPG, and VeraCrypt. It is significant to opt for a reliable and secure tool for assuring the integrity and confidentiality of shared documents [16].

Numerous methods can be utilized for sharing papers or files through BC technology. One approach is to use a decentralized document-sharing platform that can be built on top of a BC. Such platforms permit users to share and upload files, and the files are saved in a decentralized manner on the BC [17]. This guarantees that the files are secure and cannot be deleted or modified without the original author's permission. Another method was to use a BC-related document certification system, which permits users to certify the file's authenticity by adding a hash of the file to the BC [18]. This can be valuable for verifying the authenticity of research papers or other significant files.

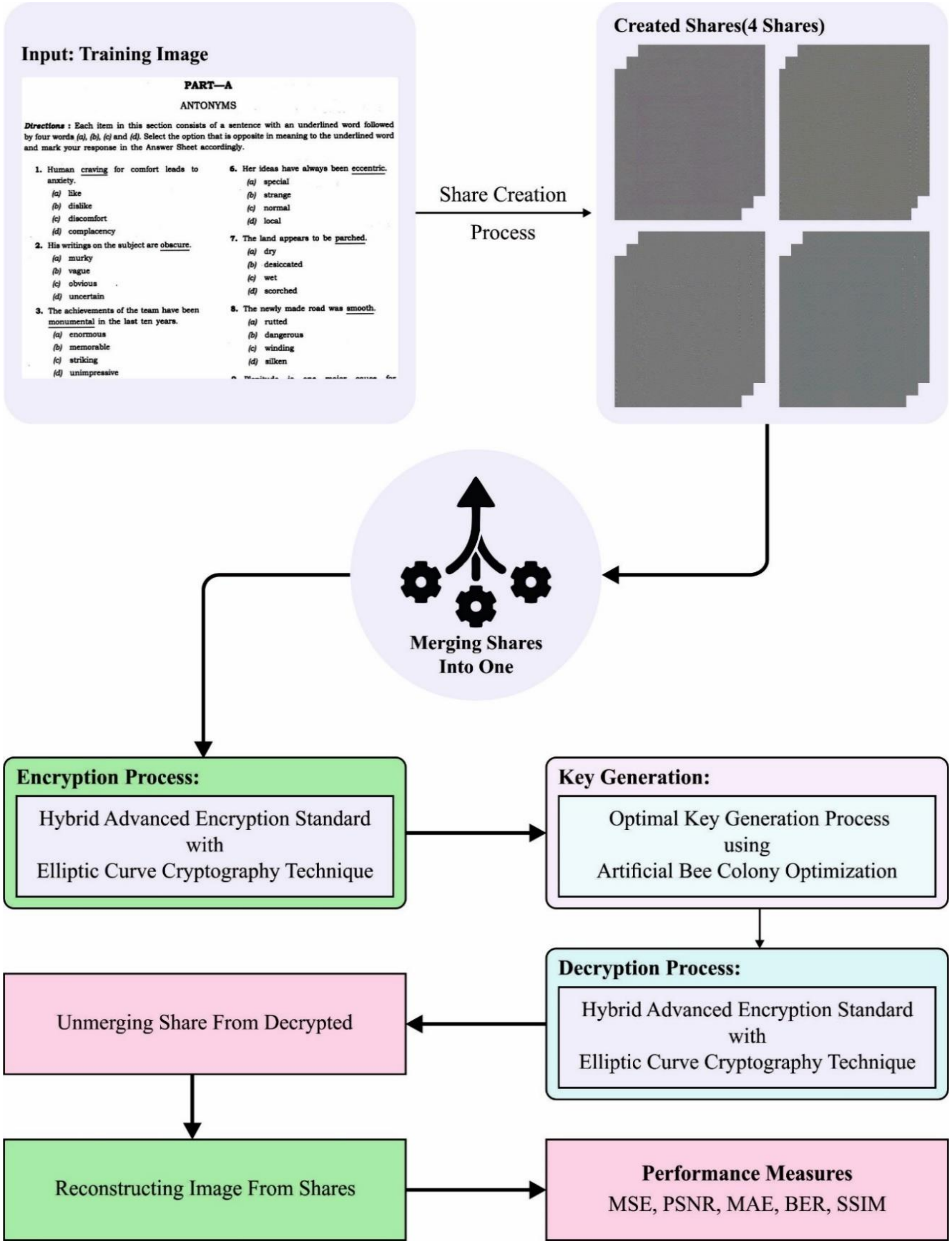
This study presents an Artificial Bee Colony Optimization with Hybrid Image Encryption with Random Key Driven Share Creation Scheme for Blockchain Assisted Question Paper Sharing (ABCHIE-RKDSC) technique. During the process of share creation, a set of four shares is created for every input image and the random key generation process is performed by a user input equation instead of a conventional random seed function. Next, the generated shares undergo encryption by an Advanced Encryption Standard with the Elliptic Curve Cryptography (AES-ECC) algorithm. Moreover, the key generation method of the AES-ECC method is performed by the use of the ABC algorithm. The proposed ABCHIE-RKDSC technique involves BC technology that enables secure transmission of encrypted QPs. Finally, the share reconstruction and image decryption process take place to retrieve the original QPs. The experimental validation of the ABCHIE-RKDSC algorithm is investigated, and the outputs are evaluated under varied measures.

