International Journal For Technological Research In Engineering
Volume 5, Issue 5, January-2018 *ISSN (Online): 2347 - 4718*

A ROBUST LZW AND BIT PLANE BASED DATA ENCRYPTION TECHNIQUE

Ganesh Nimanpure[1], Yogendra P.S. Maravi[2], Sanjeev Sharma[3]
[1]Research Fellow M-tech, Department of School of Information Technology (SOIT), Bhopal
[2]Assistant Professor and Supervisor, Department of School of Information Technology (SOIT), Bhopal
[3]Professor and HOD, Department of School of Information Technology (SOIT), Bhopal

Abstract: As internet users are increasing day by day with drastic data available on the servers. So the need to protect the data has increased with the introduction of computer networks. In the same way the attacks on the data is also increasing to break the security. The traditional cryptography methods cannot be useful in today's computing world. Thus, the use of modern cryptography approaches are significantly increasing for protecting the data in comparison to the issues related with the traditional approaches. Proposed work provides a robust algorithm for encryption by using LZW and binary input combination. As LZW help in compressing the information and binary input increase the size security level with easy pattern findings. Here algorithm are so designed that common algorithm take all kind of data as input for encryption of image and text. This flexibility obtained because of binary working environment in the algorithm. One more reasons for binary input is to get more set of patterns from the input file which reduces the output file size of the LZWalgorithm. It has been obtained from result section that proposed work execution time is less as compare to the previous work, in both cases of encryption and decryption. It was obtained that average execution time of the various sets of text and image data of proposed work was less as compared to previous A-S algorithm because of small key size that proposed work encrypted file size is less as compare to the previous work. As proposed work use LZW algorithm for the encryption which compress input data. The proposed algorithm have been tested
against different known dataset for various types of data. Results shows that proposed has improved various evaluation parameters as compared to previous work.
Key words: Data Security,LZW Algorithm, Encryption and Decryption

I. INTRODUCTION

In today's Information technology era, computer networks are widely used to share information and to communicate with others. The conceivable outcomes of hacking the information being transmitted over the systems are expanding. Sensitive information is required to be shielded from unapproved access for transmitting over uncertain systems, for example, the Internet. Security of information has turned out to be one of the testing issues in these systems. For moving information in protected and secure way cryptography procedure is utilized. It utilizes encryption and decryption calculations for securing the information being transmitted over the systems. It is an old methodology that has been used around number of years for protecting the information from others. These days current cryptography strategies are advanced to give security which utilizes scientific systems and in light of two essential segments: Algorithm (a strategy) and a key to decide the particular of calculation operation. These advanced cryptographic techniques plan to accomplish the security objectives, for example, information secrecy, uprightness, non-repudiation and confirmation. Utilizing the digital systems for exchanging the Visa data, sending electronic reports, internet shopping, and so on all require a proficient security component. There is a plausibility of perusing the data by an outsider. Cryptography is an effective procedure that utilizations encryption and decoding strategy to shield the information from unapproved access to protect trustworthiness and security of information, encryption and decryption strategies are utilized. The plaintext is the first type of information and the cipher content is the encoded type of information. Encryption strategies take plain content (unique type of information) as an info and change over it into cipher content (encoded type of information), in view of calculation utilizing a key. A key is a part based on which information is encryption. Decryption procedures takes the cipher content (encoded type of information) and change over it into plain content (unique type of information) in view of calculations are arranged into two classes in light of calculation utilizing a keys utilized: Symmetric Key Cryptography calculations and Asymmetric Key Cryptography algorithms. [1-6] In Symmetric Key Cryptography calculations a solitary key is utilized for encoding and decryption the information. A key is transmitted to both sender and recipient before correspondence. It is in like manner called private or secret key cryptography.

Some common symmetric key cryptographic algorithms are shown in Table 1.

Table 1: Common symmetric key cryptographic algorithms [1-10]

Algorithm	Description	Key Length	Comments
Blowfish	Block cipher developed by BrucSchneier	1-448 bits	Old and slow
DES	DES adopted as a U.S. government standard in 1977	56 bits	Too weak to use now
IDEA	Block cipher developed by Massey and Xuejia	128 bits	Good, but patent

RC4	Stream cipher developed by Rivest	1-2048 bits	Caution: some keys are weak
RC5	Block cipher developed by Rivest and published in 1994	128-256 bits	Good, but patent
Rijndael	NIST selection for AES, developed by Daemen and Rijmen	128-256 bits	Best choice
Serpent	AES finalist developed by Anderson, Biham, and Knudsen	128-256 bits	Very strong
Triple-DES	A three-fold application of the DES algorithm	168 bits	Second best choice
Twofish	AES candidate developed by Schneier	128-256 bits	Very strong; widely used

Then again, Asymmetric key Cryptography calculations utilize a key match known as public key and private key. Public key is utilized for encoding the message while private key is utilized for decoding the message. They are likewise called public key cryptography methods.Symmetric key encryption is quicker than topsy-turvy key encryption [6].

