IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, Apr 2019 E-ISSN: 2347-2693

Investigation of Efficient SKC Cryptic Algorithm for Image Encipherment and Decipherment Using SMCrypter

Shivlal Mewada[1*], Pradeep Sharma[2], SS Gautam[3]

[1]Department of Physical Sciences (Computer Science), MGCGV, Chitrakoot, Satna, (M.P), INDIA
[2]Department of Computer Science, Govt. [Autonomous] Holkar Science College, Indore (M.P), INDIA
[3]Department of Physical Sciences (Computer Science), MGCGV, Chitrakoot, Satna, (M.P), INDIA
**Corresponding author: shiv.mewada@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i4.12201226 | Available online at: www.ijcseonline.org

Accepted: 06/Apr/2019, Published: 30/Apr/2019

Abstract- Without image data security, number of problems arises with the security of different image data files, important data and security is required to send and store on cloud with assurance of confidentially, integrity and authenticity of information over the internet, in public or local networks. Image security has become a critical issue, and is playing a vital role in the domain of network communication system and web. So, there is always a need to have a method to guard the confidentiality, integrity and authenticity of images and avoid the unapproved access of image data over insecure communication environment. Various techniques have been investigated and developed to protect data and personal privacy like cryptic algorithms so far. Cryptic algorithms play a vital role in providing the information security against malicious attacks. It is challenging stuff for researchers to find out more efficient and accurate symmetric block cipher cryptic algorithm for image enciphering and deciphering, and to implement cryptic algorithm. There are many research institutes working on block cipher cryptic algorithm for secure data communication web in the form of digital images like; JPEG/JFIF, BMP, PNG TIFF, GIF, Exif, PPM, PNM, HEIF, PGM, PBM, BAT, BPG. In this paper, presents performance analysis of various symmetric algorithms and investigate of more efficient, confidential and secure symmetric block cipher cryptic algorithm for image encryption and decryption, against cryptanalysis attacks using SMCrypter tool.

***Keywords*:** Block Cipher, SKC Algorithms, Cryptosystem, Image, Encipherment, Decipherment, Statistical Analysis, SMCrypter

I. INTRODUCTION

Encryption and decryption are a regular method to uphold digital image security. Image and video encryption/ decryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication.

Image security is one of the peak challenging problems in current era of technological world. There are already various techniques for protecting confidentiality of image, from hackers and malicious attacks. Some are biometrics, passwords, cryptography and steganography. Traditional passwords aren't so good for this job due to their low entropy. Biometrics methods produce harmful effects on the human body (beings) and it is more costly. For these above discussed problems, Steganography combined with cryptography techniques, can be one of the best choices for solving the problem of information security on network or web. The main goal of cryptography (fig.1, fig.2) is keeping data secure from unauthorized users.

Cryptic [1] method has a long history to store sensitive digital information or transmit it across insecure web (internet, in public or local networks.) so that it cannot be read by anyone except the intended recipient, where the crypto method is a set of several algorithms combined with keys to convert the plain-text to cipher-text (hidden image/ data) and convert it back in to intended recipient side to the original message. Information cryptography mainly is the scrambling of the content of information, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. There are two general categories for key based encryption algorithm first one is called symmetric algorithm which uses a single key to encrypt the plain text and decrypt the Cipher text. Second is asymmetric algorithm which uses two different keys a public key [2] to encrypt the plain text, and a private key to decrypt the cipher text [3].

Exchange of textual documents is TIFF, GIF, BMP, PNG, PPM, PGM, PBM, PNM, HEIF, BAT, BPG, and business image data needs encryption for secure exchange. For this encryption or decryption with various key files are done with longer key with large no of algorithms. Like; AES, 3DES, Blowfish, Twofish, RC6 and more. The major issue to design any encryption and decryption algorithm is to improve the more security level. Therefore, this paper investigation of performance analysis for exchange of textural documents is image data and business is presented.

It also investigate more efficient, confidential and secure symmetric block cipher cryptic algorithm for image encryption and decryption, against cryptanalysis attacks using SMCrypter tool.This paper aims to propose an efficient symmetric algorithm to improve the security level and increase the performance by minimizing a significant amount of delay time to maintain the security and makes simulative study [4].