2. Related Works

In [19], a Blockchain (BC)-related homework grading system was introduced using multiple Cryptographic techniques for establishing a fair and transparent platform for teacher–student communications. The novelty of this study is to confirm the transparency and fairness of mutual communication among teachers and students to provide assurance that every student should be equally treated while grading. Significantly, post-grade cheating events are obstructed by recording grading activities and outcomes on the chain. The author realized the presented method relies upon Ethereum source code to demonstrate the applicability. In [20], a naive BC and watermarking-associated social media structure can be modelled for controlling fake news propagation. The author postulated a novel BC method for mitigating existing difficulties in this domain. Furthermore, the new solution assists in minimalizing the spreading of false information by tracing the origin or root of the incorrect information on social networking platforms.

In [22], the authors developed an effective Lightweight integrated Blockchain (ELIB) to meet IoT requirements. This method was arranged in smart home settings as a significant illustration for verifying its pertinency in several IoT scenarios. The ELIB method generated overlay networks where heavily equipped sources can merge to the public BC, which verified dedicated privacy and security. Tarawneh et al. [23] presented a key management technique for securing exam storage utilizing a public key Cryptosystem; it leverages an RSA system to offer distinct data authentication, integrity, and privacy features. It is leveraged in centralized cloud-based or server-related systems. The presented structure offers security without a surge in decoding and encoding hours without raising the file size.

In [24], the author studied BC and Secret Sharing to address personal data security problems in exterior cloud servicing and enriching information security and integrity by devising a dispersed mechanism. CSPs were linked in a BC to authenticate the integrity of user information and offer more accessible access to data via transmission [25]. CSP utilizes the BC for storing dispersed users' data securely using the Secret-Sharing technique as a dispersed method with the enhanced safety of the present centralized mechanism. In [26, 28], the author aims to solve the central issue of correct image attribution for uploading images on P2P image-sharing marketplaces and stock photo sites, ensuring that original photographers were detected and accredited. To overcome such issues, the author proposed a decentralized P2P photo-sharing marketplace framed over the Ethereum test chain and demonstrated how it is reasonable, practical and trustworthy [29]. The decentralized applications use a strong, smart contract and perceptual hashes of Ethereum to mechanically reject and identify tampered imageries parallel to an image presented on the marketplace [30, 31].


Input: Training Image
Share Creation Process
Created Shares(4 Shares)
Merging Shares Into One
Encryption Process:
Hybrid Advanced Encryption Standard with Elliptic Curve Cryptography Technique
Key Generation:
Optimal Key Generation Process using Artificial Bee Colony Optimization
Decryption Process:
Hybrid Advanced Encryption Standard with Elliptic Curve Cryptography Technique
Unmerging Share From Decrypted
Reconstructing Image From Shares
Performance Measures
MSE, PSNR, MAE, BER, SSIM

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

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

Fig. 1 Overall workflow of ABCHIE-RKDSC system

3. The Proposed Model

In this research, we have presented a novel ABCHIE-RKDSC approach for safe QP sharing in the educational sector. In the presented ABCHIE-RKDSC approach, three key procedures are utilized, namely share creation, share encryption, and BC-enabled transmission. Fig. 1 represents the comprehensive workflow of the ABCHIE-RKDSC technique.

3.1. Optimal Share Creation with User Input

Primarily, the proposed model generates a set of four shares using a share creation scheme. The pixel value of the imaging was determined, and the RGB values were defined by R_m, B_m, and G_m matrices [20]. The matrix dimension corresponds to the dimension of the PxQ input images as:

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

Where $pixel$ shows the R_m, B_m, and G_m pixel values, the given pixel in the input image undergoes n transformed manner named a share. The RGB sharing can be represented as R_s, $G_{s,}$ and B_s. The RGB share is based on the pixel value existing in RGB imaging.

$$\begin{gathered} R_s = \int_1^k lim_{k\rightarrow 1ton} R_{ab} \\ G_s = \int_1^k lim_{k\rightarrow 1ton} G_{ab} \\ B_s = \int_1^k lim_{k\rightarrow 1ton} B_{ab} \end{gathered} \tag{2}$$

Where a & b demonstrate the matrix location, R_s, Gs, andB_s present the RGB share, $and\ R_{ab}$, $G_{ab}\ and\ B_{ab}$ show the component of image pixels. Beforehand sharing data, the fundamental matrices must be derived according to the number of shares to be produced. The basic matrix amount is set to 2, and the share amount is set to 4. Afterwards, the fundamental matrix can be attained using the above-mentioned method and is represented as B_{M1} and B_{M2}. The consequent process is accomplished on the matrices XR_1 and XR_2 beforehand, making a share.

$$XR_1 = 128 - B_{M1} \tag{3}$$

$$XR_2 = B_{M2} \tag{4}$$

The red band share is produced by XOR operations amongst the key and elementary matrix as follows.

$$\begin{gathered} Rs1 = XR_1 \oplus K_M \\ Rs2 = XR_2 \oplus XR_1 \\ Rs3 = XR_2 \oplus Rs_1 \\ Rs4 = Rs1 \oplus R \end{gathered} \tag{5}$$

In the reconstruction method, more than one share is integrated to make the original image that is provided in the following:

$$\begin{gathered} R = Rs_1 \oplus Rs_2 \oplus Rs_3 \oplus Rs_4 \oplus Rs_4 \oplus K_M \\ G = Gs_1 \oplus Gs_2 \oplus Gs_3 \oplus Gs_4 \oplus Gs_4 \oplus K_M \\ B = Bs_1 \oplus Bs_2 \oplus Bs_3 \oplus Bs_4 \oplus Bs_4 \oplus K_M \end{gathered} \tag{6}$$

As soon as the shares are recreated, the decryption and encryption techniques with the ECC algorithm occur on all the colour bands. The band images are divided into blocks beforehand decryption and encryption. Such blocks are divided into the dimension of 4x4.

