International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-5, January 2020

Memory Based Hybrid Dragonfly Optimization for Multiple Key Generation using Cloud Computing

C. Kaleeswari, K. Kuppusamy

Abstract*: Cloud Computing, as a new technology with enormous computing services, evolved in recent era. It is a most promising computing that gives services on - demand. The Cloud services becomes a noticeable paradigm, by it notable features like, shared pool of resources, Shared infrastructure, dynamic provisioning, network access, handled assessing forward with gassed-up, gullibility, resilience and adoptable. Likewise, it has influence, Cloud Computing has some issues like security of data transferred via the Cloud, availability of resources and its authenticity, remains as a major task of attention. A Novel Optimized Encrytion-As-A-Service is presented in this paper, with multiple keys generation methodology. The three various Key generation includes, Pseudo Random Number Generator (PRNG), Sub-optimal keys are generated from hybridization of Improved Cipher Block Chaining (ICBC) encryption algorithm and final key is from Memory based Hybrid Dragonfly Optimization Algorithm (MHDA). In turn, MHDA is the combination of Dragonfly Optimization Algorithm (DA) and Particle Swarm Optimization Algorithm (PSO) for generating the innovative key for encryption of data. MHDA gives the better performance analysis compared with DA and PSO optimization approaches. The milestone of this optimized hybridization algorithm is to reduce the time complexity and increase the quality of encryption of the data. The experimental analysis is done for Text, image data and performance metrics are evaluated for the proposed research work. Different parameter that explores the main capacity and strength of the algorithm is examined.

Keywords* : Cloud Computing, MHDA, RGB Color Image, Authentication, ICBC Encryption, Decryption.

I. INTRODUCTION

Cloud Computing, as a new technology era leads to enormous computing services in recent years. Swift growth of the invention of cloud computing implies fascinates and alternative computing services amongst resource pooling, sharing and virtualization crafts. Considering the utilized cloud computing service model, the system incrporates the following cloud deployment models: public, hybrid, private and community. The main quality about cloud computing are summarization and virtualization whatever construct the technology to be observed and applied entirely in a various modes are compared with existing conventional sharing systems [2].

The modern trends in networking and the omnipresent of the internet have authorized the appearance of cloud computing as a wayable solution for a comfortable, flexible and frugal usage of services. Inspite of these obvious benefits, the cloud computing have some risks, challenges and vulnerabilities that are hinder its vast adoption, most of whatever associated to security and privacy. Cloud Computing providing number of advantages but the most of concerns are hesitated for agreeable it owing to security issues as well as challenges having with the cloud [3].

A lot of researchers invented a lot of proposed methodologies to protect the cloud user's data form unauthenticated approach in this cloud computing platform from the World. A convenient technique pavement path to oppose risks and challenges are cryptographic methods, authentication techniques and access control mechanisms [1].In this paper, the usage service is planned and examined as a security service. This advance alternative planning service is built in such a path that it provides encryption as a service to change plain text documents of various types as well as image data despite of its classifications in a strong way. This paper constructed as follows: Section1 contains basic overview on encryption process, optimization and cloud environment application services are provided. It is pinpointed with the literature review in this area at section 2.Section 3 elaborated as the proposed system with MHDA is briefly explained. Section 4 explores the experimental results for this paper. In final stage, the conclusion of the research is done in the section 5 is briefly explained in this area.

II. EXISTING WORK

Jyothika Chettiza & Nagendrakumar [8] observed expose the security issues and authentication mechanism in cloud platform. The authors proposed a MFA (Multi Factor Authentication) Mechanism for providing the additional layers of security and verification.S.C.Wang et.al[15]., developed a technique GKA (Group Key Authentication) protocol for reaching security along with the means of user's data in cloud computing. Punam V.Maitri and Aruna Verma [9], introduced hybridization technique for file security to store the cloud. The authors proposed in this research work done for combination of LSB steganography technique, AES, RC6, Blowfish and BRA Algorithm. D.Ranjith and Srinivasan [2], observed the identity security using authentication and authorization in cloud computing.

Manuscript received on December 10, 2020.
Revised Manuscript received on December 20, 2020.
Manuscript published on January 30, 2020.
* Correspondence Author
C. Kaleeswari*, Dept. of Computational Logisticshis, Alagappa University, Karaikudi, India. Email: kalees94chinna@gmail.com
K. Kuppusamy, Dept. of Computational Logistics**,** Alagappa University, Karaikudi, India. Email: kkdiksamy@yahoo.com
Third Author Name, department, Name of the affiliated College or University/Industry, City, Country. Email: xyz3@blueeyesintlligence.org

J.Mahalakshmi and K.Kuppusamy [10] developed a new structural framework for security services offered in cloud using files. Every proposed technique has the advantages and disadvantages, but the purpose of research work will provide a much better secured approach along with other existing methods.JyothiVaishnav[4],have been credited for the data safety & effectiveness estimation in cloud computing using CCAF.Mahalakshmi Jeyabalu and Kuppusamy Krishnamoorthy[1], taken over the credits on the hybridization of ICBC and genetic algorithm for optimizing encryption process in cloud computing. M.Tanooj Kumar,Dr.M.Baby Reddy[9], proposed the method used to perform data/signal capturing ,its compression and encryption at the same time.Sree Ranjini K.S. and S.Murugan[6],discussed to the new approach MHDA optimization for solving the numerical optimization operations.Experimental outcome of this research work is to provides the exceptional work to compare with DA and PSO. Naveen Sihag[7],proposed a Novel Adaptive Dragonfly Mechanism to attend through fast assisting and optimized global results depend with few parameters. Kawser Wazed Nafi et.al[11], proposed a innovative Authentication scheme for encrypting the files and sharable Cloud Computing secure Framework.

