ArtificialButterflyOptimizationBasedQuantumKeyImage Encryption Approach for Cloud Security

S.Sheela[1,2*],N.Subbulakshmi[3]

[1]ResearchScholar,DepartmentofComputerApplications,KalasalingamAcademyofResearchand Education, Krishnankoil, Tamil Nadu, India
[2]AssistantProfessor,MarianCollege,KuttikanamAutonomous,Kerala,Email:Indiasheelastju@yahoo.com[3]Associate Professor, Department of Computer Science and Engineering, school of computing, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India,
Email:n.subbulakshmi@klu.ac.in
*CorrespondingAuthor

Received:19.04.2024 Revised:22.05.2024 Accepted:27.05.2024

ABSTRACT
With the increasing popularity of multimedia technologies and the occurrence of several smart electronic devices, severe security problems are newly occurring in data and communication schemes. Image maintenance is preserved as a classical instance of cloud memory outsourcing as images need much higher memory than text documents. An image encryption approach with maximum effectual is vital for preserving the privacy of sensitives and vital images from cloud-edge communication. This studydevelopsanartificialbutterflyoptimizationalgorithmbasedquantumkeyimageencryption (ABOA-QKIE) approach for cloud security. The presented ABOA-QKIE technique accomplishes security in cloud environment via image encryption with optimal key generation process. Primarily, the ABOA-QKIE technique uses quantum key encryption approach to encrypt the input images. Besides, ABOA is applied for optimal key generation process and then the encrypted images are transmitted to the cloud server. At the receiving end, the encrypted images are accessed from the cloud server and the quantum key decryption process takes place to retrieve the original input images. The experimental validation of the ABOA-QKIE technique is tested using a series of images and the results are inspected under different measures. Extensive comparison studies highlighted the improved performance of the ABOA-QKIE technique over other recent approaches.

Keywords: Cloudcomputing;Security;Imageencryption;Keygeneration;Quantumkeyencryption

1. INTRODUCTION

The storage of multimedia data and real-time fast processing on the internet greatly depend on cloud computing (CC). Though the cloud is hardly a decade old, it influences the computing environment likeany other technology [1]. Other than offering several other advantages, the main benefit is that this technology is easy to understand even for technical neophytes [2]. The streaming multimedia, flexible nature, establishment of applications across platforms, and utilizing analytic data paradigms to make estimations, make it the right choice for businesses which are highly dependent on data analytics [3]. Moreover, there occurs growth in data production, and storage space is, inadequate. In short, many authors arestill working on data security inCC, since the reliable environment of the technology is highly significant to obtain users' confidence [4]. CC can be defined as a technology which renders flexibilities likemanagedservice, infrastructureasaservice,Web-basedcloudcomputing,utilityservices,platformas a service (PaaS), software as a service (SaaS), etc. The generated data is stored on storage given by cloud system providers [5]. The great advantage of the cloud is that when an employee or a user or anycompany needs to access that data authentication has done in advance. Still, it also has some disadvantages like flexibility, cost, vendor lock-in, prone to attack, limited control, and most significant privacy and security.
Authentication like conventional techniques is done by PINs and passwords [6], but users have to remember them. As the users cannot remember many passwords, they usually use the same password everywhere which will be easier for hackers [7]. Today, multi-factor authentication is utilized by mobile phones and cloud services, but then cost disparity is created.Efficient and Secure encryption of image informationbecomesthecoresubjectofmuchmultimediaresearch[8].Owingtothelowentropyof

digital imagery, along with the high redundancy and strong pixel correlation, conventional encryption techniques are usually ineffective while encrypting image data. The model of novel cryptographicmethods related to chaotic mechanisms is becoming a preferable image encryption solution [9]. Various new image encrypted methods were devised like image passwords relevant to chaotic mechanisms. Efficient and Secure encryption of image information is the focus of much multimedia research [10].

This study develops an artificial butterfly optimization algorithm based quantum key image encryption (ABOA-QKIE) approach for cloud security. The presented ABOA-QKIE technique uses quantum key encryption approach to encrypt the input images. Besides, ABOA is applied for optimal key generation process and then the encrypted images are communicated to the cloud server. At the receiving end, the encryptedimagesareaccessedfromthecloudserverandthequantumkeydecryptionprocesstakesplace to retrieve the original input images. The experimental validation of the ABOA-QKIE technique is tested using a series of images and the results are inspected under different measures.

2. RELATEDWORKS

Sasikumar etal.[11]developedanSQKD-CDSmodelabbreviatedasSecureQuantumKeyDistribution forCloud Data Securitymethod. For encoding the clientinformation, the simulation method makes use of Non-AbelianEncryption(NAE) for offering secure data security along with that the quantum key is utilizedtoaccessthestoreddataincloud.Likewise,utilizingthe quantumchannel,thekeyswillbeshared securely among nodes. Kacheru, G. [12] devise a quantum identity related authentication and key agreement technique for cloud server structure. For confidentiality and securing privacy in the domain of network security, Quantum cryptography related to the laws of quantum physics becomes a crucial technology. The security analysis of presented method proved to be robust in all security attacks.

Ahybridencryptedtechniquefor quantumsecurevideo conferencingintegratedwithBCwasmodelledin [13].Duringthesystemsolutionstructure,thequantumkeydistributionnetworkinghasbeenentrenched in the classical network; after, the "classical and quantum" hybrid encrypted technique was modelled as per thesecretleveldemandedvideoconferencecontents.In[14],anewcolorimageencryptiontechnique relevant to DNA sequence operations and controlled alternate quantum walks (CAQW) was modelled. DNA encoding rule can be utilized for replacing the pixel values, CAQW was utilized as a pseudo-random number generator (PRNG) for scrambling pixel positions, and the series of pseudo-random numerals produced by DNA and PRNG function rules were utilized in 2 rounds of encrypting plaintext images.

Sundar et al. [15] formulated an ECSM-QKDP method abbreviated as Enhanced Cloud Security Model and Quantum Key Distribution Protocol, to manage data dynamics and offer cloud storage security, quantum key cryptography was included. During the initial stage, BB84 QKDP was utilized and under the nextstage, Secure Authentication Protocol was constructed related to secure keys and distance bounding, which can be generated through Hierarchical Attribute-Set related encrypted. In [16], the authors usedthe structures of quantum walk for framing a novel S-box method which serves the main role in block cipher methods for 5G-IoT technology. To satisfy requirements of encryption for diverse files in 5G-IoT, the authors used the quantum walk features for devising a new encryption method forsecuringbroadcast of sensitive recordsfrom 5G-IoT. Liu et al. [17]modelled a new Quantum-related Secure and Lightweight Transmission (QSLT) system to ease overweight pain for IoT gadgets from eavesdropping. Through one among them, QSLT decodes or encodes IoT delicate information.

3. TheProposedModel

In this study, we have introduced a novel ABOA-QKIE approach for image encryption process.The presented ABOA-QKIE technique accomplishes security in cloud environment via image encryption with optimal key generation process. Primarily, the ABOA-QKIE technique uses quantum key encryption approach to encrypt the input images. Besides, ABOA is applied for optimal key generation process and then the encryptedimages aretransmittedtothecloud server.Atthereceiving end,the encryptedimages are accessed from the cloud server and the quantum key decryption process takes place to retrieve the original input images. Fig. 1 depicts the workflow of ABOA-QKIE approach.