Instead, the user input equation is used to create the keys, and the random value is generated. For instance, the user equation of (x+y+z) with x=2, y=3, z=1 values, i.e. a total of 6, is fed as input for the random seed function. The seed() technique takes place for initializing the randomly generated number, and it needs a number to initiate with (a seed value), to produce a random number. The randomly generated number employs the present system time by default. The seed() technique is used for customizing the initial number of the randomly generated number. The same input user equation is executed at the reconstruction side, and the resultant value is given as input to the seed(), which generates the exact random value used at the share creation side.

3.2. Image Encryption Process using AES-ECC Technique

In this work, the AES-ECC technique is used for the encryption of shares. AES algorithm is a type of cipher texting that exploits the block cipher and only applies a single key for encrypting and decrypting processes for data protection [22]. It is a more commonly used strategic method over CC to increase the safety policies over cloud storage. This study exploits the AES since it is time compatible and easily implemented with cloud storage data accessibility. Thus, a single AES is slightly slower than the ECC-AES technique due to the large key sizing.

In contrast, a faster security system is used for securing the information, and the hybrid model allows for a reduction of the key size. As a smaller key size is the ECC's fundamental property, once AES applies ECC for encrypting, the performance increases and the key size is reduced. To decrease the key sizing and generate a safe key system, ECC makes use of encrypting and decrypting key standards. ECC is the suitable AES method for securing the data from unauthorized access. Then Ciphertext generates the encrypting and decrypting of information when the key sizing is set. The key created by ECC is utilized by AES. This might assist in decreasing the storage size with secured data.

It is evident AES and ECC efficiently secure information over cloud storage. The innovation of the presented technique is secured communication of information to the server, and the storage system is also protected because of the encrypted dataset. Furthermore, novelty could be defined with respect to time and computational cost. But attack prevention could be performed as, for instance if the attackers want to perform an attack on the user's side to get the user's personal data or any other purpose when the user is uploading the input document, the documents are transformed into encrypted textual form by using AES. Hence the texts are completely encrypted. Thus, if the attacker performed an attack and, in some way, obtained the uploaded files of the user, next it is impractical since the data is previously encrypted during upload. Likewise, if the attack is implemented, the attacker cannot decrypt the encrypted files; thus, the information is secure from attacks.

3.3. Key Generation Process using ABC Algorithm

The ABC model is used for the optimal selection of the keys in the AES-ECC algorithm. ABC is a populace-based optimizing technique based on the minimal honeybee foraging mechanism [23]. The ABC population comprises onlooker bees (OBs) and employed bees (EBs). In this work, the search space signifies the atmosphere, and every point in the search range correlate to the source of the food (solution). The quality of food sources can be provided by the value of the function. Firstly, the EB scout and every EB decided to make use of a food source it had found. Thus, the EB number correlates to the food source number. EB communicates their food sources to the OB. The OB decides whether or not to visit it according to the quality of the food source. Good food source attracts further OBs. When the OB has selected a food source, search for the best location in its neighbourhood with the help of local search techniques. EB changes the location and promotes the novel food source when the new location quality found by the OB is superior to that of the location quality originally interacted by the corresponding EB, and then, the EB remain on the present food source. The EB abandons the food source and scouts for the novel one when the solution of EB hasn't been enhanced for the specific number of steps.

More formally: Assume a population of n virtual bees and a D dimensional function F consisting of n_{ob} EBs and n_{ob} OBs $(n = n_{ob} + n_{ob})$. Firstly, scout EB $i(i \in [1 \dots n_{ob}])$ is located in the randomly selected location $p_i = (x_1^i, \dots, x_D^i)$. Then, every EB i tries to enhance the existing location with a newly generated candidate location. p_i^* using the subsequent local searching rule.

$$p_i^* = \left(x_1^i, \dots, x_j^i + rand(-1,1)\left(x_j^k - x_j^i\right), \dots, x_D^i\right) \qquad (7)$$

Where $j \leq D$ represents an arbitrarily selected dimension, $k \neq i$ signifies a random-wise selected EB (reference EB), and $rand(-1,1)$ is a randomly generated integer that is ranging from -1 to 1. Through Eq. (7), assume that $1D$ is changed. All the EBs decide to remove p_i rather than p_i^* according to the following greedy selection mechanism,

$$p_i = \begin{cases} p_i & if\ f(p_i) > f(p_i^*) \\ p_i^* & \text{else} \end{cases} \qquad (8)$$