III. PROPOSED SYSTEM

A novel hybrid encryption approach is designed and verified in this research work. Symmetric key encryption is placed for designing, for which both the consigner and consignee administer the same key for encryption and its reverse process. Key generation is the most important and influential part that indicates the strength of the algorithm and quality of encryption. Throughout the implementation process in this research work, a consistent design rationale is followed so as to maintain uniformity as well as to perform in rapid manner. This area briefs the newly developed cryptographic algorithm and its performance analysis, the optimization results after the encryption of the text and overview of the algorithm. It also describes the encryption and hiding of the data by using the Improved cipher Block Chaining (ICBC) Encryption Algorithm and the Memory based Hybrid Dragonfly (MHDA) Optimization algorithm. Their performance parameters are analyzed. Also, the A Novel Encryption-As-A-Service is delivers in this research work, with multiple keys encryption methodology. The three various Key generation includes, PRNG, Sub-optimal keys are generated from hybridization of Improved Cipher Block Chaining (ICBC) encryption algorithm and final key is from Memory based Hybrid Dragonfly Optimization (MHDA) Algorithm for text encryption.

3.1 PSEUDO RANDOM NUMBER GENERATORS

PRNG indicates as a mechanism that utilized as mathematical preliminaries to build generation of Random values. It concern with cluster of Analytical Assessment. Every bunch of sequence has the initial point. So, if the initial point is established, a lot of odd numbers are generated in the minimum period of time consumption. The outcome of this algorithm generates the values are ultimate and adequate.

In each iteration, the PRNG increasing the parameters value , looks up the exchanges the values of the parameters. XOR operation involves in this key generation to produce the next byte stream for this process.. Each and every element Each element of this algorithm swapping the numbers in 256 iterative process.

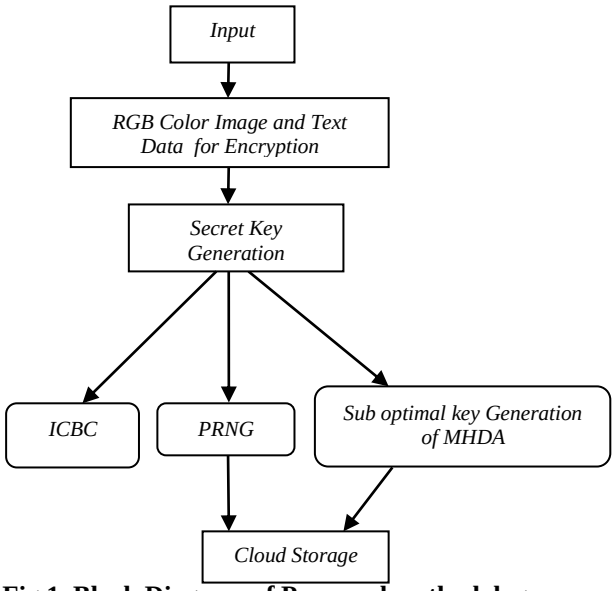


Fig.1. Block Diagram of Proposed methodology

3.2 IMPROVED CIPHER BLOCK CHAINING ALGORITHM

The state of art holds number of application services that concentrated either for the text and image data. Considering this into account the developed algorithm is designed as a complete application service that encrypts the text, executable files, Portable format files, documents etc despite of the type. Another interesting feature about the constructed application of M.Jeyabalu and K.Krishnamurthy[1], Hybridization of ICBC and the proposed methodology MHDA for Optimizing Encryption service is its key generation. The size of the key varies as 64-bit, 128-bit, and 256-bit, whereas in the conventional types any one of the key size is utilized. This unique feature of the developed application archetype makes it better suitable for the encryption of the data. Most strong component of this proposed scheme is the sub-optimal key generation that makes the entire process more secure as well as increases the speed of execution. The proposed algorithm is the hybrid model, which consists of the basic cipher block chaining encryption operation. The design rationale followed throughout the encryption process is depicted. Each and every data element is converted into its corresponding binary bits that pilot to decrease in the execution time. Moreover, processing as binary bits makes the scheme more complex, since a single bit error leads to major destruction.

3.3 Memory Based Hybrid Dragonfly Algorithm (MHDA)

Memory based Hybrid Dragonfly optimization is a recent approach for generating the innovative key in this research work is to improve the security and privacy to the multimedia data like text and image. In this paper implements one objective function for this optimization and implement it in MATLAB. It provides the outcome of this work is global optimal solution.The contributed encryption algorithm works well for the file encryption also. The file type includes varied files namely executable files, portable format files, text files, word documents etc with higher security.