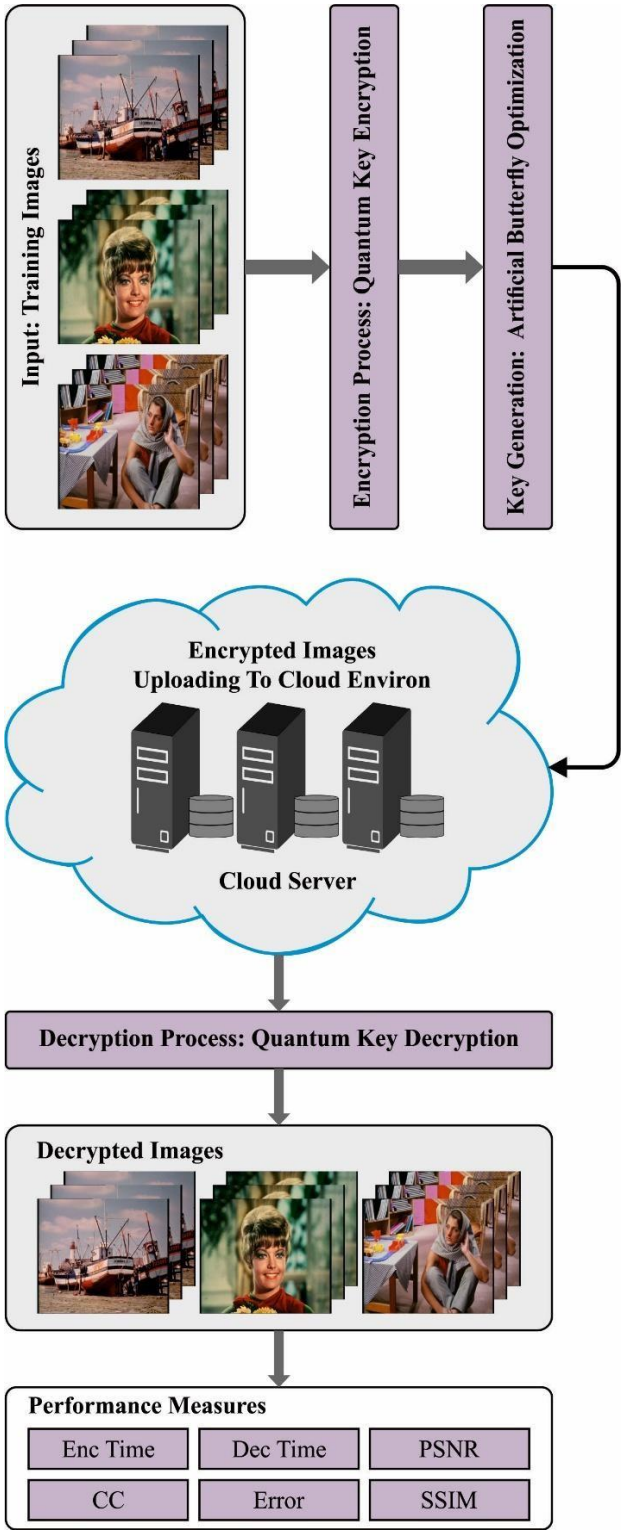

Fig1. WorkflowofABOA-QKIEapproach

QuantumKeyEncryptionandDecryptionProcess

At this stage, the input images are initially encrypted by the use of quantumkey encryption technique. A new quantum image (QI) encryption technique dependent upon quantum key images (QKI) wasprojected.

KeyStream Generation

A cryptographic technique was utilized for generating the keystream, and could not border the algorithm [18].AnyonethatproducesanarbitraryorderisutilizedforgeneratingtheKS.Considerthekeystream

(KS)is:$K = \{k_0,k_1,k_2,\ldots,k_{qn-1}\}$,whereas$k_i \in \{0,1\}, i \in [0,qn-1]andn = HW$denotethelengthof keystream that similar to plain image size.

PreparationofQKI

This step makes the KSKas to quantum computer as a QKI that is dependent upon GQIR. Without producingconfusion,thekeyimages arestillsignifiedby K.Every pixelapplies$q$ bitsinKSK consecutively as its gray value. The preparation of GQIR comprises three phases.

Theinitialstageisforpreparing$h+w+q$qubitsandfixedto$|0\rangle$.UsingEq.(1),aprimarystatehasbeen formulated:

$$|\psi\rangle_0 = |0\rangle^{\otimes h+w+q} \quad (1)$$

The 2nd stage applies the single qubit gates, H (the Hadamard gate) and I (the identity gate), for constructingblank$2^h \times 2^w$boxes.Aprimarystate$|\psi\rangle_0$isconvertedastoin-betweenstate$|\psi\rangle_1$.U_1denotes the quantum function that is formulated by Eq. (2):

$$U_1 = I^{\otimes q} \bigotimes H^{h+w} \quad (2)$$

andthen

$$U_1(|\psi\rangle_0) = (I|0\rangle)^{\otimes q} \bigotimes (H|0\rangle)^{\otimes h+w}$$

$$= \frac{1}{\sqrt{2^{h+w}}} |0\rangle^{\otimes q} \bigotimes \sum_{i=0}^{2^h-12^w-1} |i\rangle$$

$$= \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{} \sum_{X=0}^{} |0\rangle^{\otimes q} |YX\rangle \quad (3)$$

$$= |\psi\rangle_1$$

The 3rd stage set the "gray value" for all the pixels. The gray value is HxW block of the KS, every block is set to one pixel. During this step, it can be classified into HxW sub-operations forstoring the KS forallthe pixels. In the following, the quantum sub operation $U_{YX}$is demonstrated:

$$U_{YX} = (I \bigotimes \sum_{ji \neq Y \cdot X} |ji\rangle\{ji|) + \Omega_{YX} \bigotimes |YX\rangle\{YX| \quad (4)$$

InEq.(4),Ω_{YX}indicatesthequantumfunctionthatistoalterationthepixelvalues$(XY)$from$|0\rangle^{\otimes q}$to $\{YH+Xth$ blockofKS.Meanwhile,itmakesuseof$q$qubitsforrepresentingthepixel,Ω^i_{YX} isutilizedfor changingthevalueofithqubitofpixels(YX)'sKSblock.$k_{q(YH+X)+i}$indicatesthevalueofi^{th}qubitsof pixels(XY)KS block and it is represented by K^i.

