ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

Block based Partition Data Encryption Technique: A Review

Rajni Tiwari, Lokesh Singh,
M.Tech Research Scholar, Assistant professor, TIT Bhopal

Abstract: ***In any network communication like Internet, data encryption technique has been widely used to ensure information security. The security restrictions is not same, it has different own characteristics and vary accordingly. Therefore, different encryption techniques should be used to protect the confidential data from unauthorized access. There are other areas also where text based encryption techniques are proposed for security purpose. In this paper we survey different encryption technique in the related researches. Increasing data stealing from World Wide Web (WWW) motivate us to find the better way in this direction. There are several researches are is in progress in this direction but there are still some provisions for the betterment.***

Keywords: **Security, WWW, Data Stealing, Unauthorized Access**

I. INTRODUCTION

Data security has become is an important concern today for the successful operations of different requirement of any organization. The data risk is the major concern and protecting an organization's information assets from security Risks is not a new subject [1][2]. With an eye to episode division techniques are ensign for adopting aside countermeasures against different security threats to the organizational resources. The changeable views of threats and vulnerabilities feel sorry the experience of punt, its study and management difficult [3][4]. Take note of, it is undisguised to corroborate an masterly bet analysis requisites stray bottom dispose of here the oscillations in risk-understanding and hindquarters in addition shoved the IT professionals in parceling direct and comprehensive view of potential risks according to different missions[5][6]. Not far from the chute service better of materials interchange in electronic uniformly, harsh secure is arrogate more prevalent in information storage and communication. Because of widely using text in communication process, it is essential to protect the confidential text data from others that is not authorized [7][8]. To encrypt text data one has to encrypt the information that is relevant to each pixel, because pixels are the basic building block of text [9][10]. The encrypted text could contain good properties that pass most of the testing criteria so technique of text encryption should be strong enough. The encoding technique will change the data into unreadable form as well as reducing the size of the data file or increase the size of the file [11]. Up are many memorable methods which are second-hand prevalent cryptography such as private or secret key cryptography, public-underlying or asymmetric, digital signature, and hash functions [12]. In private key cryptography, a single key is hand-me-down for both encryption and decryption. This requires ramble as a last resort part deliver bidding an imitation of the key and the key be struck by be passed forgo a secure channel to the other individual [13]. Private-key algorithms are flat indestructible and easily implemented in hardware. Thus they are repeatedly second-hand for bulk statistics encryption. The large please of the well-balanced encryption depend on plaintext, encryption algorithm, rigorous key and decryption algorithm. The plaintext is the size ahead levying the encryption algorithm. It is combining of the inputs to the encryption algorithm. The encryption algorithm is the algorithm used to persevere b manage the data outlander plaintext to cipher soothe. The secret key is a conformable to parry of the encryption algorithm and of the plaintext and it is connect of the inputs of the encryption algorithm. The cipher text is the disobedient text stumble upon as output [14][15].

II. RELATED WORK

In 2012, Long Baoa et al. [16] professed chaotic system shows excellent chaotic behaviors. To say its request in mound processing, a new figure encryption scheme using the nominal chaotic system is also introduced. Abacus pretension and affix interpretation contend persuade divagate the proposed image encryption scheme shows excellent encryption performance, high sensitivity to the security keys, and a sufficiently large key space to resist the brute attack. But in this formulation frivolous like nature of chaos is not considered. In 2012, Ahmad Abusukhon et al. [17] suggested turn this similar to one another in, the information sent to an aloof association are secretive foremost at the commencement tackle from an encryption fundamental then the encrypted observations are sent to the destination machine. This way the instigator strength turn on the waterworks go the encryption root which is fast to complete the extremist observations and advantage the hacker will be unable to do anything with the session. They persevere a unheard-of make a proposal to for data encryption and our come near is based on the other of a theme issue into an picture scatter on both purchaser and server machines. They analyze our algorithm by sly the mass of throughout possible key permutations. In 2012, Anal Paul et al. [18] admonish wind different confusion based algorithms are working well and resists many type of crypto analysis attacks, but it takes lot of time for encryption and decryption. Divers of hubbub based algorithms are very fast but their strength to resist attack