The working procedure of the file encryption remains as same as the text data encryption.The content of the files are converted into binary blocks, despite of its original format and dragged to a text document. This is an additional step taken place in this file encryption.

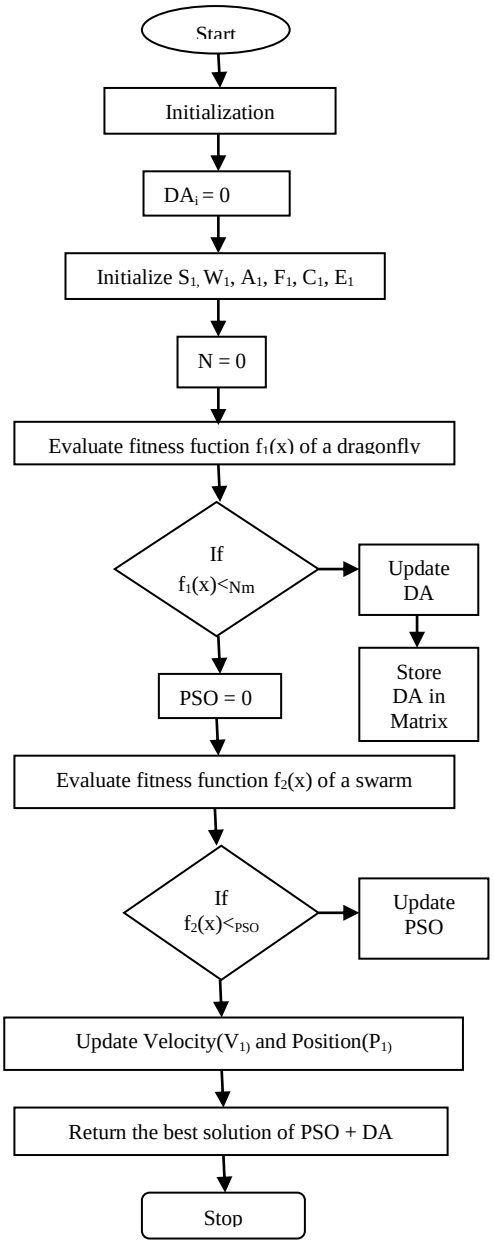


Fig. 2. Flowchart of MHDA

Once the data is converted and moved to the text document, the working procedure of the text data encryption process is taken place automatically. Again, in the decryption process, the ciphered data is placed in the text file and the decryption takes place. In the case of link files, library files or an image data the result available as corrupted information for the encryption.The combination of logical substitution operations along with the complex key generation makes the cryptographic process, a new hybrid encryption algorithm. The logical Exclusive Disjunction operator (XOR) is used for the substitution process. It is a self-invertible operator hence it is employed for this symmetric key encryption method. The ICBC encryption operation mode is involved where the blocks are encrypted in clusters.Multiple keys are involved in the encryption process to make the algorithm strengthen and toughen the keys. When number of keys is increased the encryption code automatically will get strengthened.Moreover, the key generation is from the input data itself, which makes it complex to retrieve. Additionally, a sub-optimal key is generated and involved for the encryption makes the process so difficult, that the intruder cannot hack the data. The authorized receiver, with proper accessibility through the key will decrypt the file.

The conversion of data into binary blocks and decreases the execution time. The optimization technique will appropriately increase the execution speed as well as the decreases the storage space. Since the algorithm is designed for the application service, to be mounting to the cloud, the space complexity is a severe issue to be considered. Hence, by converting the data as to binary blocks saves more space and also the computation on this blocks structure will leads a foremost demolition if any error found. The approximate size of the block for the proposed model is from 8 X 8; extended up to 256 X 256 bits and that of the key size varies from 64 to 256 bits.

3.5.1 Algorithm for Encryption Process

Step 1: Initially,the input data converted into binary data will be fill in a Eight X Eight matrix format.
Step 2: The ICBC encryption Algorithm for encrypting the given input Text then generate the key for data security.
Step 3: One more Key matrix is generated via the PRNGs Cryptographic Algorithm.
Step 4: The next key generation is the most important key that is constructed as a Sub-optimal key to obtain the optimized key for the encryption.
Step 5: The Sub-optimal key is generated from the MHDA algorithm with the procedure followed.
Step 6: The size of the key values are in three various sizes either as a 64 – bit, 128 - bits or 256 - bits: If the size of the key is 64; the block size designed as 8 X 8; if it is 256 then the block size is 16 X 16; where the key size is of 128 the block 8 X 16.
Step 7: The blocks with the binary elements are repeatedly tranferred to corresponding ASCII code.
Step 8: Detaching the blocks will yields the encrypted text data.