$$\Omega_{YX} = \Omega^{q-1}_{YX} \quad (5)$$

$$\Omega^i_{YX}: |0\rangle \rightarrow |0 \oplus K^i\} \quad (6)$$

Theexpression$\oplus$showstheXORfunction.Itcanbe$a(h+w)$-CNOTgate,when$K^i=1$thenΩ^i_{YX} : $|0\rangle \rightarrow |0 \oplus K^i\}$.Orelse,itcanbequantumidentitygatewhichΩ^i_{YX} :$|0\rangle \rightarrow |0\rangle$.Afterward$U_{YX}$doonthe in-betweenstate$|\psi\rangle_1$,thatthe$|\psi\rangle_1$waschangedinthefollowing:

$$U_{YX}(|\psi\rangle) = U_1 \quad (\frac{1}{\sqrt{2^{h+w}}} \sum_{j=0}^{2^h-12^w-1} \sum_{i=0} |0\rangle^{\otimes q} |ji\rangle)$$

$$= \frac{1}{\sqrt{2^{h+w}}} U_{YX} \sum_{ji \neq YX} |0\rangle^{\otimes q} |ji\rangle + |0\rangle^{\otimes q} |YX\rangle) \quad (7)$$

$$= \frac{1}{\sqrt{2^{h+w}}} U_{YX} \sum_{ji \neq YX} |0\rangle^{\otimes q} |ji\rangle + \Omega_{YX} \quad |0\rangle^{\otimes q} |YX\rangle)$$

$$= \frac{1}{\sqrt{2^{h+w}}} U_{YX} (\sum_{ji \neq YX} |0\rangle^{\otimes q} |ji\rangle + |K_{YX} \quad \rangle |YX\rangle)$$

In the following equation, it is noticeable that every sub-operation U_{YX}set the gray values of their matching pixel. Thus, the quantum function$U_2$of 3rd step was determined by Eq. (8) that is comprised of all the sub-operations for all the pixels.

$$U_2 = \mathbf{G} \mathbf{G}_{Y=0}^{H-1} \mathbf{G}_{X=0}^{W-1} U_{YX} \quad (8)$$

WiththequantumfunctionU_2,thein-betweenstate$|\psi\rangle_1$isconvertedastolaststate$|\psi\rangle_2$thatis

QKIKdependentuponGQIR.

$$U_2(|\psi\rangle)_1 = \frac{1}{\sqrt{2}^{h+w}} \left(\sum_{Y=0}^{H-1}\sum_{X=0}^{W-1} |K_{YX}\rangle|YX\rangle + \sum_{Y\in\{H,\ldots,2^h-1\} or X\in\{W,\ldots,2^w-1\}} \bigotimes_{i=0}^{q-1}|0\rangle|YX\rangle\right) (9)$$

InEq.(9),theKSwaspreparedtotheQKIwhichisequivalenttoplainimagesizes.

XORoperation

TheQKIKhasXORedwith$I$theplainimageforgettingtheencryptionQIM.TheXORfunctionwas represented in the following:

$$\begin{aligned} |I\rangle \oplus |K\rangle &= \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1}\sum_{X=0}^{W-1} \bigotimes_{i=0}^{q-1}|C^i\}|YX\rangle \oplus \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1}\sum_{X=0}^{W-1} |K_{YX}\rangle|YX\rangle \\ &= \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1}\sum_{X=0}^{W-1}\sum_{i=0}^{q-1} |C^i\}|YX\rangle \oplus_{YX} \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1}\sum_{X=0}^{W-1}\sum_{i=0}^{q-1} |K^i\rangle|YX\rangle_{YX} \\ &= \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1}\sum_{X=0}^{W-1}\sum_{i=0}^{q-1} |C^i \oplus_{YX} K^i\rangle|YX\rangle_{YX} \\ &= |M\rangle \end{aligned} \quad (10)$$

The $h+w$ CNOT gate in an initial dotted block is utilized for aligning the position data of the two images: if$YX_I = YX_K$,whereYX_Iindicates thepositiondataoftheplainimage I andYX_Kdenotes thepositiondata ofkeyimages$K$,the$h+w$CNOTgatechangesYX_Ktostate$|0\rangle^{\otimes(h+w)}$,since$CNOT(O,0)=(0,0)$and $CNOT\ (1,1)=(1,0)$.Duringthenextdottedblock,$|A\rangle$denotestheauxiliaryqubit.IfYX_Kfromthestate $|0\rangle^{\otimes(h+w)}$,viz., $YX_I = YX_K$,then $|A\rangle$ischanged to $|1\rangle$. Specifically, $|A\rangle$isa flagto show if $YX_I = YX_K$.During the 3rddotted block, if $|A\rangle = |1\rangle$, the color data of plain images$I$ is XORed with color data of plain images$K$ and produced the encrypt image M.

OptimalKeyGenerationProcess

Inthisstudy,theABOAisappliedtoproduceanoptimalsetofkeysforencryptionanddecryptionprocess. The inspiration and movement behaviors of the butterfly are expressed by the optimization technique, where butterfly presents the search agent and the generated fragrance denotes the fitness value [19]. In thepresentedmethod,thesearchagentsorbutterfliescouldproducefitnessorfragrancevaluewithsome power to be distinguished from other fragrances. This behavior might assist other search agents to upgrade the location during the search space. As soon as the butterfly finds the better nectar food in the search space, it generates the fragrance, then each neighborhood butterfly moves to the better butterfly position. This updating model is named global search. At the same time, the butterfly randomly move in the search space once another butterfly fragrance was identified, called a local search in ABOA.

Thefragranceconcentrationisarithmeticallyexpressedbythefollowingequation:

$$pf_i = cI^a, \quad (11)$$

In Eq. (11), pf_iindicates the fragrance strength of i-th butterflies, I shows the stimulus intensity, c indicates the sensory modality, and a represents the power exponent dependent upon the modality that presentsavaryingabsorptiondegree.Everybutterflypositionispresentedasavectorofspecificproblem value. This position is upgraded in attempting to discover the best position using the subsequentequation:

$$x_i^{t+1} = x_i^t + F_i^{t+1}, \quad (12)$$

InEq.(12),x_i^tindicatesthepresentlocationofbutterfly$i$at$t$iteration,x_i^{t+1}denotesthefollowing location of butterfly i and F_i^{t+1}shows the fragrance used by $x_i$for updating its location in the iteration.

From the abovementioned, the updating model can be in two stages, involving global and local searches. In the global search, the butterfly i moves towards the best butterfly g^*that is shown below:

$$F_i^{t+1} = (r^2 \times g^* - x^t) \times pf_i, \quad (13)$$

In Eq. (13), r denotes a random value within [0,1]. In local search, the updating movement is expressedby:

$$F_i^{t+1} = (r^2 \times x_j^t - x_k^t) \times pf_i, \quad (14)$$

InEq.(14),x_j^tandx_k^tdenotesthepositionof$j$-$th$and$k$-thbutterfliesinthesearchspace.Anovelvariable named switch probability p, is applied in ABOA for switching the algorithm's behavior between local and global search to obtain a better balance amongst exploitation and exploration.The ABOA comprises five major steps as comprehensively deliberated in the following.

Step1:ABOAandtheproblemparameterinitialization.

TheproblemparameterandeveryABOAareinitializedinthisstep.ABOAcomprisesfiveparameters, involving c,a, p, population size (N), and number of iterations (Itr).

Step2:Populationinitialization.

UsingtheABOA,everysolutionisrandomlygenerated.Thesolutionisgivenasvectoroflength equivalent to the problem dimension d.