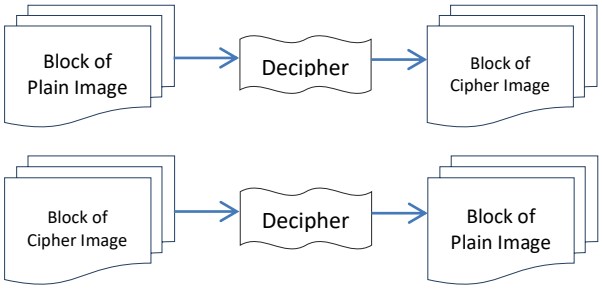

Fig.1. Basic in encryption and Decryption in the real world

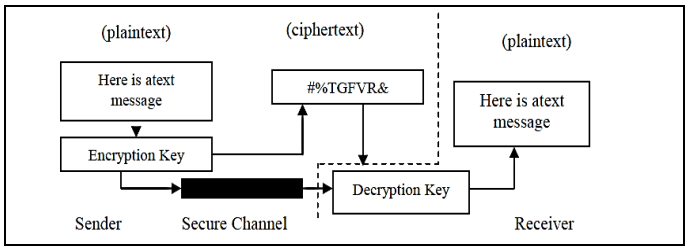

Fig.2.Working Cryptographic Model

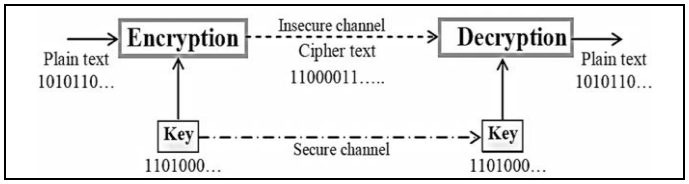

Fig.3.Symmetric encryption and decryption using Single/Private Key

In Fig. 3, Private Key 'K' is used for Encryption and Plaintext is converted into Ciphertext. Same Private Key 'K' is used for Decryption and Ciphertext is again converted back into Plaintext.

II. BACKGROUND AND RELATED WORK

This section involves the information, results and work done by the several research scholars in the field of symmetric cryptographic algorithm for image security. From the related work (books, magazines, journal articles, and websites), observation have been drawn and stated at the end of this section. Finally from the observation objectives of this work have also been derived.

For encryption and decryption of same type of files numerous symmetric algorithms are available in the literature, for finding out better method to optimize communication cost[5] presents results of comparison for AES algorithm. Apart from efficient algorithm search, the classification of these methods for behavior analysis has been presented in [6, 7].

The generation of symmetric key is a challenge, In [8] key generation has been presented using Cassini formula. In[9] key generation has been presented by using location information of sender and receiver. In [10] and [11] the implementation of these approaches has been presented. The analysis of key generation methods has been discussed in [12] for analysis of cipher text. The application of data mining in analysis of cipher text for useful information such as keysize has been presented in [13]. Classification of cryptic family has also been presented in [14].Thus auditing of cryptic algorithm is essential step for development of secure information exchange system.

In [15, 16] comparison of the advance encryption standard algorithm with several modes of operation has been done, while [17] presented an efficient block cipher encryption method based on cubical techniques and improved key. In [18], it proposed a method to protect the data in faster way by using classical cryptography.

In [19] proposed a new block cipher SKC algorithm named TACIT encryption method for secure routing. In [20] proposed an image encryption using advanced hill cipher algorithm or encrypt an image. In [21] worked on secret data communication system using steganography, AES and RSA. In [22] proposed an efficient symmetric key cryptography algorithm for information security.

In [23] it is provided the analysis and comparison of some symmetric key cryptographic ciphers. In [24] author compared AES and DES algorithms on image file, MATLAB software platform was used for implementation of these two cipher algorithms. In [25] the author compared AES and RC4 algorithm, In [26] the author compared cipher algorithms (AES, DES, Blowfish) for different cipher block modes (ECB, CBC, CFB, OFB) on different file sizes. Author talks about comparison between three algorithms (DES, Triple DES, Blowfish) on processing time [27], varying file size [28]. In [29]an image encryption scheme has been proposed based on use of 2D logistic map and AES. In [30] performed digital image AES encryption MATLAB simulation. In [31] presented the implementation of modified RC6 on the basis of encryption and decryption time on the basis of different file size and file types.

The related works have provided a guideline for symmetric cryptic work and brief summary shown in Fig. 4, Fig.5 and Fig.6. The graphical representation highlights the count of

publication, cryptic methods, tools and algorithms used for trend investigation with time.