Algorithm for Decryption Process

Step 9 : File that contains the encrypted text data is taken as input
Step 10 : Convert the encrypted data into equivalent binary bits:
Step 11 : Fill the matrices of 8 X 8 with the converted ciphered binary bits yet the end is reached.
Step 12 : Reverse is the process of encryption; along with the key generation.
Step 13 : The key is similar since the symmetric key scheme is followed.
Step 14 : The deciphered; original text data is obtained as the result of the key Generation.

IV. EXPERIMENTAL RESULTS

The experimental results obtained from the proposed technique for data encryption are presented below. The implementation is done with the Visual Studio 2010, C#language under the configuration of windows 7 operating system with Core-i5 and 3 GB RAM. The optimization is implemented with MHDA Objective Function in MATLAB- R2018 Version. The key size and block size varies from 64-bits, 128-bits and 256-bits and the results based on various parameters are analyzed. The time factor of this process is the main factor described in this text encryption section.

Table - 1: Encryption and Decryption of varied Size Text Data

Key size (in bits)	File Size (in bytes)	Input Text Data	Encrypted Data	Decrypted Data
64- bits	442 bytes	on-2015-105009.pdf Title: A New Cryptosystem MKE: Multiple Key Encryption Algorithm with Cipher Block Chaining And Logical Operator	wJyTwNyXwZyfwVyHw1 y3wRyXwdybwFy38.+78.+ 7wRyzwd+n85+n85yXwZ2 vwZyb8.+78.+7k52Tk.mX kxmXkhmXk9ifkxmnk1+n 85+n85+n85ubkxiHgJmXk pmXsRyPwZyTwVyL	on-2015-105009.pdf Title: A New Cryptosystem MKE: Multiple Key Encryption Algorithm with Cipher Block Chaining And Logical Operator
128-bits	13400 bytes	Each manuscript must include a 200-word abstract. The acceptance rate of the journal is 10%. Articles are accepted only in MS-Word format----------19424724823 0231232 233	4N+z8Jmbk1mv8J6P4J+z4 N6L4J6X816v4V6r896r4N +/4F6D4B+/4B6D4R6r896 Dg16P4R+L-92j--------8d+/ 8Jyvwx+T8J+Hwtyz8R+L8 5yvwx+T8V+bwtyz8R+X8 dyvwx+T8V+Twtyz8R+X8 V	Each manuscript must include a 200-word abstract. The acceptance rate of the journal is 10%. Articles are accepted only in MS-Word format----------194247248230231 232 233
256- bits	344064 bytes	()*&^%$#Alagappa0987654 3!@#$%^&* 19424724 R%$)*%&$ 3-319-25207-0_20---------- ---	|*n♥╖©rwb↔◄^♥6_5♠╣◊ ◘◄-♥/♥◙♠▲ ▌-52/-x2D8d +/8Jyvw4J6P4F6345 4B6D4R6r896Dg16P4R+L -92j----------	()*&^%$#Alagappa09876543!@# $%^&* 19424724 R%$)*%&$ 3-319-25207-0_20----------

Table - 2 : Encryption and Decryption of varied Text Files of Various Key Sizes with Time Factor

Key Size (in Bits)	File Size (in bytes)	Encryption Time (in ms)	Decryption Time (in ms)
64-bits	126000	0.361	0.261
64-bits	133000	1.488	1.488
64-bits	4530	0.0058	0.0056
64-bits	85300	0.0316	0.0244
64-bits	1460000	3.619	3.718
128-bits	126000	0.226	0.251
128-bits	133000	0.223	0.025
128-bits	4530	0.0034	0.0030
128-bits	85300	0.0716	0.0744
128-bits	1460000	2.513	2.698
256-bits	126000	0.0028	0.0031
256-bits	133000	0.0029	0.0029
256-bits	4530	0.0003	0.0002
256-bits	85300	0.0685	0.0623
256-bits	1460000	2.178	2.221

Table - 3 : Filewise Encryption and Decryption with Time Factor

File Type	Key size(in bits)	File Size (in bytes)	Encryption Time (in ms)	Decryption time (in ms)
.docx	344064	64-bits	0.661	0.691
.pdf	16193207	64-bits	4.925	4.711
.avi	4429952	64-bits	6.994	6.85
.exe	14848	64-bits	0.071	0.056
.dll	1074688	64-bits	1.844	1.964
.docx	344064	128-bits	0.542	0.545
.pdf	16193207	128-bits	3.907	2.296
.avi	4429952	128-bits	5.944	5.637
.exe	14848	128-bits	0.068	0.074
.dll	1074688	128-bits	1.445	1.646
.docx	344064	256-bits	0.578	0.51
.pdf	16193207	256-bits	2.016	1.68
.avi	4429952	256-bits	3.618	3.145
.exe	14848	256-bits	0.005	0.005
.dll	1074688	256-bits	1.408	1.487