The quality of a cryptographic calculation relies upon the operations utilized and the difficulty of speculating the key. A calculation is said to be great on the off chance that it is difficult to figure the substance of information without knowing the key. There will no other procedure as opposed to efficiently attempting each conceivable mix of key if a calculation is decent. On the off chance that the lifetime of the substance increments as the time required breaking the figure expands, a calculation is called as unconditionally secure. Traditional security calculations are enhancing with fresher ideas to improve the security of information and the adequacy of calculation. In this way, enormous looks into are being done to build up some solid encryption calculation as opposed to customary existing calculations, for example, AES, DES, and so on to secure the encoded message captured by the gatecrasher. These calculations plan to give preferred security and effectiveness over traditional algorithms [10].

Now at present, the computers systems are fundamentally utilized for exchanging the information. The security of information has turned into an essential issue when utilizing the unreliable system like web for sharing the private data, for example, Visa data, electronic structures, and so on. The information can't be transmitted in decoded shape as it might be captured by an aggressor. In this way, to secure the delicate information, cryptographic calculation is required. Recently, various researches are being done to develop a strong encryption algorithm to improve the security of the data than traditional existing algorithms. Single password for encryption and decryption come up as an answer. The implementation is being performed on a transferring data which include all (image, text). The security technique is encouraging and shows that the decoded data have a great throughput [11-16].

These days, there are a few cryptographic calculations accessible that agreements the security of the information. The need to secure the information has expanded with the presentation of digital systems. Similarly the thrash on the information is additionally expanding to break the security. The customary cryptography strategies can't be valuable in the present processing world. In this manner, the utilization of current cryptography approaches are fundamentally expanding for securing the information in contrast with the issues related with the traditional methodologies such as [6]:

- Generation of the large cipher text consumes a huge amount of space.
- Increase in the encryption and decryption time with the increase in the amountof data.
- Large amount of memory utilization and battery consumption.

Therefore, the main objectives of this research work are that to propose a new solution for our day to day life for secure communication and exchanging information. For secure communication here work uses a compression and cryptography techniques.Implement the proposed algorithm and analyze the performance of proposed algorithm on different parameters. Compare the performance of proposed algorithm with existing algorithms and have a more profound cryptographic and compression procedure. To evaluate and select number of security products and policies, the owner who is responsible for security needs some planned approach of defining the need of security and characterizing the approaches to satisfy those needs [16-20].

II. METHODOLOGY

This work concentrates on the computerized information concealing systems. Here entire work was arranged to the point that information get preprocessed first that change binary format as per the numeric representative of the data. Here work was divide into data encryption and decryption stages. For In case of decryption hided data should be successfully retrieve from the received data without any information loss of the original data as well as data hiding [7, 8]..Flow Diagram for Proposed works is shown in Figure 1.

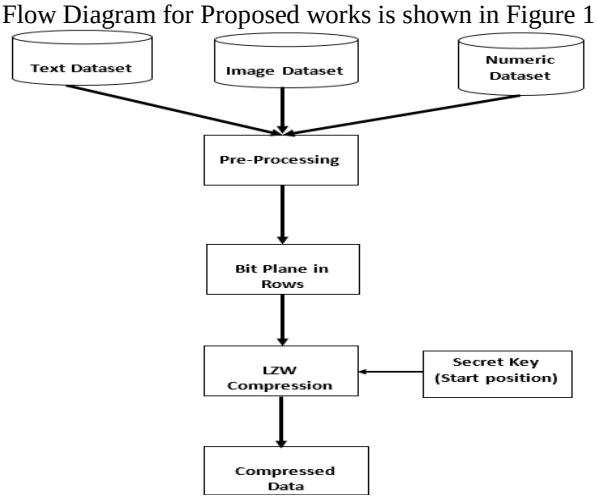

Figure 1. Flow Diagram for Proposed works

III. IMPLEMENTATION

In this chapter a detail about the implementation and results is presented. Implementation is done on matlab tool. The tests were performed on an Intel Core i3 machine, outfitted with 4 GB of RAM, and running under Windows 7 Professional.MATLAB 2012a is the tool use for the execution of this work.