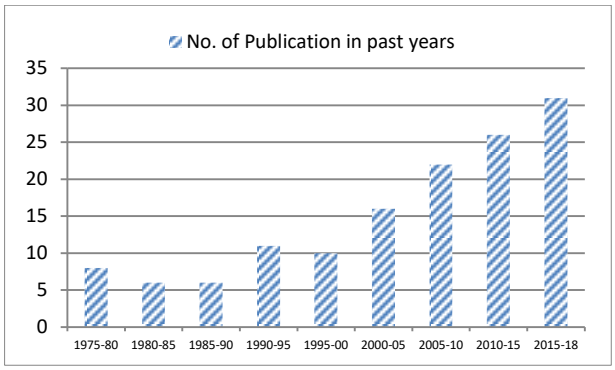

Fig.4. Some previous work in the Past Year with a Count [8,12]

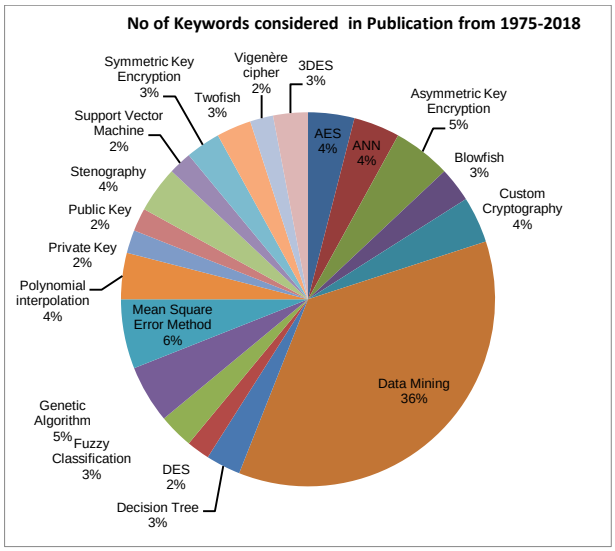

Fig.5. Keywords used for cryptic process and analysis [8,12]

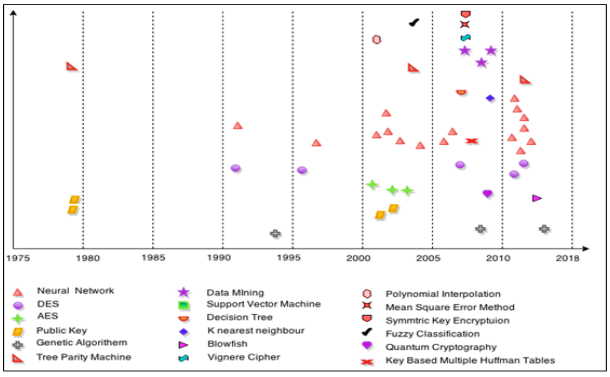

Fig.4.Publications v/s Algorithms [8, 12]

III. ARCHITECTURE OF SKC BLOCK CIPHER ALGORITHMS

Data Encryption Standard- The DES [5,6,7,32]is private-key cryptography and extends spine concept of Feistel Structure (Substitution-Permutation Network) accepts a 64 bit input with 16 iterations + a keysize (56 or 128 bits).Initially 64 bits (blocks size), but in every byte 1 bit as 'parity'. A single plain text block transformed into cipher text over the different stages.

Blowfish-Blowfish Algorithm: It includes key- expansion and data-transformation part with 64 bit input text + 16 iterations, key length up to 448 bits, 18 sub- keys each of 32- bit length can be used on 32 or 64-bit processors[33, 34].

Rijndael- AES-Rijndael [5,6,7,24,26,28] work with block sizes 128, 192 and 256 bits., key size - 128,192 and 256 bits. It depends on the length of key e.g. 10 round for 128 bit key, 12 iterations for 192-bit key and 14 iterations for 256 bit keys. In AES, plain text transformed into cipher text after passing through the different stages like; byte substitution, row shift, column and round key.

Twofish- Twofish [35,36] is a symmetric block cipher algorithm with bock size128-bit, Key lengths of 128 bits, 192 bits, and 256 bits+ 16 iterations.

RC6- RC6 [31,37,38] is a symmetric block cipher algorithm with bock size 128, 256-bit, Key lengths of 128 bits, 192 bits, and 256 bits+ recommended 16 iterations. All these are presented in table 1.