Everysolutionispositionedinthematrixforthepopulationgeneration,asdemonstratedinEq.(15).

$$Population = \begin{pmatrix} x_1^1 & x_2^1 & \cdots & x_d^1 \\ x_1^2 & x_2^2 & \cdots & x_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ x_1^N & x_2^N & \cdots & x_d^N \end{pmatrix} \quad (15)$$

Step3:Fitnessvaluecalculation.

Every solution is estimated according to the objective function of optimization problem in this step. Afterward, the better solution is allocated to g^*. Fig. 2 demonstrates the flowchart of ABOA.

Step4:Updatethepopulation.

Using theABOA, every solutionis upgraded to find the best solutionbased on the fitness value attained in Step3.Inthiswork, r israndomlyproducedandcomparedto $p$forleadingthesearchingbehaviorglobally or locally. If$r$islesser than$p$,then Eq.(13)isusedfor the global movement of the butterfly;orelse,Eq. (14) is used. Consequently, if case new solution is better than the older one, then replace the older solution. Last, upgraded the value of g^*.

Step5:Checkthestoppingcriteria

Repeatedsteps3to4untilthemaximalamountofiterationsisattained.

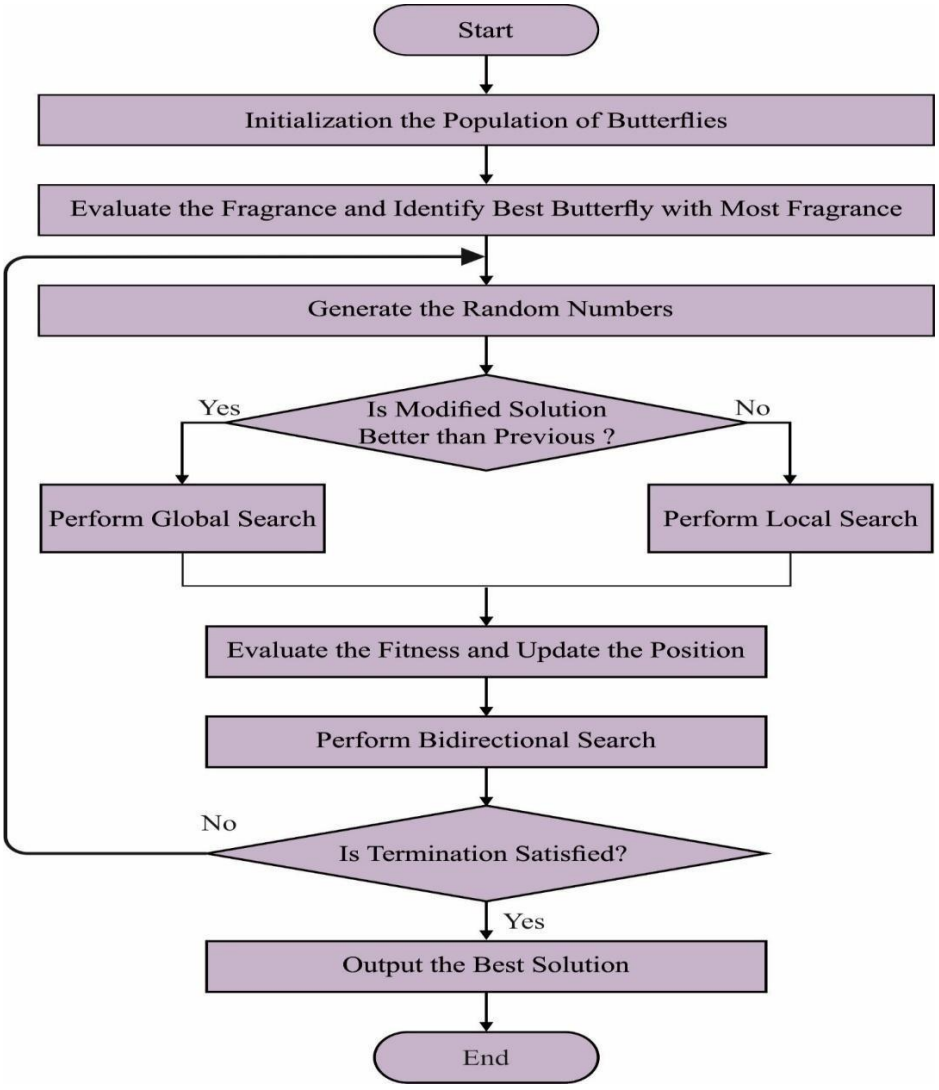

Fig2. FlowchartofABOA

The MBO algorithm generates a fitness function for HE technique. The maximization of peak signal to noise ratio (PSNR) is considered the fitness function, as given below.

$$Fitness=\max\{PSNR\} \quad (16)$$

Algorithm1: PseudocodeofABOA

```
Initializingtheproblemparameters
InitializingtheABOAparameters(Itr,N,c,a,p)
Initializingpopulationmatrix while
(itr≤ Itr) do
        forallthesolutionsdo
                Evaluatethesolution'sfitnessvalue
                g*=theoptimum solution
        endfor
        forallthesolutionsdo
                Creater(arbitrarynumbersin[0,1])
                ifr<pthen
                        UpgradethesolutionutilizinginEq.(13)
                else
                        UpgradethesolutionutilizinginEq.(14)
                endif
                Ifthesolutionisoptimum,upgradethepopulation.
                Upgradec
        endfor
        ifItrisnotreachedthen
                                                itr=itr+1
        endif
endwhile
Returng*
```

4. RESULTSANDDISCUSSION

This section investigates the experimental results of the ABOA-QKIE model with recent models under differentimages.Fig.3demonstratesthevisualizationresultsofthereconstructedimagesobtainedbythe ABOA-QKIE model. Fig. 3a and 3c depict the original images and their reconstructed versions are given in Fig. 3b and 3d. Figs. 4 and 5 illustrate the original and decrypted images under samples 1 and 2.