Experiment was done on two different type of dataset, first was text dataset while second was for image.Text dataset was obtained from the Copernicus dataset where Newsgroups: rec. sport. Hockey Subject are branch into different sets. So experimentstandard images are use fromhttp://sipi.usc.edu/database/database.php?volume=misc. Here detail of different images are explain in Fig. 2.

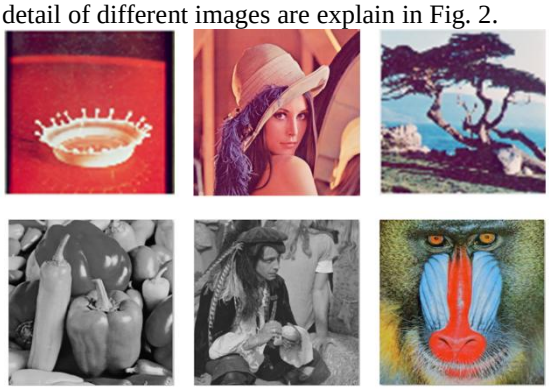

Figure 2. Dataset Images

Execution Time

In this evaluation parameter proposed algorithm shuffling time is calculate. Here it is desired that shuffling time of the new image should be less. Execution time is calculate in terms of second.

Encrypted file Size

Size of the encrypted file is found by counting the pattern representing number in the file. Here all kind of special characters, alphabets and space are transform into its representative data form. It is required that size of the encrypted file should be less than the original file.

Decrypted file Size

Size of the decrypted file is found by counting the number of characters in the file. Here all kind of special characters and space is also count. It is required that size of the decrypted file should remain same as the original file.

IV. RESULT ANALYSIS

Security is the biggest concern for the data, there are many cryptographic techniques which is used to encrypt data and provide security for that data.in this section a comparison analysis for propose technique with the existing technique is presented. Time is the prime measure for any algorithm, which shows the efficiency of the algorithm that how efficiently an algorithm can provide desire results.

To compare proposed technique with the existing technique encryption time, decryption time are taken as a measure to analyze the propose technique. It has been obtained from Table 2 that proposed work encrypted file size is less as compare to the previous work. As proposed work use LZW algorithm for the encryption which compress input data. It was obtained that average file size of the various sets of text data of proposed work was less as compared to previous A-S algorithm.

Table 2. Comparison of proposed and previous work encrypted data size

Text Data	Text Data Encrypted Size	
	Proposed Work	Previous Work
Set A	1620	1791
Set B	1380	1457
Set C	754	774

It has been obtained from Table 3 that proposed work encrypted execution time is less as compare to the previous work. As proposed work use LZW algorithm for the encryption which compress input data. It was obtained that average encrypted execution time of the various sets of text data of proposed work was less as compared to previous A-S algorithm because of small key size.

Table 3. Comparison of proposed and previous work average encrypted execution time

Text File	Text Data Encryption Execution Time	
	Proposed Work	Previous Work
Set A	24.1	24.29
Set B	15.11	17.65
Set C	6.06	11.68

It has been obtained from Table 4 that proposed work decrypted execution time is less as compare to the previous work. It was obtained that average decrypted execution time of the various sets of text data of proposed work was less as compared to previous algorithm because of small key size.

Table 4. Comparison of proposed and previous work average decrypted execution time

Text data	Text Data Decryption Time	
	Proposed Work	Previous Work
Set A	1.41	2.72
Set B	1.36	2.64
Set C	0.61	1.96

It has been obtained from Table 5 that proposed work average input text data with key size is less as compare to the previous work. As proposed work use LZW algorithm for the encryption which required small key for encryption. So it was obtained that average input text data with key size of the various sets of text data of proposed work was less as compared to previous A-S algorithm.

Table 5. Comparison of proposed and previous work average input text data with key size

Text Data	Average Input Text Data with key Size	
	Proposed Work	Previous Work
Set A	3240	1622
Set B	2760	1382
Set C	1508	756

It has been obtained from Table 6 that proposed work encrypted image size is less as compare to the input size. As proposed work use LZW algorithm for the encryption which compress input data.

Table 6 Comparison of proposed and previous work encrypted image data size

Image Size	Proposed Work Encrypted Size
3072	2798
3072	2784
4704	3938

It has been obtained from Table 7 that proposed work encrypted execution time was quit high as compared to text data. As image size is quite large as compared to text file data. Here time required for the decryption was less because of less number of comparison for string table.