Table 1. SKC Algorithms Architecture [5,6,7]

Algorithm	Block sizes	Key Size	Number of Rounds
AES	128 bits	128,192,256	10,12,14
3DES	64 bits	168	48
Blowfish	64 bits	128-448	16
Twofish	128 bits	128, 192, 256	16
RC6	128, 256 bits	128, 192, 256	20

IV. METHODOLOGY

We are choosing more efficient symmetric key cryptographic encryption and decryption technique have been an issue. To choose the best symmetric key cryptic algorithm from a list of symmetric key encryption and decryption algorithms like: AES, Blowfish, 3DES, RC6 and Twofish, we can encryption and decryption them first to get the best out of them. But for that we need some tool to encryption and decryption their working. Also there should be some parameters like key size, data size, encryption and decryption time for judging which one is the best among them.

We may analyze SKC encryption and decryption algorithms using the web application of SMCrypter, which provides

actual statistics generated during encryption or decryption in several cases. It supports 3 cases of encryption and decryption and provides many types of graphs supported by SMcrypter are as follow:

Category I: Data size vs execution time graphs for encryption using a single key and 4 different data files.
Category II: Data size vs execution time graphs for decryption using a single key and 4 different data files
Category III: Memory utilization vs different key files

V. EXPERIMENTAL DESIGN

For our experiment, We Designed SMCrypter and use a SMCrypter. SMCrypter has been created by us using various programming technologies such as JavaScript (JAVA), HTML, PHP, CSS, JpGraph, and Bootstrap.

SMCrypter tool supports the user to choose a symmetric key based cryptic algorithm from a list of conventional cryptic algorithm, to analyze or compare these algorithms to choose best out of them based on objective measures like Encryption /Decryption time, key size, data size, throughput.

In this work, we are trying to find out performance *analysis* of five symmetric key cryptographic algorithms like: AES, 3DES, Blowfish, Twofish and RC6 on different text file size range from 10KB to 1042KB. Based on the performance analysis and result, we will conclude that which algorithm is better to use based on different performance parameters. We have considered the following parameters for performance analysis of *SKC encryption algorithms on certain parameters: Key size, Data size, Encryption time, Decryption time etc*.

Simulation setup: The simulation has been done on a machine with the specifications: Core™ I3-2120 CPU GHz 3.30 GHz with Intel® Q65 Express 2 GB 1333 MHz DDR3 (RAM) and 32 window-7 operating system. With these specifications the performances are gathered. In this paper the simulation have taken place for text files from the size 10 kb – 2618 kb.

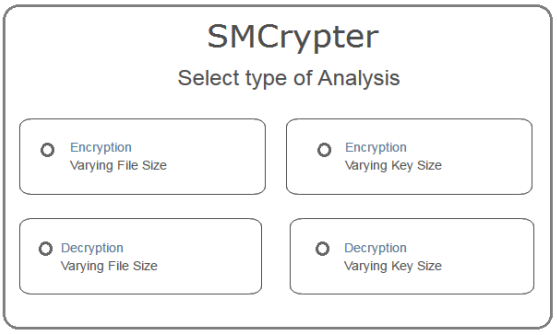

Fig. 7. Home Screen of SMCrypter

Fig. 8. Interface of Select data file for graphs

VI. PERFORMANCE ANALYSIS, RESULT AND DISCUSSION

From the literature survey, it is realized that none of the work did a very detailed analysis of the performance analysis of many symmetric algorithms, on several parameters of different type of image or data files. In order to select the most suitable symmetric cryptic algorithm and to investigate the performance of AES 3DES, Blowfish, Twofish and RC6 algorithm over several image files with variable encryption key size and corresponding time taken to generate encrypted image files is discussed in this section in great details. The counter part of this process that is decryption of encrypted image files (processed with various key lengths).

The Comparative performance of AES, 3DES, Blowfish, Twofish and RC-6 algorithm over various image files with variable encryption key size and corresponding time taken to generate encrypted cipher image files is discussed in this section in great details. Here simulation results corresponding to four input image files (20,30,40,50 KB respectively and corresponding approximate binary representations are 19.9599609375kb, 29.9052734375kb, 39.92578125kb, 50.033203125kb) of different length has been fed to simulator to a specific-Cryptic AES, 3DES, Blowfish, Twofish and RC-6 module and corresponding encryption time in seconds is expressed in second column. Please refer below Table 2-image file size v/s. execution time analysis for encryption using a key with 4 different size text files. Corresponding bar-chart represents performance of symmetric algorithms with encryption time in Fig.9.