In Eq. (8), $f(p)$ means the fitness at location p; thus, $f(p) = F(p)$ for the maximizing problem and $f(p) = U - F(p)$ for the minimizing problem with U upper bound.
When every EB has upgraded its location, then each OB selects the present EB position by utilizing the roulette wheeling selection such that the P_i probability of selecting the location p_i of EB i is

$$P_i = \frac{f(p_i)}{\sum_{k=1}^{n_{eb}} f(p_k)}. \qquad (9)$$

When the OB selected the location of EB, i searched for the best location using Eq. (7). With that regard, the corresponding EB upgrade the location if the OB had found the best location. The presented method will monitor the number of times the location of an EB isn't updated by the local search (EBs or OBs). Once these numbers reached a limit $l \geq 1$, EB abandoned the location and scouted for a novel one. The process ends once a stopping criterion (a good function value or maximal amount of iteration) is satisfied. A summary of ABC is provided in Algorithm 1. The optimum key sets are now selected by taking the "fitness function" as the max key by implementing PSNR for scrambled and unscrambled information from clinical images. The objective function was established by using the ABC algorithm as follows.

$$Fitness = MAX\,\{PSNR\} \qquad (10)$$

Algorithm 1: Artificial Bee Colony

```
Place every employed bee in a random-wise location in the search space
While the stop condition is not satisfied, do
For every employed bee, do
If # steps on same location = 1 then
Select a random location in searching space
else
Search for the best location (Eqs. 7 and 8)
if the best location is found, then
                move from the present location to found location
end if
end if
end for
for each onlooker bee, do
        select an employed bee and move toward the location (Eq. (9))
update location (Eqs. (7) and (8))
end for
end while
```

3.4. BC-based Secure Transmission

The proposed ABCHIE-RKDSC technique involves BC technology that enables secure transmission of encrypted QPs. The BC was originally established for monetary purposes and emerged from cryptocurrency, and can cause a dramatic effect across a number of industries [24].

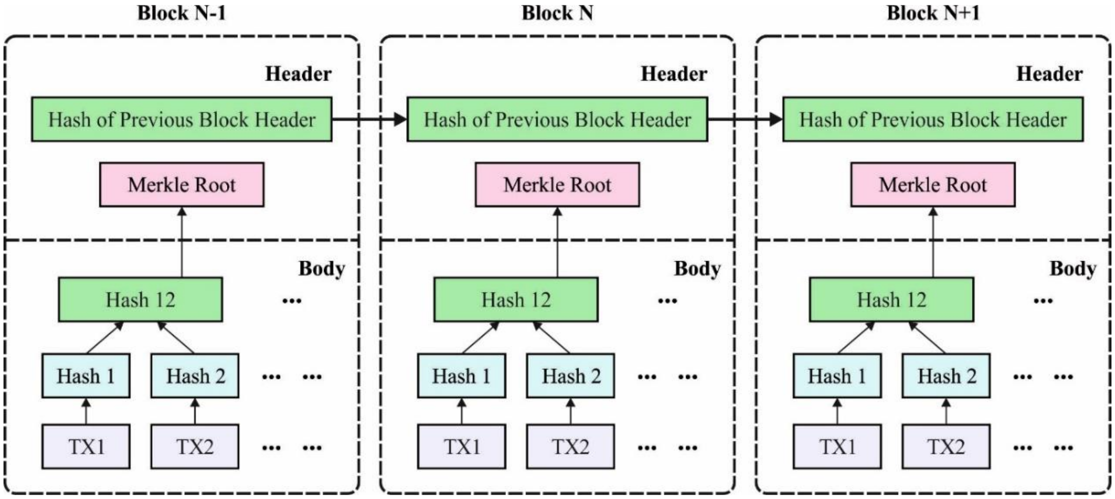


Fig. 2 Structure of BC

The primary goal is to eliminate 3rd parties from money transfers by constructing trustworthy digital money. The BC is a distributed ledger with complete transaction details in the networking. It is an addition of interconnected blocks that are connected by hash values that are developed over time. Each data on the BC cannot be changed and is permanent. The genesis block is an initial block of the BC. All the nodes of this chain have every single data, and it is connected to the hashed address of the preceding node. A hash finds the block and content. Similar to human fingerprints, it is often unique. When the block is generated, the hash has to be computed. Altering something inside the block might source the hash changing. This powerfully makes a chain of blocks. A BC is a P2P network; hence it doesn't have CA. All the nodes of BC receive a full copy of the entire chain; therefore node uses that copy to authenticate whether everything is still in order.

Fig. 2 represents the structure of BC. All the blocks are timestamped; thus, it is hardly possible to tamper with the information. Once the new block is generated and transferred to each chain node, all the nodes verify that these blocks have not been tampered with and create a consensus. There is no CA in the BC; hence it is a decentralized architecture. BC comprises private that are specially made for specific organizations, and the other one is public, for example, Ethereum and Bitcoin. The self-executable script is named smart contract. This smart contract is beneficial with respect to preventing fraud. Finally, the share reconstruction and image decryption process take place to retrieve the original QPs.

4. Results and Discussion

The presented approach is put under simulation by employing Python 3.6.5 tool on PC i5-8600k, GeForce 1050Ti 4 Giga Byte, 16GB RAM, 250GB SSD, and 1 Tera Byte HDD. In this section, the experimental result analysis of the ABCHIE-RKDSC method is investigated under discrete features. Fig. 3 visualizes the set of 4 shares produced by the ABCHIE-RKDSC technique on the applied image. The four shares represent no important data about the input image.