Fig3.(aandc)OriginalImages(bandd)ReconstructedImages

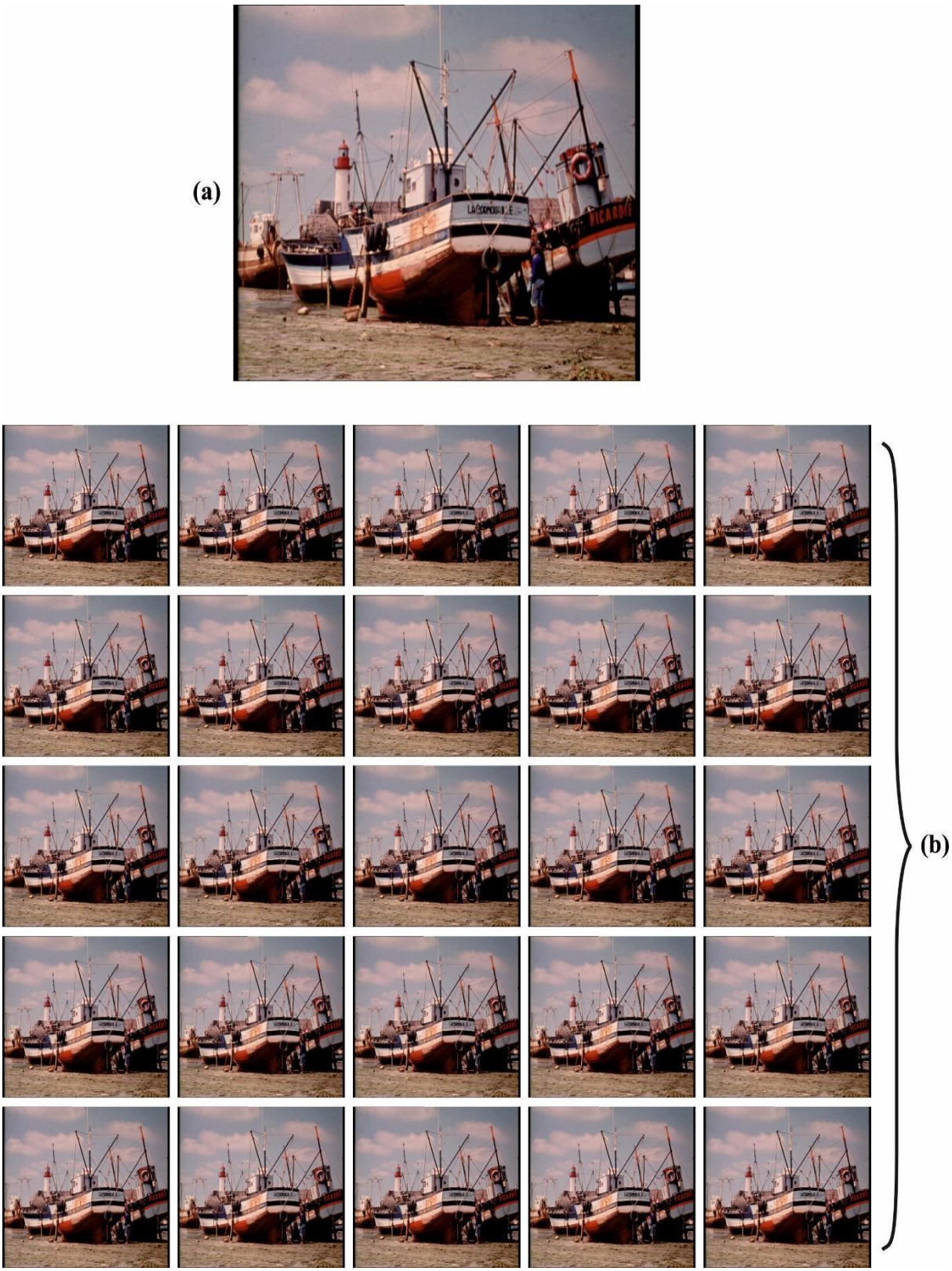

Fig4.a)OriginalImageb)25-IterationDecryptedImages(Sample1)

Table 1 reports the encryption results of the ABOA-QKIE model on image-1 with diverse iterations. The experimental results indicated that the ABOA-QKIE model has reached maximum performance under all iterationsintermsofencryptiontime(ET),decryptiontime(DT),PSNR,correlationcoefficient(CC),error, and structural similarity (SSIM). For instance, with iteration 1, the ABOA-QKIE model has obtained ET of 0.00009s, DT of 0.00017s, PSNR of 64.84dB, CC of 0.9998, error of 0.0213, and SSIM of 0.9979.

Fig5.a)OriginalImageb)25-IterationDecryptedImages(Sample2)

In addition, with iteration 10, the ABOA-QKIE approach has attained ET of 0.00010s, DT of 0.00015s, PSNR of 63.90dB, CC of 0.9997, error of 0.0265, and SSIM of 0.9975. Moreover, with iteration 25, the ABOA-QKIEalgorithm hasgained ET of 0.00018s, DT of 0.00018s, PSNR of 64.09dB, CCof0.9997, error of 0.0253, and SSIM of 0.9977.

Table1. ResultanalysisofABOA-QKIEtechniquewithvariousmeasuresanditerationsonImage-1

Iterations	Encryption Time (s)	Decryption Time (s)	PSNR	Corr. Coef	Error	SSIM
1	0.00009	0.00017	64.84	0.9998	0.0213	0.9979
2	0.00010	0.00024	64.24	0.9997	0.0245	0.9974
3	0.00013	0.00018	64.66	0.9997	0.0222	0.9972
4	0.00012	0.00018	64.27	0.9997	0.0243	0.9973
5	0.00012	0.00018	64.42	0.9997	0.0235	0.9975
6	0.00011	0.00024	64.40	0.9997	0.0236	0.9975
7	0.00009	0.00024	64.41	0.9997	0.0236	0.9975
8	0.00013	0.00019	64.35	0.9998	0.0239	0.9981
9	0.00014	0.00015	64.00	0.9998	0.0259	0.9981
10	0.00010	0.00015	63.90	0.9997	0.0265	0.9975
11	0.00009	0.00010	64.36	0.9997	0.0238	0.9977
12	0.00012	0.00014	64.07	0.9997	0.0254	0.9975
13	0.00010	0.00013	64.19	0.9997	0.0248	0.9974
14	0.00015	0.00023	64.53	0.9998	0.0229	0.9980
15	0.00015	0.00016	65.35	0.9998	0.0190	0.9979
16	0.00013	0.00017	63.94	0.9997	0.0263	0.9974
17	0.00017	0.00025	64.44	0.9997	0.0234	0.9976
18	0.00014	0.00015	64.54	0.9997	0.0229	0.9973
19	0.00017	0.00015	64.20	0.9998	0.0247	0.9977
20	0.00011	0.00012	64.83	0.9998	0.0214	0.9979
21	0.00010	0.00026	64.37	0.9998	0.0238	0.9982
22	0.00014	0.00020	63.91	0.9997	0.0264	0.9973
23	0.00015	0.00016	64.88	0.9997	0.0212	0.9971
24	0.00016	0.00018	64.62	0.9997	0.0225	0.9974
25	0.00018	0.00018	64.09	0.9997	0.0253	0.9977

Table 2 presents the optimal encryption results obtained by the ABOA-QKIE model. The results indicated that the ABOA-QKIE model has attained effectual outcomes under all images with different iterations.

Table2. OptimalresultanalysisofABOA-QKIEtechniqueundervarioustestimages

No.ofImages	Optimal Iteration	PSNR	Error	CC	SSIM	Encryption Time(s)	Decryption Time(s)
Image1	15	65.35	0.0190	0.9998	0.9979	0.000149	0.000164
Image2	15	65.35	0.0190	0.9998	0.9979	0.000149	0.000165
Image3	15	64.78	0.0216	0.9998	0.9985	0.000144	0.000154
Image4	9	62.29	0.0384	0.9998	0.9974	0.000097	0.000077
Image5	15	64.78	0.0216	0.9997	0.9978	0.000143	0.000152
Image6	7	Infinity	0.0000	1.0000	1.0000	0.000053	0.000207

Table 3 and Fig. 6 report a comparative PSNR study of the ABOA-QKIE approach with other encryption techniques. The outcomes indicated that the ABOA-QKIE system has gained increasing values of PSNR under all images. For sample, on image 1, the ABOA-QKIE model has offered higher PSNR of 65.35dBwhile the ECC and RSA techniques have attained lower PSNR of 42.12dB and 38.12dB respectively. Meanwhile, on image 3, the ABOA-QKIE system has offered superior PSNR of 64.78dB while the ECC and RSAmethodshave attainedlower PSNR of42.18dBand 37.15dBcorrespondingly. Eventually,onimage 6, the ABOA-QKIE system has offered maximum PSNR of 64.78dB while the ECC and RSA techniques have attained lower PSNR of 39.15dB and 37.12dB correspondingly.