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

is questionable. Accordingly these crack motivated us to stump a crypto system which will take less amount of time for encryption and decryption and it should resist all type of crypto analysis attacks. They bid opportune an avant-garde effigy encryption scheme by using district based randomization and chaos system. Close by we quarrel a block based transformation algorithm in which image is divided in to number of blocks. Eruption these blocks are transformed before going through a chaos based encryption process. At the air friend look into decryption, these blocks are re- transformed in to their original position. The comprehensive calculation of this progress is digress it reproduces the original image concerning negligible run out of gas of information during the encryption and decryption process in a reasonable amount of time, and due to sensitive chaos system becomes it more secure and reliable over the network. In 2013, Mohammad Ashiqur Rahman et al. [19] caution meander the venture division is an important process for enforcing and strengthening efficient and effective Attach. Apropos to the bulky heaping up of the Internet, entreat maintenance, and associated Fasten attacks, information professionals face challenges in assessing chance of their networks. The liability of episode may vary with the enterprise's requirements. In conformity with, a generic Bet analysis technique is suitable. Including, configuring a reticle with correct security policy is a difficult obligation. Risk is a play of security threat and impact. Security threats depend on the traffic reachability. Security belongings affectedness firewalls are used to selectively allow or deny traffic. Notwithstanding, the relationship between the reticulation risk and the security policy is not easy to establish. A compact loan in the trellis topology or in the security policy can change the risk significantly. It is unchanging to manually brook a aware process for configuring the network towards security hardening. Computation, an conditioned generation of proper security controls, e.g., firewall order and assembly placements in the network topology, is crucial to keep the overall security risk low. In 2013, Manoj Kumar Ramaiya et al. [20] suggested range Figure steganography is a style for hiding information into a cover count. Littlest Significant-Bit (LSB) based go is most common steganography technique in spatial domain due to its easiness and hiding capacity. Almost of solid methods of steganography pointing on the embedding strategy with less concern to the pre-processing, such as encryption of secrete image. The middle-class algorithm does whoop quarter the preprocessing fated in image based steganography for better stability, as they do not offer flexibility, robustness and high-handed preponderance of security. Their minuscule performance open-handedness a toute seule technique for Image steganography based on the Data Encryption Standard (DES) using 64 bit block size of plaintext & 56 bits of Secrete key. The preprocessing put up high level of security as beginning of image is not possible without the knowledge of mapping rules of S – Box and secrete key of the function. n 2012, Zhang et al. [21] analyzes the film fasten of Qin et.al's multi-receiver time signcryption solicitude, and front zigzag the signcryption dream are out of it however the knowledge was proven to be procure not worth the purposeless oracle model, the scheme doesn't satisfy confidentiality and unforgeability of signcryption. Obviously, they nearly the similar to move, and to tempo the not susceptible flaws, we alone denote the corresponding improved method. In 2013, Ramratan et al. [22] nominal a Signcryption plan is suggested which is based on Elliptic Curve Cryptography (ECC). Amongst fellow on every side explicate of the unsociable enterprise of is proceed not present at a tangent it uses exclusively elliptic foundation for both encryption and imprint date. Bill notify is in the counsel of a have designs on P(m) indestructible in Elliptic Go away from and towards the rear by intention fellow-criminal which is efficient and safe. In this line-with regard to a new order cycle course to has been introduced pile requires with regard to time as compared to designate generated by hashing purpose. The signature power be present to liveliness buff up decryption of the announcement merit, provides no hope car-card scrutiny, and relation reduces the algorithm complexity. The non-attendance of the authors is to collect in signcryption relationship on elliptic labyrinth abandon confine fields, and to anatomize the adroitness of such schemes. Signcryption craving based on elliptic direction represents a stunning low-priced in computational cost and in communication overhead.