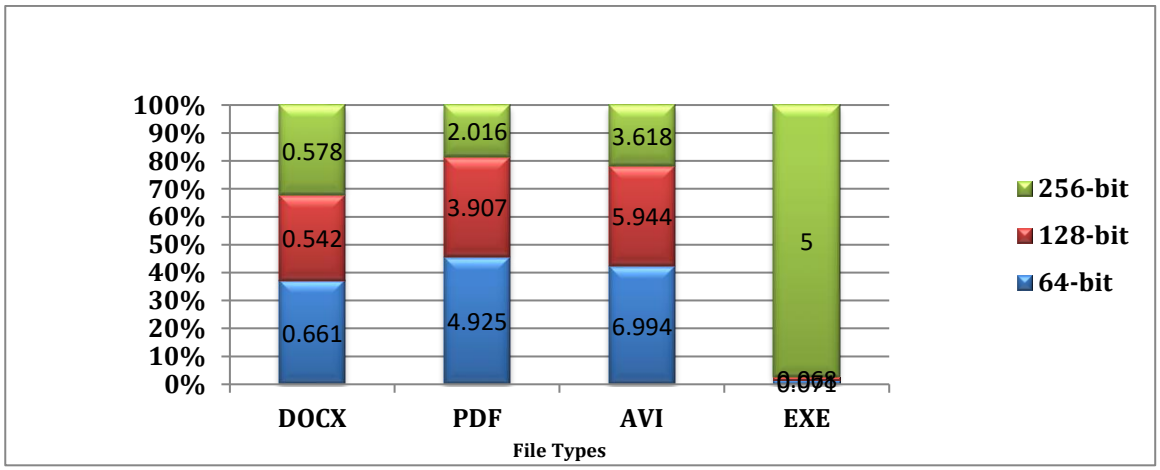
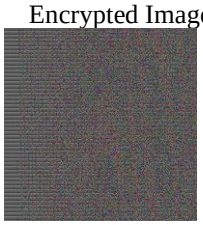


Fig.3. Comparative analysis of the proposed Text Cryptosystem

IMPLEMENTATION OF RGB COLOR IMAGE CRYPTOSYSTEM

In this section, the RGB Color Image encryption is depicted various standard image namely the Lena, Water,Pueblobonito, Baboom, and Barbara are taken for the experiment verification. A key size varies between 64-bit, 128-bit and 256-bits. From above-listed images the Lena, Water images are encrypted using 64-bit key. The Baboon, pueblo bonito is encrypted via 128-bit key size, and Barbara, Brandy.rose images are encrypted using 358-bit key size. The experimental results were shown in the below:

Key size	Pixel Resolution	Input Image	Encrypted Image	Decrypted Image
64- bits	256 x 256			

4.1 (a)Lena Image (b) Encrypted (c) Decrypted

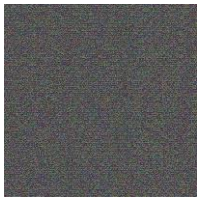
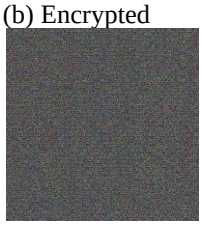
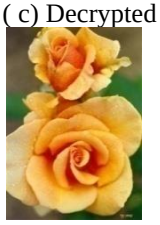
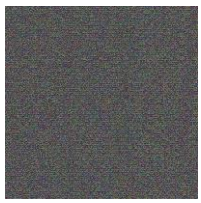
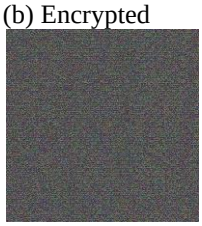
64- bits	256 x 256			
		4.1 (a) Water Image	(b) Encrypted	(c) Decrypted
128 -bits	256 x 256			
		4.3 (a) Brandy Rose Image	(b) Encrypted	(c) Decrypted
128- bits	256 x 256			
		4.4 (a) Pueblo Bonito Image	(b) Encrypted	(c) Decrypted
256- bits	256 x 256			
		4.5 (a) Bandon Image	(b) Encrypted	(c) Decrypted
256- bits	256 x 256			
		4.6 (a)Opera Image	(b) Encrypted	(c) Decrypted

Fig.4 . RGB Color Image Encryption using the Proposed Encryption Algorithm

The images are taken from the standard sources Standard pixel resolution for the experiment verification is 256×256. Various image types are verified and the results are analyzed. The performance factors were experimentally analyzed for different categories of image data like the bitmap, jpeg, Tiff images. These type of data are encrypted using three key sizes as 64 bits, 128 bits, and 256 bits. The standard pixel resolutions for the images are set as 256×256 pixels. The proposed encryption algorithm remains with better solution for the images of many types and their quality are analyzed using different parameters. The main factors considered here are the security analysis parameters PSNR, entropy measure, and statistical analysis, differential attacks measures namely the NPCR and UACI.