Table2.Encryption time rate for image files of different sizes with key size of "ASDFGHJKL"

File Size (Image)	AES	Blowfish	3DES	Twofish	RC6
19.9599609375 kb	0.00066	0.000849	0.003712	0.019284	0.504337
29.9052734375kb	0.001115	0.001232	0.00547	0.029031	0.74995
39.92578125kb	0.001136	0.001649	0.007391	0.039592	0.884961
50.033203125kb	0.00141	0.001998	0.009064	0.048042	1.090689

Table 3.Decryption time rate for image files of different sizes with key size of "ASDFGHJKL"

File Size (Image)	AES	Blowfish	3DES	Twofish	RC6
19.662109375kb	0.000567	0.000761	0.003591	0.017833	0.418852
29.3466796875kb	0.000821	0.001112	0.005336	0.026194	0.615369
39.7314453125kb	0.001130	0.001517	0.007170	0.036136	0.836856
49.7333984375kb	0.001356	0.001850	0.008749	0.043809	1.031282

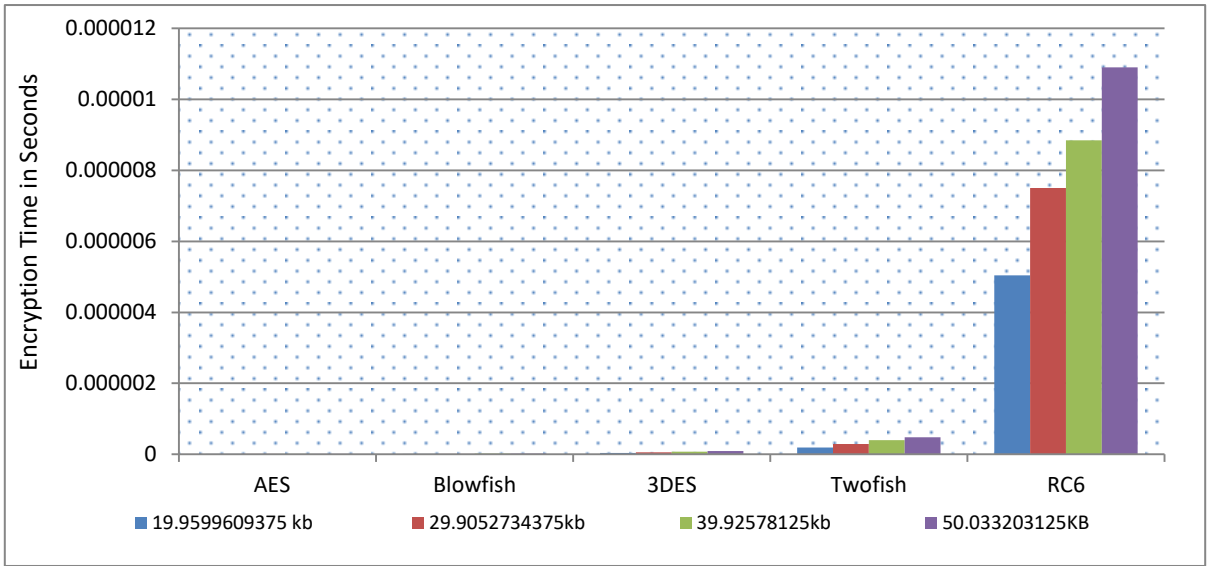

Fig.9.File size v/s Encryption time for Image file of different sizes

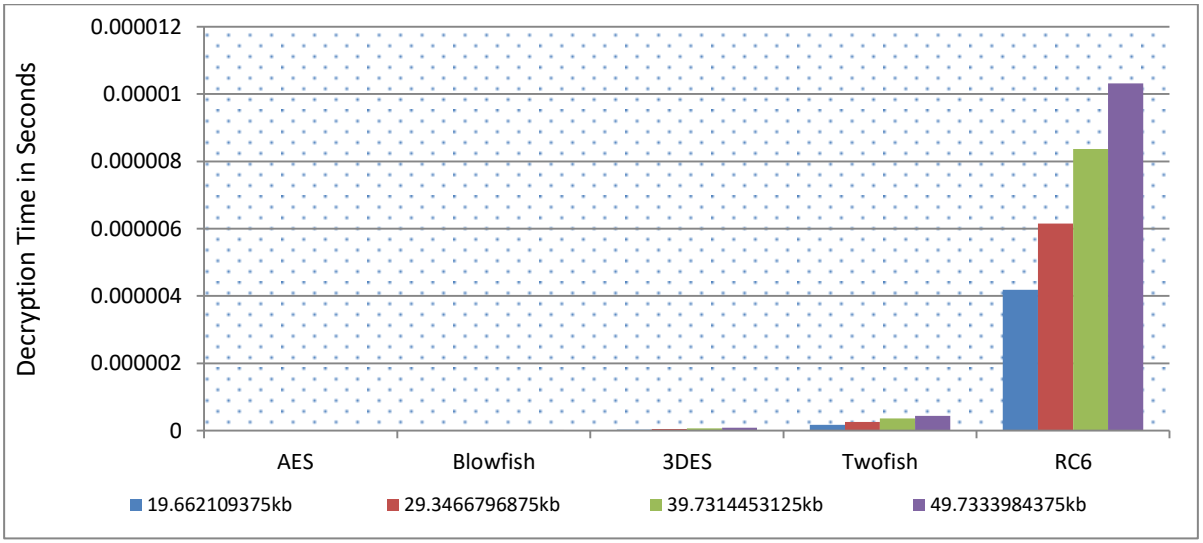

Fig.10. File size v/s Decryption time for Image file of different sizes

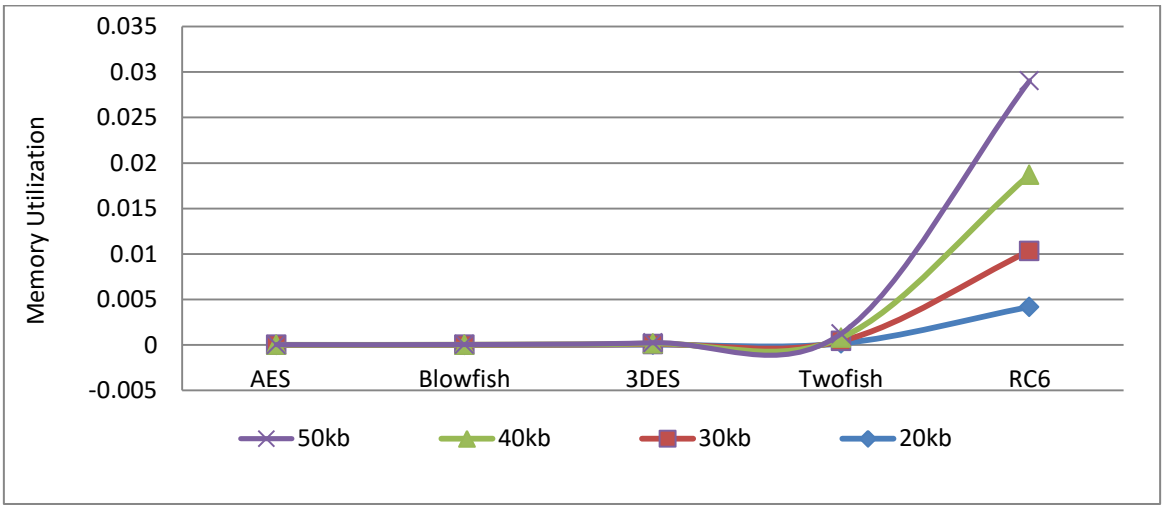

Fig.11.File Size v/s Memory Utilization

Here simulation results corresponding to four encrypted input image files (19.662109375kb, 29.3466796875kb, 39.7314453125kb, 49.7333984375kb) of different length has been fed to simulator to a specific-Cryptic AES, 3DES, Blowfish, Twofish and RC-6 module and corresponding decryption time in seconds is expressed in second column. Please refer below Table 3 image file size v/s. execution time analysis for decryption using a key with 4 different size text files. Corresponding bar-chart represents performance of symmetric algorithms decryption time in Fig.10.

VII. CONCLUSION

Different SKC algorithm have been analyzed for performance evaluation for several matrixes like different data type, data size, key size, encryption time and decryption time and tested how the encryption time varies for different SKC algorithms. This paper presents various state of art symmetric cryptography algorithm for encryption of image files (*19.9599609375kb, 29.9052734375kb, 39.92578125kb, 50.033203125kb*) and cipher image file (*19.662109375kb, 29.3466796875kb, 39.7314453125kb, 49.7333984375kb*). Here all these algorithms have been analyzed for image file encryption and decryption performance. The Experiments investigation demonstrates AES shows better performance, over its competitors in terms of encryption time, decryption time, CPU process time and memory utilization. The performances over huge range of image files like are yet to be investigated. After analysis of all parameters, AES was found to be most suitable encryption algorithm in four modes. In future, this would be beneficial for document and article management system including news.