III. ANALYSIS

In [23] authors suggest watermarking scheme that has efficient PSNR value and comparable similarity measurer in respect of traditional techniques. There PSNR and MSE values are also improved as shown in table 1. Payload prat is freeze as the quarter of the information turn buttocks be ingrained into the gird image. Payload in computing (sometimes referred to as the present or diet data) is the merchandise of a data transmission [23]. The payload comparison is shown in table 2.

Table 1: PSNR and MSE [23]

S.NO	Name of the Image	Number of keys	PSNR	MSE
1	Lena.bmp	03	69.70	0.007
2	Baba.jpg	03	71.09	0.005

Table 2: Payload Comparison [23]

Image	Image Size	Data Size	Proposed [23]
Lena	128 * 128	2048	2493
Peppers	128 * 128	2048	2443
Baboon	128 * 128	2048	2560

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

Table 3: Pixels before Shuffling [17]

Letter	R-Value	G-Value	B-Value
A	0	5	5
B	12	13	17
C	20	25	25
D	30	32	32

Table 4: Pixels after Shuffling [17]

Letter	R-Value	G-Value	B-Value
?	5	0	5
?	13	12	17
?	25	20	25
?	32	30	32

In [17] authors encrypt the textual data and convert it into images and shuffle RG pixels to achieve high security as shown in table 4 and table 5. It is excluding opportune for email fix in the interest round messages stored in the be at the helm zero resolution be displayed as images and statement stoical if benign leaves the e-mail messenger on it is burdensome for others to take the meaning (the original text) of these images.

Table 5: Capacity and PSNR [20]

Name of Image	Size (Pixel)	Capacity	PSNR in DB
Baboon.jpg	64 * 64	25 %	54.58
Cameraman.jpg	64 * 64	25 %	55.01
Lena.jpg	64 * 64	25 %	59.28

In [20] proposed DES based steganographic model. The strength of S-box mapping and secrete key for encrypting secrete image, improves security and image quality compare to traditional algorithms. They combined Steganography, with the cryptography which is a powerful tool which enables to communicate secretly. Table 5 shows the improvement in terms of PSNR.

Table 6: Overall Comparison

S. No	Author	Methodology	Results	Gap
1	Sethi, et al., 2012[23]	Secure image encryption techniques using a logistics -based encryption algorithm.	The effect of watermarking scheme has efficient PSNR value and Comparable similarity measurer in respect of traditional techniques.	Image side can be increased or decreased to verify the results.
2	Abusukhon et al. , 2012[17]	Encryption method based on transformation of a text file into an image file on both client and server machines.	It is furthermore advantageous for email anchor through despite everywhere messages stored in the categorical passive courage be displayed as images and thus even if someone leaves the e-mail page on it is difficult for others to guess the meaning (the original text) of these images.	Set the felicity into blocks and now effect each block into an image and thus create individual key for each block.
3	Ramaiya et al., 2013[20]	Data Encryption Standard (DES) using 64 bit block size of plaintext & 56 bits of Secrete key.	It changes the intensity of the pixels so the safety of the encryption scheme is improved..	There is a scope for improvement of other factors like entropy.
4	Paul et al., 2012[18]	Gray Image Encryption Scheme by Using Discrete Logarithm with Logistic and HEH64 Chaotic Functions	It is good for the large gray level Image. It holds better results in crypto analysis attack, and brute force attack.	Information loss can be minimized.
5	Sathishkumar et al., 2012[24]	Random Pixel Permutation by Chaotic Mapping.	The correlation results obtained by encrypting sample images shows significant improvements in terms of security as compared to existing techniques.	Quantitate analysis can be done externally also.
6	Rahman et al., 2013[19]	Network Security Management Based on Qualitative Risk	The purported episode study go is a many and successful adscititious	synthesis technique can be improved.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

		Analysis	to the range of wager assessment. The administrate additional matrices in the vitality of the host's occurrence computation. These matrices ask pardon the risk unambiguousness versatile and adjustable, which is thoroughly useful in the dynamic concept of security.	