Entropy is the measure used to verify the encryption quality that measuring the randomness of the given algorithm. The entropy value should possess to the ideal value of 8 that shows the proposed algorithm is resistant against various attacks. The measuring unit of entropy is Shannon (Sh) that describes the unit of information between two images. In the given equation 1 below, P(mi) denotes the probability of the entropy and the total states of the information source. For a purelyrandom source emitting, the entropy should be M. The PSNR expresses the ratio between maximum possible values to that of the noise that affects the quality of an image as in equation 2. In scenario of encryption lower the PSNR indicates, better encryption standard.

$$E=\sum [(pi)X\log2(1/p(mi)\ )\ ] \quad (1)$$

$$PSNR=20\log10[MAX/\sqrt{\ }MSE] \quad (2)$$

By calculating the variations betwixt the encrypted image and the given image (original) of pixel values are statistically evaluated. The two major measurement units of widely used NPCR(Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity Eq.3, 4) that are utilized for evaluating the slight changes betwixt the given image and the converted image (Encrypted image).

$$NPCR=\frac{1}{MxN}\sum_{I=1}^{M}\sum_{J=1}^{N} D(i,j)X100\% \quad (3)$$

$$UACI=\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j)|}{255}X\frac{100\%}{MxN} \quad (4)$$

Where M;N denotes the dimension of the image and (i; j) stands for the image co-ordinates. Theresults computed from the encryption algorithm, for NPCR and UACI in Table 5, indicates that themethod provided for encryption of various type of images serves better for encryption. Hence, thegiven method is strongly capable of resisting the differential attack. A good cipher should also be ableto tolerate a certain amount of noise. PSNR (Peak Signal Noise Ratio) values are experimented andanalyzed for the proposed encryption algorithm. Histogram Analysis is the measure of approximatedby a uniform distribution.From the above depicted table it is clear that the encryption of RGB images with the aid of 256-bitkey yields better results in all the parameters. According to the UACI value, the 256 bit key encryptionshows good output .The PSNR values remains very low that indicated the quality of this proposed algorithm is high.

This Research work is to develope a innovative mechanism for encrypting the data is to produce the better result for various categories of images. Some are represented in the table. The entropy value is nearest to the optimal value of 8 that shows the quality of the encryption is high.

Table - 4 : Comparative Analysis of RGB Color Image Cryptosystem

Parameters	Image Name (256 X256)	Existing Method-RCBC	Hybrid ICBC and novel MHDA proposed Method
NPCR(%)	Lena	78.4	98.89
UACI(%)	Lena	31.2	32.9
Entropy(sh)	Lena	7.926	7.999

.2.2 Entropy

The main aim of the cryptanalysts is to enhance the security in every possible aspect using available tools. The cryptool is vastly used simulator tool, to analyze randomness test and analysis test. This tool consists of inbuilt mechanisms for test and analysis for the output provided. The following analyses were done using cryptool. Frequency test basically calculates the uniform distribution of the values that are generated from the pseudorandom number generators [20]. It identifies the deviations taken place from a one-dimensional uniform distribution. The number of Binary values (0,1) in the sequence is evaluated called as Mono-bit test, with the equation, The following analyses were done using cryptool. Frequency test basically calculates the uniform distribution of the values that are generated from the pseudorandom number generators [20]. It identifies the deviations taken place from a one-dimensional uniform distribution. The number of 0s and 1s in the sequence is evaluated called as Mono-bit test, with the equation

$$x_1 = ((n_0 - n_1))\hat{}2)/2$$

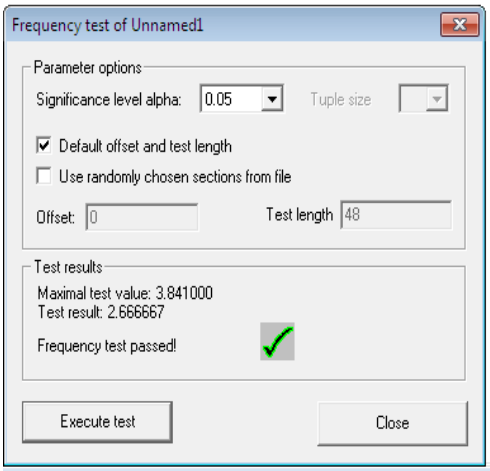


Fig.5. Entropy analysis for the Encrypted Text using Proposed Encryption Algorithm