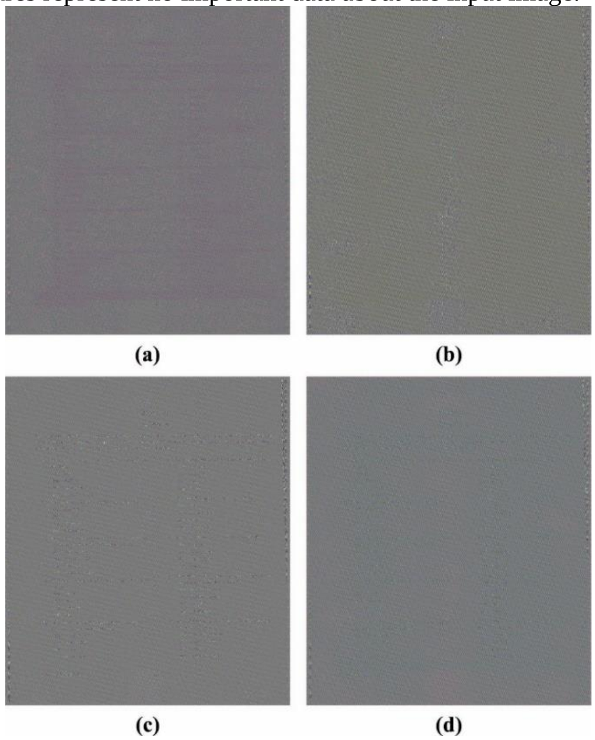


Fig. 3 Visualization of 4-Shares

In Table 1 and Fig. 4, the wide-ranging outputs of the ABCHIE-RKDSC model are investigated under different measures. The experimental values indicate that the ABCHIE-RKDSC method reaches effectual outcomes under the total imaging. For example, in the 1st image, the ABCHIE-RKDSC technique gains PSNR of 61.6855dB, SSIM of 0.9996, MSE of 0.0441, MAE of 5.9875, and BER of 0.0441.

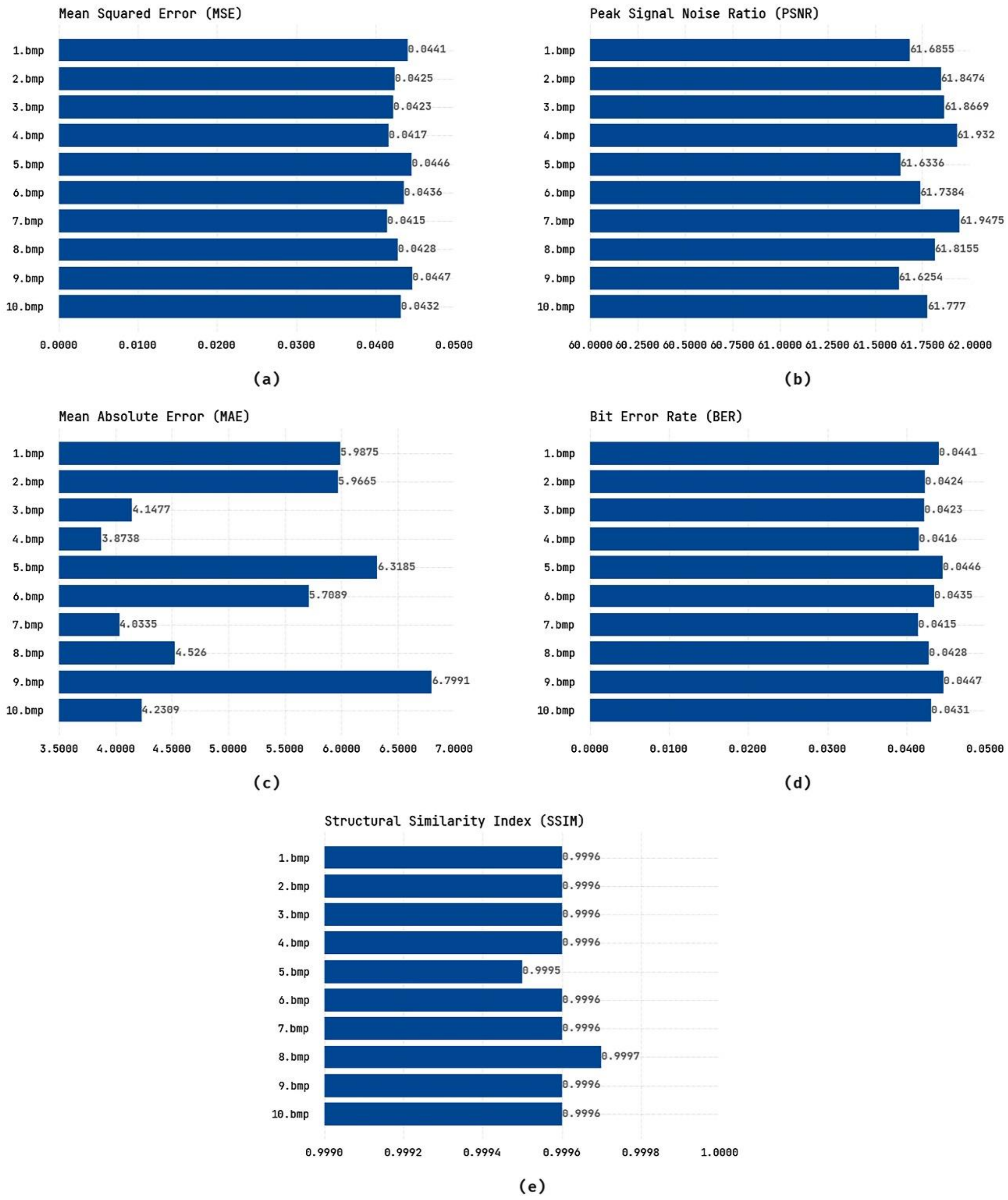


Fig. 4 Classifier outcome of ABCHIE-RKDSC system a) MSE b) PSNR c) MAE d) BER e) SSIM