VIII. FUTURE SCOPE

The future work can be compromise of implementing this work for cloud computing environment and the efficiency of the cryptic system can be improved even more by implementing it in Hadoop environment.

Conflict of interest declaration: The authors declare that there is no conflict of interest of any sort on this research.

REFERENCES

[1]. J.-S. Coron, "What is cryptography," *IEEE Security & Privacy*, Vol.4, Issue.1, pp.70-73, 2006.

[2]. R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol.21, Issue.2, pp.120-126, 1978.

[3]. William Stallings, "Cryptography and network security: Principles and Practices," *Pearson Education India, 7th edition*, 2009.

[4]. H. Mohan, and R. Raji, " Performance Analysis of AES and MARS Encryption Algorithms," *International Journal Computer Science Issues (IJCSI), Vol.*8, Issue.4, 2001.

[5]. Shivlal Mewada, Pradeep Sharma, S. S. Gautam, "Exploration of efficient symmetric AES algorithm, ". *IEEE Symposium on Colossal Data Analysis and Networking (CDAN):*), Indore,pp(1-5), 2016.

[6]. Shivlal Mewada, Sharma Pradeep, Gautam S.S., "Classification of Efficient Symmetric Key Cryptography Algorithms," *International Journal of Computer Science and Information Security (IJCSIS) USA*, Vol.14, Issue.2, pp.105-110, 2016.

[7]. Shivlal Mewada, Sharma Pradeep, Gautam S.S., "Exploration of Efficient Symmetric Algorithms," *IEEE 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. pp(663 – 666), 2016.

[8]. ShaligramPrajapat, Aditi Thakur, Kajol Maheshwari and Ramjeevan Singh Thakur, "Cryptic Mining in Light of Artificial Intelligence" *International Journal of Advanced Computer Science and Applications*(IJACSA), Vol.6, Issue.8, 2015..

[9]. Shaligram Prajapat, Ramjeevan Singh Thakur, "Key Diffusion Approach for AVK based Cryptosystem," *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies ICTCS-16 published by ACM*. 78, 2016.

[10]. Shaligramprajapat, R. S. Thakur, "Realization of information exchange with Fibo-Q based Symmetric Cryptosystem.," *International Journal Computer Science and Information Security*, IJCSIS, Vol.14, Issue.2, pp.216-223, 2016.

[11]. Prajapat, Shaligram, Ramjeevan Singh Thakur, "Markov Analysis of AVK Approach of Symmetric Key Based Cryptosystem. In