Table3.PSNRanalysisofABOA-QKIEtechniquewithexistingalgorithmsundervarioustestimages

PSNR(dB)			
No.ofImages	**ABOA-QKIE**	**ECC**	**RSA**
1	65.35	42.12	38.12
2	65.35	44.15	35.14
3	64.78	42.18	37.15
4	62.29	40.18	36.52
5	64.78	39.15	37.12
6	Infinity	45.65	40.18

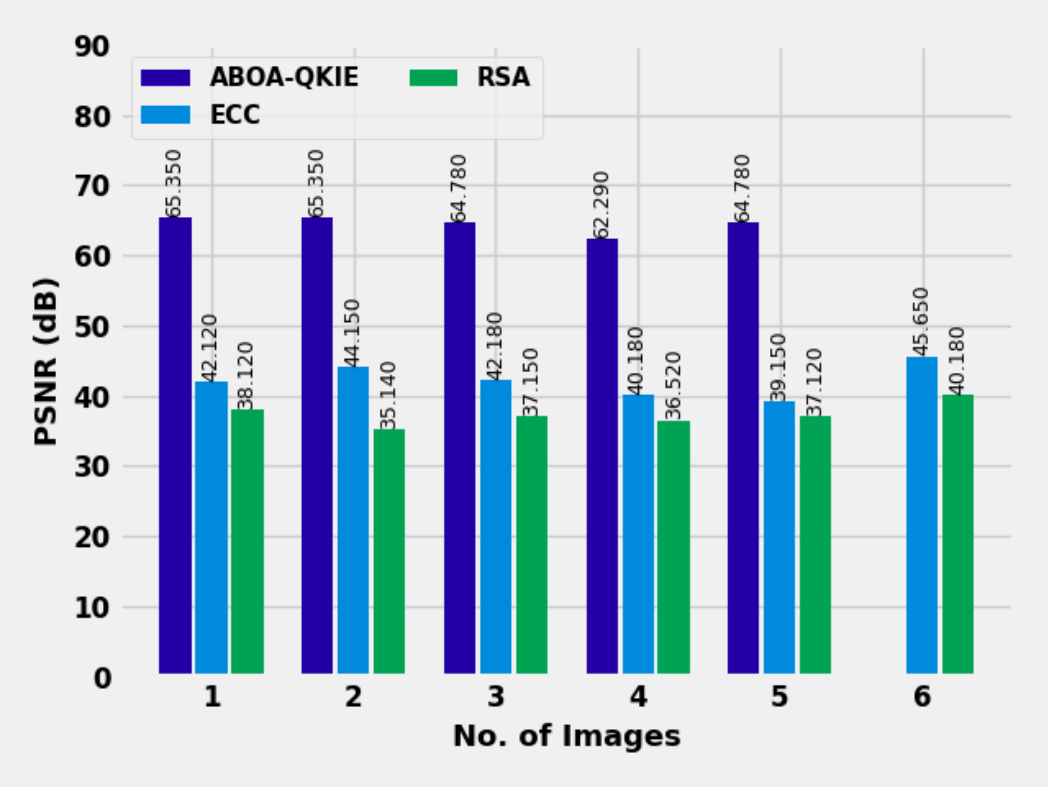

Fig6.PSNRanalysisofABOA-QKIEapproachunderdistinctimages

In Table 4 and Fig. 7, an overall ET inspection of the ABOA-QKIE system with existing techniques is studied. The obtained outcomes inferred the effectual characteristics of the ABOA-QKIE model with minimal ET values. For instance, with image 1, the ABOA-QKIE model has obtained least ET of 0.000149s while the ECC and RSA models have attained increasing ET of 0.0541s and 0.0615s respectively.

Table4.ETanalysisofABOA-QKIEtechniquewithexistingalgorithmsundervarioustestimages

EncryptionTime(sec)			
No.ofImages	**ABOA-QKIE**	**ECC**	**RSA**
1	0.000149	0.0541	0.0615
2	0.000149	0.0451	0.0741
3	0.000144	0.0215	0.0514
4	0.000097	0.0154	0.0451
5	0.000143	0.0154	0.0234
6	0.000053	0.0181	0.0512

Along with that, with image 3, the ABOA-QKIE system has achieved minimum ET of 0.000144s while the ECC and RSA models have attained increasing ET of 0.0215s and 0.0514s correspondingly. Meanwhile, with image 6, the ABOA-QKIE algorithm has attained least ET of 0.000053s while the ECC and RSA methodologies have attained improving ET of 0.0181s and 0.0512s respectively.

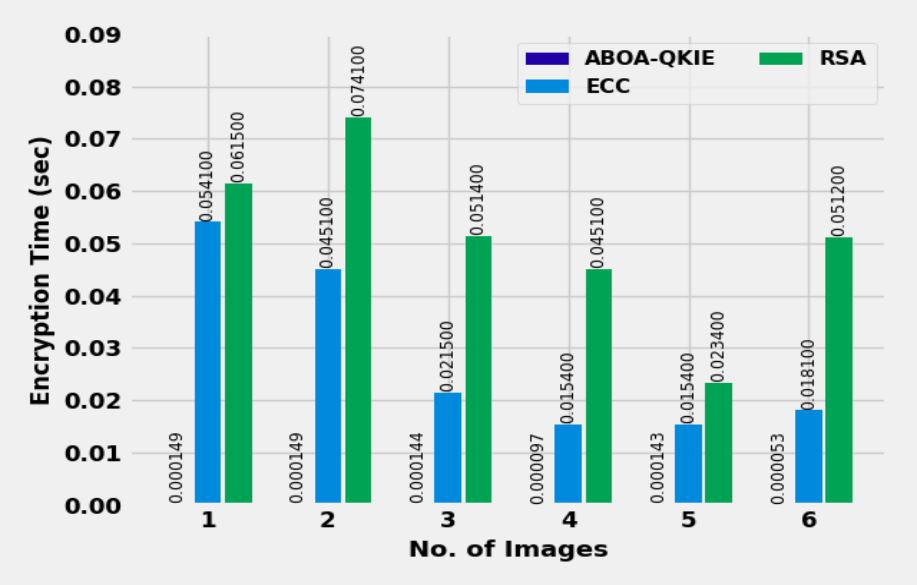

Fig7.ETanalysisofABOA-QKIEapproachunderdistinctimages

In Table 5 and Fig. 8, an overall DT examination of the ABOA-QKIE approach with existing techniques is studied. The attained outcomes inferred the effective characteristics of the ABOA-QKIE model with minimalDTvalues.Forinstance,withimage1,theABOA-QKIEsystemhasreachedlesserDTof0.000164s while the ECC and RSA techniques have attained maximum DT of 0.0201s and 0.0305s correspondingly. Besides, withimage3,theABOA-QKIEapproachhasobtainedminimalDTof0.000154swhiletheECCand RSA algorithms have obtained increasing DT of 0.0163s and 0.0342s correspondingly. In the meantime, with image 6, the ABOA-QKIE approach has attained decreased DT of 0.000207s while the ECC and RSA methods have gained increasing DT of 0.0160s and 0.0514s correspondingly.