Likewise, in image 4, the ABCHIE-RKDSC technique gains PSNR of 61.9320dB, SSIM of 0.9996, MSE of 0.0417, MAE of 3.8738, and BER of 0.0416. Similarly, in image 8, the ABCHIE-RKDSC method gains PSNR of 61.8155dB, SSIM of 0.9997, MSE of 0.0428, MAE of 4.5260, and BER of 0.0428. Finally, in image 10, the ABCHIE-RKDSC method gains PSNR of 61.7770dB, SSIM of 0.9996, MSE of 0.0432, MAE of 4.2309, and BER of 0.0431.

Table 2 reports a relative PSNR research of the ABCHIE-RKDSC technique with other encryption standards. The experimental values represent that the ABCHIE-RKDSC model attains increasing values of PSNR. Fig. 5 inspects a brief PSNR assessment of the ABCHIE-RKDSC technique with other encryption techniques on images 1-5. The results demonstrate that the ABCHIE-RKDSC technique reaches maximum values of PSNR under the total imaging.

Table 1. Classifier outcome of ABCHIE-RKDSC approach under distinct images and measures

No. of Images	PSNR	SSIM	MSE	MAE	BER
Image-1	61.6855	0.9996	0.0441	5.9875	0.0441
Image-2	61.8474	0.9996	0.0425	5.9665	0.0424
Image-3	61.8669	0.9996	0.0423	4.1477	0.0423
Image-4	61.9320	0.9996	0.0417	3.8738	0.0416
Image-5	61.6336	0.9995	0.0446	6.3185	0.0446
Image-6	61.7384	0.9996	0.0436	5.7089	0.0435
Image-7	61.9475	0.9996	0.0415	4.0335	0.0415
Image-8	61.8155	0.9997	0.0428	4.5260	0.0428
Image-9	61.6254	0.9996	0.0447	6.7991	0.0447
Image-10	61.7770	0.9996	0.0432	4.2309	0.0431

For instance, with 1st image, the ABCHIE-RKDSC technique attains an increasing PSNR of 61.6855dB while the CE, ECC, OE, and MSE models accomplish reducing PSNR of 47.90dB, 47.57dB, 47.54dB, and 47.42dB correspondingly. Along with that, with image 2, the ABCHIE-RKDSC method attains an increasing PSNR of 61.8474dB while the CE, ECC, OE, and MSE algorithms accomplish reducing PSNR of 48.09dB, 47.97dB, 47.74dB, and 46.98dB correspondingly. Likewise, with image 3, the ABCHIE-RKDSC method gains a maximum PSNR of 61.8669dB while the CE, ECC, OE, and MSE models accomplish minimal PSNR of 47.24dB, 46.81dB, 46.79dB, and 45.52dB subsequently. Similarly, with image 5, the ABCHIE-RKDSC methodology attains an increasing PSNR of 61.6336dB. At the same time, the CE, ECC, OE, and MSE approaches accomplish minimal PSNR values of 47.82dB, 47.50dB, 47.09dB, and 46.57dB subsequently.

Table 2. PSNR analysis of ABCHIE-RKDSC approach with other encryption techniques

PSNR (dB)					
Number of Images	ABCHIE-RKDSC	Chaotic Encryption	Elliptic curve Encryption	Optical Encryption	Metaheuristic Encryption
Image-1	61.6855	47.90	47.57	47.54	47.42
Image-2	61.8474	48.09	47.97	47.74	46.98
Image-3	61.8669	47.24	46.81	46.79	45.52
Image-4	61.9320	47.07	46.86	46.85	46.32
Image-5	61.6336	47.82	47.50	47.09	46.57
Image-6	61.7384	47.89	47.12	47.03	46.57
Image-7	61.9475	47.29	47.12	47.08	45.01
Image-8	61.8155	46.65	45.25	45.15	44.87
Image-9	61.6254	47.38	46.99	46.42	46.06
Image-10	61.7770	47.24	47.24	46.99	45.97