Table 7 Comparison of proposed and previous work execution time

Text File	Execution Time (Seconds)	
	Encryption	Decryption
Lena	21.209	1.24239
Mandrilla	44.1644	1.37271
Obama	69.0208	2.12194

V. CONCLUSION

This work presented new approach for complex encoding and decoding information. In spite of the fact that there have been numerous scientists on the cryptography, yet the greater part of the current algorithms have a few shortcomings either caused by low security level or increment the execution time due the plan of the algorithm itself. Proposed work provide a robust algorithm for data security by using LZW and binary input combination. As LZW help in compressing the information and binary input increase the size security level with easy pattern findings. Here algorithm are so designed that common algorithm take all kind of data as input for encryption of image and text. This flexibility obtained because of binary working environment in the algorithm. It has been obtained from result section that proposed work execution time is less as compare to the previous work, in both cases of encryption and decryption. It was obtained that average execution time of the various sets of text and image data of proposed work was less as compared to previous A-S algorithm because of small key size that proposed work encrypted file size is less as compare to the previous work. As proposed work use LZW algorithm for the encryption which compress input data. The proposed algorithm have been tested against different known dataset for various types of data. Results shows that proposed has improved various evaluation parameters as compared to previous work.

REFERENCES

[1] Abdul D.S, Kader 1-1.M Abdul, Hadhoud, M.M.,"Execution Evaluation of Symmetric Encryption Calculations", Communications of the IBIMA, Volume 8, 2009, Pp. 58-64.

[2] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", Global Journal on Computer Science and Engineering (1JCSE), Vol. 4 No.05 May 2012, PP. 877-882.

[3] Alam Md Imran, Khan Mohammad Rafeek. "Execution and Efficiency Analysis of Different Block Cipher Calculations of Symmetric Key Cryptography", International and Computation Technology, ISSN 0974-2239 Volume3, Number3 (2013).

[4] Annapooma Shetty, Shravya Shetty K, Krithika K," A Review on Asymmetric Cryptography —RSA and ElGamal Algorithm", Intimation al Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798Vo1.2, Special Issue5, October 2014

[5] Anuj, Babita, Reena, Ayushi Aggarwal," An Approach to Improve the Data Security using Encryption and Decryption Technique", International Journal of Information

[6] Apoorva, Kumar Yogesh, "Near Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2,Issue 7, July 2013, pp. 204-206.

[7] Charru, Paramjeet Singh, Shaveta Rani "Efficient Text Data Encryption System to Optimize Execution Time and Data Security" International Journal of Advanced Computer Theory and Engineering (1J ACTE), ISSN (Print): 2319-2526, Volume - Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 4,

[8] Cornwell jason W, "Blowfish Survey", Department of Computer science, Columbus State college, Columbus, GA, 2010.

[9] Devendra Prasad, Govind Prasad Arya, Chirag Chaudhary, Vipin Kumar, "A Text Encryption and Decryption Technique Using Substitution-Transposition and Basic Arithmetic and Logic Operation", International Journal of Computer Science and AritInformation Technologies, Vol. 5 (2), 2014.

[10] E.Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most CommonEncryption Techniques", International Journal of Advanced Research in Computer Science andSoftwareEngineering,ISSN:2277-128X.

[11] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, International Journal of Network Security &Its Applications(IJNSA), Vol.3,

[12] K.B. Priyalyer, Ph.D. R. Anusha, R. ShakthiPriya," Comparative Study on Various Cryptographic Techniques,-, International Journal of Computer Applications (0975 —8887),International Conference on Communication, Computing and Information.

[13] Kondwani Magamba, Solomon Kadaleka and Ansley Kasambara, "Variable-length Hill Cipher with MDS KeyMatrix", International Journal of Computer Applications, Volume 57 – Number 13, November 2012.

[14] M. Yamuna, S. Ravi Rohith, Pramodh Mazumdar, Avani Gupta "Text Encryption Using Matrices International Journal of Application or Innovation in Engineering & Management(IJAIEM)Volume 2, Issue 3, March 2013.

[15] Mandal Pratap Chandra, "Prevalence of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9,September 2012, pp. 196-201.

[16] S.Devi, Dr.V.P Alanisamy," Multi-Level Encryption using SDES Key GenerationTechnique with Genetic Algorithm", International Journal Of Engineering And Computer Science ISSN:2319-7242Volume -3 Issue - 8 August, 2014.

[17] S.G.Srikantaswamy, Dr. H.D.Phaneendra "Enhanced One Time Pad Cipher with rations with Flexible Key Generation Algorithm. More Arithmetic and Logical Open Volume4, issue7,Ju1y2014.

[18] Saini Bahar, "Study On Performance Analysis of Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014, pp. 1-4.

[19] Singh S Preet, Mani Raman, "Correlation of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No 1, January-June 2011, pp 125-127.

[20] Tamimi A. Al., "Execution Analysis of Data Encryption Algorithms", Oct. 2008. Technology (ICCCMIT-2014).