proceedings of Computational Science and Its Applications," *Springer International Publishing*. pp. 164-176, 2015.
[12]. ShaligramPrajapat, Ramjeevan Singh Thakur, "Various Approaches Towards Crypt analysis," International Journal of Computer Applications, Vol.127, Issue.14, 2015.
[13]. Prajapat, Shaligram, Ramjeevan Singh Thakur, "Optimal Key Size of the AVK for Symmetric Key Encryption," *In Covenant Journal of Information & Communication Technology*, Vol.3, Issue.2, pp. 71-81. (2015)
[14]. Shivlal Mewada, Aarti Shrivastava, Pradeep Sharma, N Purohit and S.S. Gautam, "Performance Analysis of Encryption Algorithm in Cloud Computing," *International Journal of Computer Sciences and Engineering*, Vol.3, Issue.3, pp.83-89, 2014.
[15]. NidhiSinghal, J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization," *International Journal Computer Trends and Technology, Vol.*1, Issue.3, pp.117-181, 2011.
[16]. Neha Joshi, Megha Singh, Surabhi Shah. A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique. *International Journal of Engg. Science and management*, Vol.5, Issue.4, pp.73-78, 2015.
[17]. S KTripathi, UK Lilhore, "An Efficient Block Cipher Encryption Technique Based on Cubical Method and Improved Key," *I. J. Interdisciplinary Research*, *Vol.*2, Issue.6, pp.373-377, 2016.
[18]. Raghu M E and Ravi Shankar K C, "Application of Classical Encryption Techniques for Securing Data- A Threaded Approach," *International Journal Cybernetics & Informatics (IJCI)*, Vol.4, Issue. 2, pp.125-132, 2015.
[19]. P. Gope, A. Singh, A Sharma and N. Pahwa, "An Efficient Cryptographic Approach or Secure Policy Based Routing. *IEEE Journal on Selected Areas in Communications*, Vol.1, pp.359-363, 2013.
[20]. L. Buttyan, L. Czap and I. Vajda, "Detection and Recovery from Pollution Attacks in Coding Based Distributed Storage Schemes," *IEEE Transaction on Dependable and Secure Computing*, Vol.8, Issue.6, pp. 824-838, 2011.
[21]. S. F. Mare, M. Vladutiu and L. Prodan, "Secret data communication system using Steganography, AES and RSA," *IEEE: International Symposium for Design and Technology in Electronic Packaging*, Vol.2, pp. 339-344, 2011.
[22]. S. Verma, R. Choubey and R. Soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security," *International Journal Emerging Technology and Advanced Engineering*, Vol.2, Issue.7, pp.18-21, 2012.
[23]. RanjeetMasram, Vivek Shahare, Jibi Abraham, RajniMoona. Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based On Various File Features, *International Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.4, pp. 43-53, July 2014.
[24]. S. Soni, H. Agrawal, M. Sharma, "Analysis and comparison between AES and DES Cryptographic Algorithm. *International Journal of Engineering and Innovative Technology*, Vol.2, Issue.6, pp.362-365, 2012.
[25]. NidhiSinghal and J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization," *International Journal of Computer Trends and Technology*, Vol.2, Issue.6, pp.177-181, 2011.
[26]. Jawahar Thakur et. Al., "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol.1, Issue.2, pp.6-12, 2011.
[27]. Kofahi, N.A, Turki Al-Somani, Khalid Al-Zamil, "Performance evaluation of three Encryption/Decryption Algorithms", *IEEE 46th Midwest Symposium on Circuits and Systems, Vol.* 2, Issue.1, pp.790-793, 2003.
[28]. Y. Jha, K. Kaur and C. Pradhan, "Improving image encryption using two-dimensional logistic map and AES," *2016 International Conference on Communication and Signal Processing (ICCSP)*, Melmaruvathur, Tamilnadu, India, pp-0177-0180, 2016.
[29]. M. Kurt Pehlivanoğlu and N. Duru, Encryption of Walsh Hadamard Transform applied images with the AES encryption algorithm," *2016 24th Signal Processing and Communication Application Conference (SIU)*, Zonguldak, pp. 301-304, 2016.
[30]. Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control*, Qinhuangdao, pp.1218-1221, 2015.
[31]. K. Aggarwal, "Comparison of RC6, modified RC6 & enhancement of RC6," *2015 International Conference on Advances in Computer Engineering and Applications*, Ghaziabad, pp-444-449, 2015.
[32]. Dadhich, A.; Gupta, A.; Yadav, S..Swarm, "Intelligence based linear cryptanalysis of four-round Data Encryption Standard algorithm", *IEEE:International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp: 378 – 383, 2014.
[33]. Alabaichi, A., Ahmad, F., Mahmod, R., "Security analysis of blowfish algorithm", *IEEE: 2nd International Conference on Informatics and Applications (ICIA-13)*, pp.12– 18, 2013.
[34]. TingyuanNie, Teng Zhang, "A study of DES and Blowfish encryption algorithm", IEEE Region 10 Conference, pp.1-4, 2009.
[35]. G. Catalini, F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni and M. Reginelli, "Modified twofish algorithm for increasing security and efficiency in the encryption of video signals," *Proceedings 2003 International Conference on Image Processing (Cat. No.03CH37429)*, 1:I-525-8, 2003.
[36]. A. O. Montoya B., M. A. Muñoz G. and S. T. Kofuji, "Performance analysis of encryption algorithms on mobile devices," *2013 47th International Carnahan Conference on Security Technology (ICCST)*, Medellin, pp. 1-6, 2013..
[37]. H. K. Verma and R. K. Singh, "Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6," *2013 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, pp. 556-561, 2013.
[38]. S. Mewada, P. Sharma, and S. S. Gautam, "Investigation of Efficient Cryptic Algorithm for Text using SM Crypter," *International Journal of Information Science and Computing*, Vol.3, Issue.2, pp. 99-108, 2016.