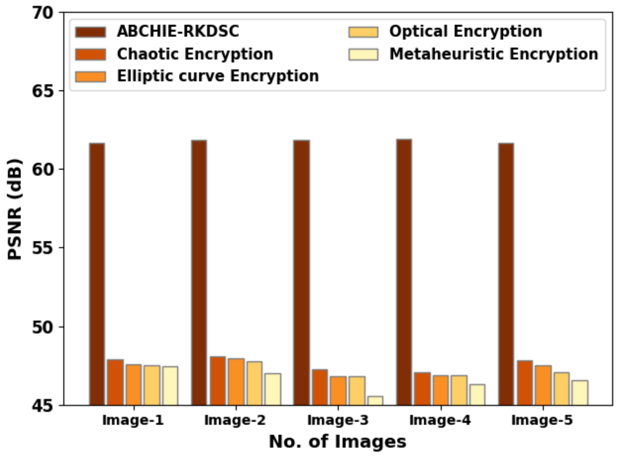


Fig. 5 PSNR analysis of ABCHIE-RKDSC approach under images 1-5

Fig. 6 examines a brief PSNR assessment of the ABCHIE-RKDSC system with other encryption methods on images 6-10. The results exhibit that the ABCHIE-RKDSC method attains maximum values of PSNR under the total imaging. For instance, with the 6th image, the ABCHIE-RKDSC model executed an increasing PSNR value of 61.7384dB, while the ECC, OE, CE, and MSE techniques accomplished a reducing PSNR values of 47.12dB, 47.89dB, 47.03dB, and 46.57dB subsequently. Along with that, with image 7, the ABCHIE-RKDSC technique attains an increasing PSNR value of 61.9475dB, whereas the CE, ECC, OE, and MSE models accomplish reducing PSNR values of 47.29dB, 47.12dB, 47.08dB, and 45.01dB subsequently. Similarly, with image 8, the ABCHIE-RKDSC technique attains an increasing PSNR of 61.8155dB while the CE, ECC, OE, and MSE techniques accomplish reducing PSNR of 46.65dB, 45.25dB, 45.15dB, and 44.87dB respectively.

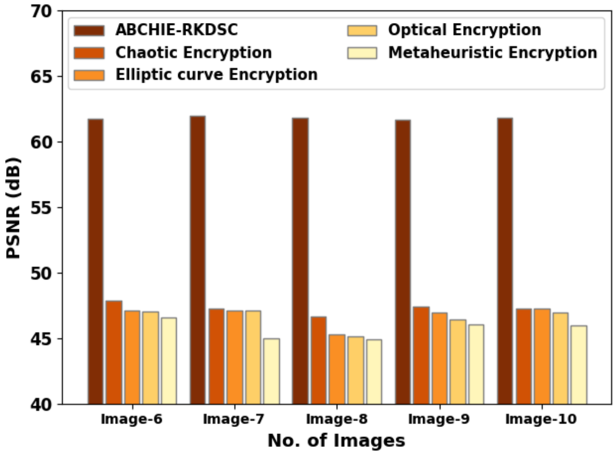


Fig. 6 PSNR analysis of ABCHIE-RKDSC approach under images 6-10

Similarly, with image 10, the ABCHIE-RKDSC method attains an increasing PSNR of 61.7770dB while the CE, ECC, OE, and MSE models accomplish reducing PSNR values of 47.24dB, 46.99dB, and 45.97dB subsequently. The outcomes assured the advanced achievement of the ABCHIE-RKDSC model.

5. Conclusion

In this research, a new ABCHIE-RKDSC approach has been introduced for safe QP sharing in the educational sector. In the introduced ABCHIE-RKDSC approach, three key procedures are utilized, namely share creation, share encryption, and BC-enabled transmission. During the process of share creation, a set of four shares is created for every input image and the random process key generation process is performed by a user input equation instead of a conventional random seed function. Next, the generated shares undergo encryption by the AES-ECC algorithm. Moreover, the key generating process of the AES-ECC model is performed by the use of the ABC algorithm. The proposed ABCHIE-RKDSC technique involves BC technology that enables secure transmission of encrypted QPs. Finally, the share reconstruction and image decryption process take place to retrieve the original QPs. The experimental validation of the ABCHIE-RKDSC method is investigated, and the outcomes are evaluated under different measures. A comprehensive result evaluation highlighted the betterment of the ABCHIE-RKDSC approach over other models. In future, the performance of the ABCHIE-RKDSC technique can be extended to a biometric verification system for online examinations.

References

[1] Fausto Neri da Silva Vanin et al., “A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach,” *Sensors*, vol. 23, no. 1, p. 14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Bannishikha Banerjee et al., “Digital Image Encryption Using Double Crossover Approach for SARS-Cov-2 Infected Lungs in a Blockchain Framework,” *Frontiers in Blockchain*, vol. 4, p. 771241. [CrossRef] [Google Scholar] [Publisher Link]

[3] C. Edward Jaya Singh, and C. Adline Sunitha, “Chaotic and Paillier Secure Image Data Sharing Based on Blockchain and Cloud Security,” *Expert Systems with Applications*, vol. 198, p. 116874, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] E. Sweetline Priya, R. Priya, and R. Surendiran, "Implementation of Trust-Based Blood Donation and Transfusion System Using Blockchain Technology," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 104-117, 2022. [CrossRef] [Publisher Link]

[5] Randhir Kumar et al., “A Secured Distributed Detection System Based on IPFS and Blockchain for Industrial Image and Video Data Security,” *Journal of Parallel and Distributed Computing*, vol. 152, pp. 128-143. [CrossRef] [Google Scholar] [Publisher Link]

[6] Taehyoung Kim, Im Y. Jung, and Yih-Chun Hu, “Automatic, Location-Privacy Preserving Dashcam Video Sharing Using Blockchain and Deep Learning,” *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp.1-23, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jhanavi J, and Dr.M.Dakshayini, "Blockchain Implementation for Storage," *SSRG International Journal of Mobile Computing and Application*, vol. 5, no. 2, pp. 9-12, 2018. [CrossRef] [Publisher Link]