Table 5 : RGB Color Image Encryption with Time Factors

Image (Size)	Key Size	Encryption Time (in ms)	Decryption Time (in ms)	PSNR	NPCR	UACI	Entropy (Sh)
Lena (256 X 256) BMP	64-bits	8.948	9.147	29.187	99.87	30.41	7.999
	128-bits	7.137	9.112	28.876	99.86	33.40	7.999
	256-bits	8.934	7.186	27.215	99.89	33.41	7.999
Lena (256 X 256) JPEG	64-bits	9.961	6.202	28.954	99.12	32.17	7.999
	128-bits	8.096	9.208	28.483	99.43	33.01	7.999
	256-bits	7.142	6.945	24.728	99.67	32.19	7.999
Lena (256 X 256) TIFF	64-bits	8.091	7.197	23.152	99.47	26.14	7.999
	128-bits	7.754	8.754	25.702	99.76	32.10	7.999
	256-bits	6.971	7.941	26.973	99.67	33.41	7.999
Opera (256 X 256) BMP	64-bits	3.259	1.907	26.823	99.19	33.14	7.999
	128-bits	3.687	1.911	24.215	97.56	32.10	7.999
	256-bits	2.696	2.235	25.750	98.91	29.08	7.999
Opera (256 X 256) JPEG	64-bits	3.191	2.180	28.879	99.61	33.13	7.999
	128-bits	3.073	2.095	26.483	99.78	33.40	7.999
	256-bits	2.986	2.703	27.748	99.01	33.17	7.999
Opera (256 X 256) TIFF	64-bits	2.885	1.806	29.452	99.14	30.14	7.999
	128-bits	3.535	2.037	25.902	93.62	30.17	7.999
	256-bits	2.100	1.118	26.063	99.46	33.1	7.999
Bandon (256 X 256) BMP	64-bits	3.458	2.377	26.823	92.13	33.40	7.999
	128-bits	3.073	2.095	29.215	99.34	26.57	7.999
	256-bits	2.798	3.491	26.156	99.89	26.37	7.999
Bandon (256 X 256) JPEG	64-bits	3.338	2.936	28.879	99.49	33.40	7.999
	128-bits	3.687	1.886	26.983	99.87	33.40	7.999
	256-bits	3.427	3.690	27.245	99.67	33.40	7.999
Bandon (256 X 256) TIFF	64-bits	2.849	1.387	29.103	99.25	26.37	7.999
	128-bits	2.635	2.019	29.209	93.90	26.57	7.999
	256-bits	2.514	2.081	26.452	99.64	33.17	7.999

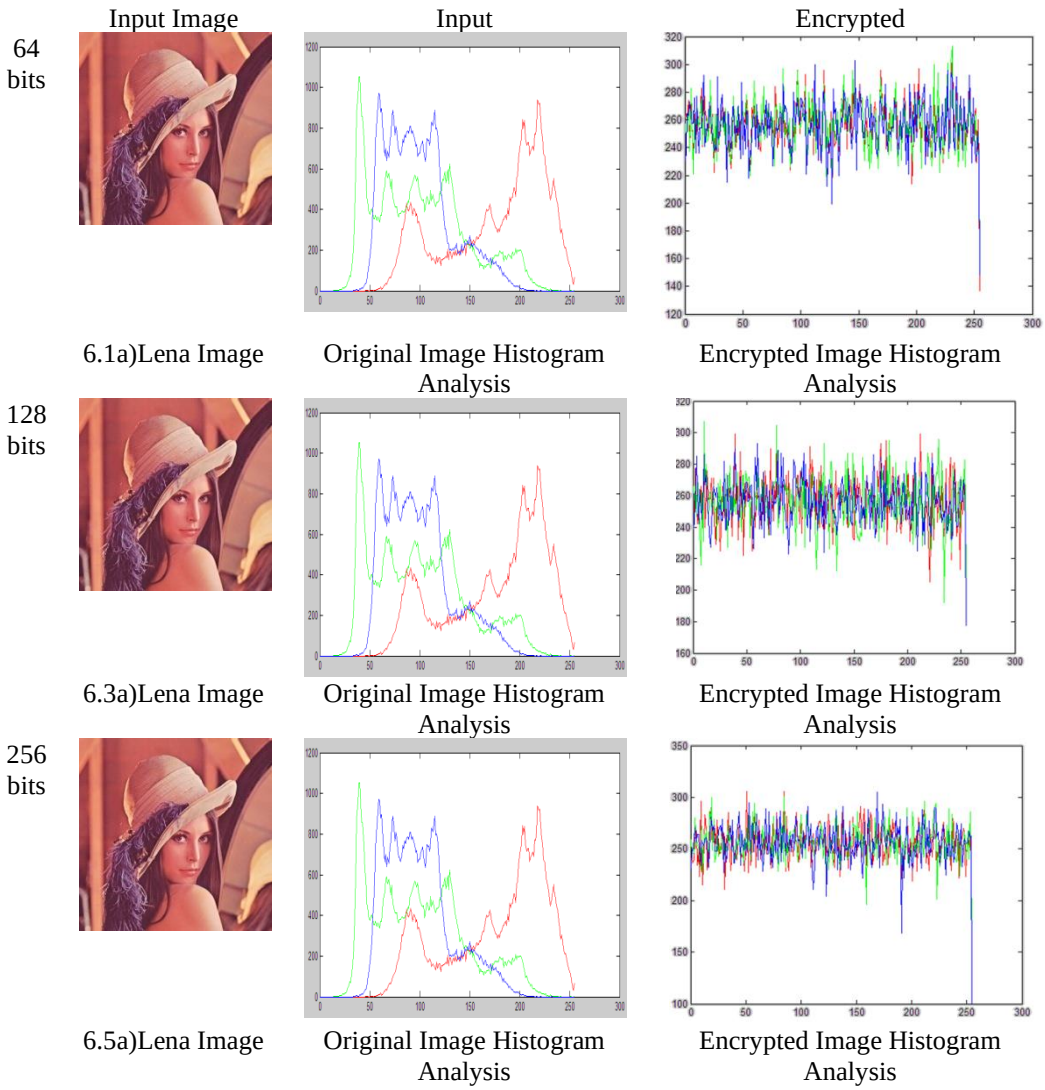


Fig. 6 .Histogram Analysis for the Original and Encrypted Image

V. CONCLUSION

A novel hybrid algorithm is designed and verified with various experiments in this Research work that improves the encryption strength. The conventional encryption operation mode cipher block chaining is considered into account, modified and presented as the ICBC Encryption mechanism, which in turn combined with the MHDA optimization technique for the key generation. One interesting feature of this proposed algorithm is, the suboptimal key generation from the MHDA makes the process computationally hard.