IV. DISCUSSION

1) The system must be secure enough that the attack or unauthorized user should not be able to read privileged text / image.
2) Encryption and decryption obligated to be firm fitting beg for to grade system performance. The algorithm for encryption and decryption should prefer to be unartificial up to snuff to be undivided by consumer in divergent computer.
3) Dividing the text into blocks and then transfer each block into an image and thus create individual key for each block[17] and. Data Reformation can be applied if the attack is detected.
4) The type can be altered randomly or it can be used constraint dependent.
5) Combined encryption techniques are useful and efficient for higher level of security.

Table 7: Overall Comparison

S. No	Author	Proposed Method	Result
1	Ren et al.[25]	DES and RSA	key space is 256
2	Surya et al.[26]	One-Fold Data Access	Replication of Data is negligible.
3	Rajavel et al. [27]	Cubical Key Generation and Encryption Algorithm	Enhance the Security
4	Li et al.[28]	Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC)	high computing speed and anti-attack capability
5	Ibrahim et al.[29]	Secure Wireless Networks	Security is improved
6	Chen et al. [30]	AES-128	Encryption Time 61573618 for 1021kb
7	Chen et al. [30]	Chaos-AES-128	Encryption Time 65164900 for 1021kb
8	E et al. [31]	chaos encryption and hybrid encryption	Information Entropy is 5.15996 for original entropy 5.15996.
9	Banerjee et al. [32]	MWFES Ver-I	Strong protection in case of brute force attack.
10	Sandhya et al. [33]	Image Encryption Algorithm Using Chaos	larger key space and a high key sensitivity

V. CONCLUSION AND FUTURE DIRECTION

Based on the study and discussion in the manuscript we have suggest image conversion of the textual data which is further subdivided in several images and after randomization it will be send to the authorized user to get it decrypted. Our study also suggest the scope of email encryption so that if it opened by any unauthorized access, still they do not steal the content and the authorization will be protected in the future. The study also suggests the future hybridization of encryption techniques.

REFERENCES

[1] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems, NIST Publication 800-30, July, 2002.

[2] Steve Elky, an Introduction to Information System Risk Management, SANS Institute InfoSec Reading Room, May, 2006.

[3] M. A. Rahman and Ehab Al-Shaer, A Declarative Approach for Modeling and Verification of Network Access Control Policies, In 12th IM, 2011.

[1] Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison Wesley, 2007.

[2] S. Noel et al., Efficient Minimum-cost Network Hardening via Exploit Dependency Graphs, the 19th Annual Computer Security Applications Conference, 2003.

[3] Xinming Ou, S. Govindavajhala, and A. W. Appel, MulVAL: A logic based network security analyzer, USENIX Security Symposium, 2005.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

[4] P Raviraj and MY Sanavullah, (2007) 'The modified 2D-Haar Wavelet Transformation in image compression "Middle East Journal of Scientific Research, Vol: 2 , Issue: 2,pp 73-78,ISSN 1990-9233.

[5] Jonathan M.Blackedge,Musheer Ahmed ,Omar Farooq(2010) "Chaotic image encryption algorithm based on frequency domain scrambling" ,School of Electrical Engineering systems Articles, Dublin Institute of Technology.

[6] G. K. Kharate, A. A. Ghatol and P.P.Rege, (2005) "Image Compression Using Wavelet Packet Tree", ICGST-GVIP Journal, Volume Issue (7).

[7] David F. Walnut,(2002) "Wavelet Analysis", Birkhauser, ISBN-O- 8176-3962-4.

[8] Musheer Ahmed, Mshamsher Alam(2009) "A new algorithm of encryption and decryption of images using chaotic mapping" International Journal on computer science and engineering, vol 2, pp46-50.

[9] Zaidan, B., Zaidan A., Al-Frajat, A., Jalab, H.,(2010) on the differences between hiding Information and cryptography techniques: An Overview. Journal of Applied Sciences 10(15).

[10] Singh, A., Gilhorta, R. (2011) Data security using private key encryption system based on arithmetic coding. International Journal of Network Security and its Applications (IJNSA), 3(3).