[8] Zhaofeng Ma et al., “Fully Homomorphic Encryption-Based Privacy-Preserving Scheme for Cross Edge Blockchain Network,” *Journal of Systems Architecture*, vol. 134, p.102782. [CrossRef] [Google Scholar] [Publisher Link]

[9] Widiwidayat, I., and Köppen, M., “Blockchain Simulation Environment on Multi-Image Encryption for Smart Farming Application,” *International Conference on Intelligent Networking and Collaborative Systems*, pp. 316-326, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Amirthalingam, and R. Ponnusamy, "Intelligent Wireless Endoscopic Image Classification Using Gannet Optimization with Deep Learning Model," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 3, pp. 104-113, 2023. [CrossRef] [Publisher Link]

[11] M. Sunitha, and G. Mary Valantina, "Fowlkes-Mallows Correlated Cohen Kappa Coefficient Block Matching Based Multi-Layer Perceptron Classification for Motion Estimation in VLSI," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 2, pp. 102-109, 2023. [CrossRef] [Publisher Link]

[12] L. Srinivasan et al., "IoT-Based Solution for Paraplegic Sufferer to Send Signals to Physician Via Internet," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 1, pp. 41-52, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Kunpeng Wang et al., "Formation Optimization of Blockchain-Assisted Swarm Robotics Systems Against Failures Based on Energy Balance," *Simulation Modelling Practice and Theory*, vol. 120, p. 102599. [CrossRef] [Google Scholar] [Publisher Link]

[14] Muhammad Mateen Yaqoob et al, "Modified Artificial Bee Colony Based Feature Optimized Federated Learning for Heart Disease Diagnosis in Healthcare," *Applied Sciences*, vol. 12, no. 3, p. 12080, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] M. Selvavathi, and S.Edwin Raja, "Anticipation of Vulnerable Attacks in Vanet Using Blockchain Technique," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 1, pp. 19-23, 2021. [CrossRef] [Publisher Link]

[16] Fadwa Alrowais et al., "Cyber Attack Detection in Healthcare Data Using Cyber-Physical System With Optimized Algorithm," *Computers and Electrical Engineering*, vol. 108, p. 108636. [CrossRef] [Google Scholar] [Publisher Link]

[17] Muhammad Mateen Yaqoob, "Hybrid Classifier-Based Federated Learning in Health Service Providers for Cardiovascular Disease Prediction," *Applied Sciences*, vol. 13, no. 3, p.1911. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohammad Babar et al., "Intelligent Computation Offloading for IoT Applications in Scalable Edge Computing Using Artificial Bee Colony Optimization," *Complexity*, vol. 2021, pp.1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Cheng Ting Tsai, and Ja Ling Wu "A Blockchain-Based Fair and Transparent Homework Grading System for Online Education," *Principles and Practice of Blockchains*, pp. 303-326, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Ashutosh Dhar Dwivedi et al., "Tracing the Source of Fake News Using a Scalable Blockchain Distributed Network," *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 38-43, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Shyamala G et al, "Home Automation Security Using Blockchain," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 7, pp. 63-68, 2020. [CrossRef] [Publisher Link]

[22] Sachi Nandan Mohanty et al., "An Efficient Lightweight Integrated Blockchain (ELIB) Model for Iot Security and Privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027-1037, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Monther Tarawneh et al., "Secure Exam Storage Using RSA Public Key Encryption," [CrossRef] [Google Scholar][Publisher Link]

[24] Jeonghun Cha et al., "Blockchain-Empowered Cloud Architecture Based on Secret Sharing for Smart City," *Journal of Information Security and Applications*, vol. 57, p. 102686, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Rishabh Mehta et al., "Decentralized Image Sharing and Copyright Protection Using Blockchain and Perceptual Hashes," *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Minu, M., and R. Aroul Canessane, "Secure Image Transmission Scheme in Unmanned Aerial Vehicles Using Multiple Share Creation with Optimal Elliptic Curve Cryptography*," Indian Journal of Computer Science and Engineering*, vol. 12, no. 1, pp.129-134, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Mansi Bosamia, and Dharmendra Patel, "An Experiment of a Parallel Entry Security Testing Approach Using Ethereum Blockchain," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 295-304, 2022.[CrossRef] [Publisher Link]

[28] Saba Rehman et al., "Hybrid AES-ECC Model for the Security of Data Over Cloud Storage," *Electronics*, vol. 10, no. 21, p. 2673, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Dr. I. Jeena Jacob, and Dr. P. Ebby Darney, "Artificial Bee Colony Optimization Algorithm for Enhancing Routing in Wireless Networks," *Journal of Artificial Intelligence*, vol. 3, no. 1, pp. 62-71, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] YongJoo Lee, Keon Myung Lee, and Sang Ho Lee, "Blockchain-Based Reputation Management for Custom Manufacturing Service in the Peer-to-Peer Networking Environment," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 671-683, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Mohananthini, N., and Yamuna, G., "Watermarking for Images Using Wavelet Domain in Back-Propagation Neural Network," *IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012)*, pp. 100-105, 2012. [Google Scholar] [Publisher Link]