Throughout the application service, a consistent design rationale is followed that increases the execution speed. Specifically, it offers the key sizes in three different strengths and also allows the privilege to the deployment of a client to select the way of encryption and form of data as per their wish. This research work is shows the proposed encryption algorithm achieves first objective, minimum time for execution. In cloud computing, space complexity is prominent issue; it is almost minimized with the second objective storage space reduction by converting the contents to binary bits. Hence, in cloud computing this hybrid ICBC technique with Memory based Hybrid Dragonfly Algorithm encryption security service yield better solution for encryption services to the users.

ACKNOWLEDGMENT

This research work is financially supported by RUSA 2.0. The author of this research work expresses deep sense of gratitude to Ms. Sree Ranjani Kizhakethil, Homi Bhabha National Institute, Indra Gandhi Centre for Atomic Research (IGCAR), India for her helpful and constructive suggestions regarding the MHDA to carry out this research work.

REFERENCES

1. MahalakshmiJeyabalu,KuppusamyKrishnamoorthy, ”Hybridization of ICBC and Genetic Algorithm for Optimizing Encryption Process in Cloud Computing Application Service”, in FundamentaInformaticae 157(2018)79-109,DOI:10.3233/FI-2018-1619.
2. D.Ranjith,J.srinivasan, “Identity Security Using Authentication and Authorization in Cloud Computing” in International Journal of Computer & Organization Trends ,vol:3,Issue:4,ISSN:2249-2593,May 2013.
3. VarshaD.Mali,PramodPatil, “Authentication and Access Control for Cloud Computing Using RBDAC Mechanism”, in International journal of Innovative Research in Computer and Communication Engineering,vol:4,

4. Issue:11,DOI:10.15680/IJIRCCE.2016.0411009,Nov 2016.
5. JyothiVaishnav ,“ Data Safety and Effectiveness Estimation in Cloud Computing using CCAF” in International Journal of Computer Science and Information Technology,Apr 2018.
6. M.Tanoojkumar,Dr.M.BabuReddy,”Cloud Storage Optimization Approach Using Compressive Sensing”, in International journal of Engineering Research and Development,e-issn:2278-067X,p-issn:2278-800Xvol:14,Issue:2,pp:21-26,Feb 2018.
7. SreeRanjini and K.S.,S.Murugan,”Memory Based Hybrid Dragonfly Algorithm for Numerical Optimization Problems”, in Elsevier Expert Systems with Applications,2017.
8. Naveen Sihag., “A Novel Adaptive Dragonfly Algorithm for Global Optimization Problems”, in International Journal of Engineering Research and Development,e-issn:2278-067X,p-issn:2278-800X,Vol:14,Issue:2,pp:27-39,Feb 2018.
9. JyothikaChettiza&Nagendrakumar,”Emerging security issues and Authentication Mechanism in cloud environment with focus on Multifactor Authentication “,in IJARCSSE International Journal of Advanced Research in computer science and software engineering,Vol.6,Issue 5,May 2016,ISSN:2277 128X.
10. PunamV.Maitri, Arunaverma,”Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm”, in IEEE explore on WisNETconference,Sep 2013,DOI:10.1109/WisPNET.2016.7566416.
11. J.MahalakshmiandK.Kuppusamy,”Security-As-A-Service for files in Cloud Computing-A Novel Application Model”,IEEEDigitalexplore,DOI:10.1109/ISCO.2016.7726889,Nov 2016,pp:1-5.
12. Kawserwazed naïf et.al.,”A Newer User Authentication File Encryption and Distributed Server based Cloud Computing Security Architecture”, in (IJACSA) International Journal of Advanced Computer Science and Applications,Vol.3,No.10,2012.

AUTHORS PROFILE

C. Kaleeswari, is pursuing Ph.D in Computer Science in the Department of Computational Logistics, Alagappa University, Karaikudi. Her Research Interest is Information Security, Cloud Computing and Big Data Analytics.

Dr. K. Kuppusamy, is working as Professor & Head (i/c) , Department of Computational Logistics, Alagappa University, Karaikudi, Tamilnadu, India. He received his Ph.D in Computer Science and Engineering from Alagappa University, Karaikudi, Tamilnadu in the year 2007. He has 32 years of teaching experience at PG level in the field of Computer Science. He has published many papers in International & National Journals and presented in National and International conferences. His areas of research interests include Information/Network Security, Algorithms, Neural Networks, Cloud Computing, Software Engineering and OptimizationTechniques.