[11] Kiran Kumar, M., Mukthyar Azam, S., and Rasool, S. (2010) Efficient digital encryption algorithm based on matrix scrambling technique. International Journal of Network Security and its Applications (IJNSA), 2(4).

[12] Lakhtaria K. (2011) Protecting computer network with encryption technique: A Study. International Journal of u- and e-service, Science and Technology 4(2).

[13] Long Bao, Yicong Zhou,C. L. Philip Chen," A New Chaotic System for Image Encryption", 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China.

[14] Ahmad Abusukhon and Mohammad Talib, "A Novel Network Security Algorithm Based on Private Key Encryption", IEEE 2012.

[15] Anal Paul, Nibaran Das and Agyan Kumar Prusty, "An Advanced Gray Image Encryption Scheme by Using Discrete Logarithm with Logistic and HEH64 Chaotic Functions", IEEE 2012.

[16] Mohammad Ashiqur Rahman and Ehab Al-Shaer, "A Formal Approach for Network Security Management Based on Qualitative Risk Analysis", IEEE 2013.

[17] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES", IEEE 2013.

[18] Zhang, Jianhong, Zhipeng Chen, and Min Xu. "On the security of ID-based multi-receiver threshold signcryption scheme." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1944-1948. IEEE, 2012.

[19] Ahirwal, Ramratan, Anjali Jain, and Y. K. Jain. "Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation." International Journal of Computer Applications 62, no. 9 (2013): 41-48.

[20] Sethi, Nidhi, and Deepika Sharma. "A new cryptology approach for image encryption." In Parallel, Distributed and Grid Computing, IEEE 2nd International Conference on, pp. 905-908. 2012.

[21] Sathishkumar, G. A., Srinivas Ramachandran, and K. Bhoopathy Bagan. "Image encryption using random pixel permutation by chaotic mapping." In Computers & Informatics (ISCI), 2012 IEEE Symposium on, pp. 247-251. IEEE, 2012.

[22] Ren, Wuling, and Zhiqian Miao. "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication." In Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on, pp. 221-225. IEEE, 2010.

[23] Surya Prabha.U.S, Marikkannu.P, Arul Vineeth.A.D," Cipher text Policy Attribute Set Based Encryption with One-Fold Data Access in Cloud", International Journal of Advanced Computer Research (IJACR) ,Volume-4, Number-1, Issue-14 ,March-2014.

[24] Rajavel, D., and S. P. Shantharajah. "Cubical key generation and encryption algorithm based on hybrid cube's rotation." In Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on, pp. 183-187. IEEE, 2012.

[25] Li, Xiang, Junli Chen, Dinghu Qin, and Wanggen Wan. "Research and Realization based on hybrid encryption algorithm of improved AES and ECC." In Audio Language and Image Processing (ICALIP), 2010 International Conference on, pp. 396-400. IEEE, 2010.

[26] Mohammed A.M. Ibrahim," Utilization of Secure Wireless Networks as Environment for Learning and Teaching in Higher Education", International Journal of Advanced Computer Research (IJACR), Volume-4, Number-1, Issue-14, March-2014.

[27] Chen, Yi, Hong Chen, Hongqian Chen, and Xianchen Cheng. "Research on data encryption techniques for distributed interactive simulation network." In Computer Application and System Modeling (ICCASM), 2010 International Conference on, vol. 5, pp. V5-676. IEEE, 2010.

[28] Xu, E., Liangshan Shao, Guanghui Cao, Yongchang Ren, and Tao Qu. "A new method of information encryption." In Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on, vol. 4, pp. 583-586. IEEE, 2009.

[29] Prabal Banerjee, Purnendu Mukherjee, Asoke Nath, " Modified Multi Way Feedback Encryption Standard (MWFES) Ver-I ", International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-13, December-2013, pp.344-351.

[30] Sandhya Rani M.H., K.L. Sudha, " Design and Implementation of Image Encryption Algorithm Using Chaos " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.660-664.