Table5.DTanalysisofABOA-QKIEtechniquewithexistingalgorithmsundervarioustestimages

DecryptionTime(sec)			
No.ofImages	**ABOA-QKIE**	**ECC**	**RSA**
1	0.000164	0.0201	0.0305
2	0.000165	0.0167	0.0299
3	0.000154	0.0163	0.0342
4	0.000077	0.0171	0.0258
5	0.000152	0.0158	0.0368
6	0.000207	0.0160	0.0514

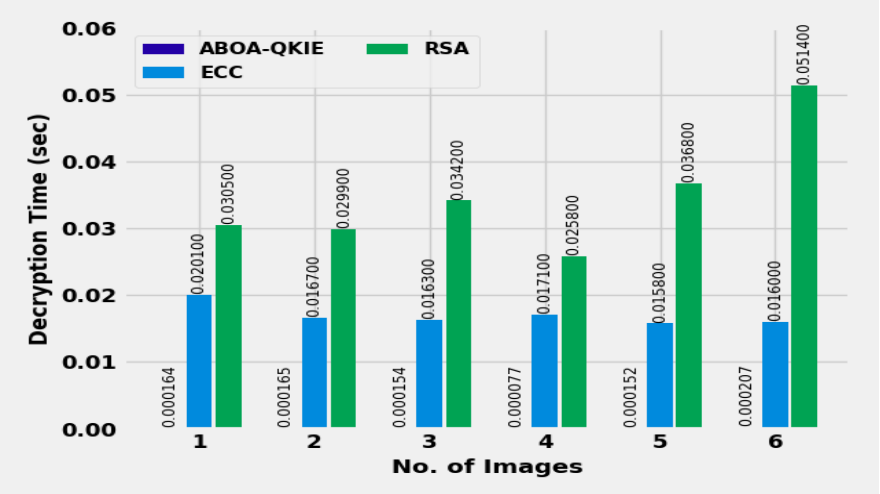

Fig8.DTanalysisofABOA-QKIEapproachunderdistinctimages

In Table 6 and Fig. 9, an overall error assessment of the ABOA-QKIE algorithm with existing methods is studied. The obtained outcomes inferred the effectual characteristics of the ABOA-QKIE system with minimal error values. For instance, with image 1, the ABOA-QKIE model has attained decrease error of 0.0190 while the ECC and RSA methods have attained higher errors of 0.0785 and 0.0912 correspondingly. Moreover, with image 3, the ABOA-QKIE model has achieved minimal error of 0.0216 while the ECC and RSA models have attained increasing errors of 0.1254 and 0.1312 correspondingly. Eventually, with image 6, the ABOA-QKIE algorithm obtained least error of 0.0000 while the ECC and RSA methods attained increasing error of 0.0421 and 0.0758 correspondingly.

Table6. ErroranalysisofABOA-QKIEtechniquewithexistingalgorithmsundervarioustestimages

Error			
No.ofImages	**ABOA-QKIE**	**ECC**	**RSA**
1	0.0190	0.0785	0.0912
2	0.0190	0.1055	0.1547
3	0.0216	0.1254	0.1312
4	0.0384	0.1112	0.1647
5	0.0216	0.1354	0.1451
6	0.0000	0.0421	0.0758

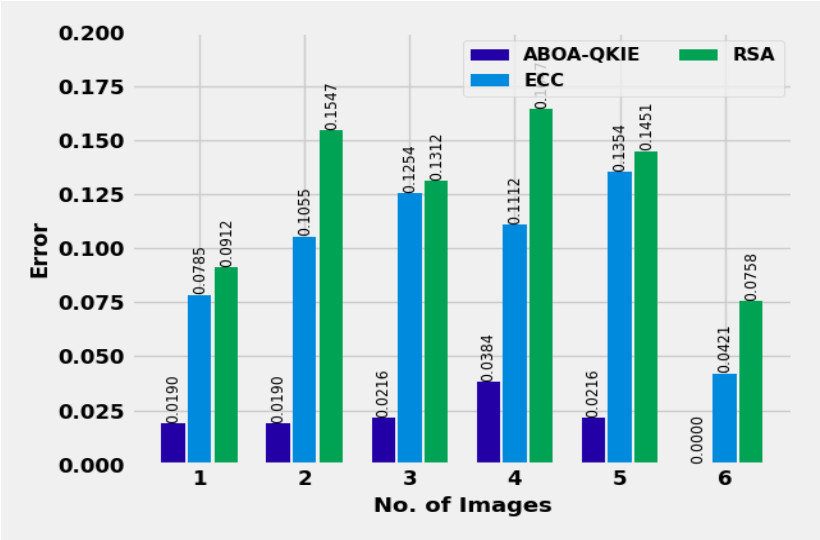

Fig9. ErroranalysisofABOA-QKIEapproachunderdistinctimages

Table 7 and Fig. 10 demonstrate a comparative CC investigation of the ABOA-QKIE system with other encryption techniques. The outcome referred that the ABOA-QKIE approach has gained increasing values of CC under all images. For instance, in image 1, the ABOA-QKIE algorithm has offered maximum CC of 0.9998 while the ECC and RSA techniques have attained lesser CC of 0.5000 and 0.6000 correspondingly. Also, in image 3, the ABOA-QKIE methodology has offered enhanced CC of 0.9998 while the ECC and RSA techniques have gained lesser CC of 0.7700 and 0.6800 correspondingly. Finally, in image 6, the ABOA-QKIE approach has offered higherCC of 1.0000 while the ECC and RSA techniques have attained lowerCC of 0.9100 and 0.8600 correspondingly.

Table7.CCanalysisofABOA-QKIEtechniquewithexistingalgorithmsundervarioustestimages

CorrelationCoefficient			
No.ofImages	**ABOA-QKIE**	**ECC**	**RSA**
1	0.9998	0.5000	0.6000
2	0.9998	0.6500	0.5500
3	0.9998	0.7700	0.6800
4	0.9998	0.6600	0.5600
5	0.9997	0.8800	0.7200
6	1.0000	0.9100	0.8600

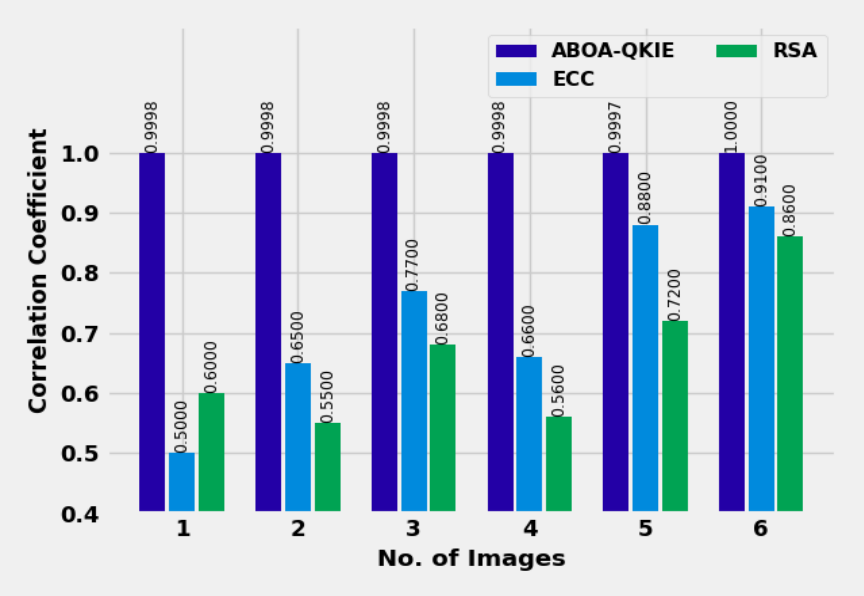

Fig10.CCanalysisofABOA-QKIEapproachunderdistinctimages

TheseresultshighlightedtheenhancedsecurityanalysisoftheABOA-QKIEapproachoverothermethods.

5.CONCLUSION

In this study, we have introduced a new ABOA-QKIE technique for image encryption process.The presented ABOA-QKIE technique accomplishes security in cloud environment via image encryption with optimal key generation process. Primarily, the ABOA-QKIE technique uses quantum key encryption approach to encrypt the input images. Besides, ABOA is applied for optimal key generation process and then the encryptedimages aretransmittedtothecloud server.Atthereceiving end,the encryptedimages are accessed from the cloud server and the quantum key decryption process takes place to retrieve the original input images. The experimental validation of the ABOA-QKIE technique is tested using a series of images and the results are inspected under different measures. Extensive comparison studies highlighted the improved performance of the ABOA-QKIE technique over other recent approaches. In future, image steganography techniques can be designed to improve the level of cloud security.

REFERENCES

[1] Pawar, H.R. and Harkut, D.G., 2018, August. Classical and quantum cryptography for image encryption & decryption. In2018 International Conference on Research in Intelligent and Computing in Engineering (RICE) (pp. 1-4). IEEE.

[2] Abidin, S., Swami, A., Ramirez-Asís, E., Alvarado-Tolentino, J., Maurya, R.K. and Hussain, N., 2022. Quantumcryptographytechnique:Awaytoimprovesecuritychallengesinmobilecloudcomputing (MCC). Materials Today: Proceedings, 51, pp.508-514.

[3] Srikanth, P. and Kumar, A., 2022. Secure Quantum Computing for Healthcare Sector: A Short Analysis. arXiv preprint arXiv:2211.10027.

[4] Santhiya Devi, R., John Bosco Balaguru, R., Amirtharajan, R. and Praveenkumar, P., 2019. A novel quantum encryption and authentication framework integrated with IoT. InSecurity, Privacy and Trust in the IoT Environment (pp. 123-150). Springer, Cham.

[5] Chennam, K.K.,Aluvalu, R.and Uma Maheswari, V., 2021.Data Encryption on Cloud DatabaseUsing Quantum Computing for Key Distribution. In Machine Learning and Information Processing (pp. 309-317). Springer, Singapore.

[6] Kacheru, G. (2018). Blockchain Technology: Architecture, Applications, and Challenges. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 9(3), 1433–1438.

[7] Farsana, F.J. and Gopakumar, K., 2020. Speech encryption algorithm based on nonorthogonal quantum state with hyperchaotic keystreams. Advances in Mathematical Physics, 2020.

[8] Li, H. and Pang, Y., 2021. FPGA-accelerated quantum computing emulation and quantum key distillation. IEEE Micro, 41(4), pp.49-57.

[9] Cavaliere, F., Mattsson, J. and Smeets, B., 2020. The security implications of quantum cryptography and quantum computing. Network Security, 2020(9), pp.9-15.

[10] Jagdale, S.K.S., 2019. Secure sharing of secret key on insecure channel using Quantum key distribution (Doctoral dissertation, Dublin, National College of Ireland).

[11] Liu, W.J., Xu, Y., Yang, C.N., Gao, P.P. and Yu, W.B., 2018. An efficient and secure arbitrary n-party quantumkeyagreementprotocolusingbellstates. InternationalJournalofTheoreticalPhysics, 57(1), pp.195-207.
[12] Kacheru, G. "Aipowered test automationframeworks: choosing the righttools." International journal of artificial intelligence & machine learning (IJAIML) 3.02 (2024): 110.
[13] Sasikumar, S., Sundar, K., Jayakumar, C., Obaidat, M.S., Stephan, T. and Hsiao, K.F., 2022. Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment. Simulation Modelling Practice and Theory, 121, p.102651.
[14] Sharma, G. and Kalra, S., 2018. Identity based secure authentication scheme based on quantum key distribution for cloud computing. Peer-to-Peer Networking and applications, 11(2), pp.220-234.
[15] Zhu,D.,Zheng, J., Zhou, H., Wu,J., Li,N.andSong, L.,2022. Ahybrid encryptionschemeforquantum secure video conferencing combined with blockchain. Mathematics, 10(17), p.3037.
[16] Yan, T. and Li, D., 2020, October. A novel color image encryption scheme based on controlled alternate quantum walks and DNA sequence operations. In International Conference on Machine Learning for Cyber Security (pp. 297-306). Springer, Cham.
[17] Sundar, K., Sasikumar, S. and Jayakumar, C., 2022. Enhanced cloud security model using QKDP (ECSM-QKDP)foradvanceddatasecurityovercloud.QuantumInformationProcessing,21(3),pp.1- 17.
[18] Abd El-Latif, A.A., Abd-El-Atty, B., Mazurczyk, W., Fung, C. and Venegas-Andraca, S.E., 2020. Secure data encryption based on quantum walks for 5G Internet of Things scenario. IEEE Transactions on Network and Service Management, 17(1), pp.118-131.
[19] Liu,G.,Han,J.,Zhou,Y.,Liu,T.andChen,J.,2022.QSLT:AQuantum-BasedLightweightTransmission Mechanism against Eavesdropping for IoT Networks.Wireless Communications and Mobile Computing, 2022.
[20] Wang, J., Geng, Y.C., Han, L. and Liu, J.Q., 2019. Quantum image encryption algorithm based on quantum key image. International Journal of Theoretical Physics, 58(1), pp.308-322.
[21] Rodrigues, D., de Albuquerque, V.H.C. and Papa, J.P., 2020. A multi-objective artificial butterfly optimization approach for feature selection. Applied Soft Computing, 94, p.106442.