Securing The Analysed Data Using Rjb21 Algorithm

R. Jaichandran[1], S. Leelavathy[3], E. Muhammed Mahsoos[4], N. Nithya [5], and B. Akash[6]
[1,3,4,5,6] *Department Of Computer Science And Engineering*
Aarupadai Veedu Institute Of Technology
Vinayaka Mission'S Research Foundation
Paiyanoor-603 104, Tamil Nadu, India.

[1]*rjaichandran@avit.ac.in,* [3]*leelavathy@avit.ac.in,* [4]*Mohammedmahsoos22@gmail.com,*
[5]*nithyan542@gmail.com,* [6]*akashb369@gmail.com*

Dr. Avinash Sharma[2**]

[2]*Professor, CSE Department, M.M. Deemed to be University, Mullana, Haryana, India, 133207*
asharma@mmumullana.org
*Corresponding Author: Dr. Avinash Sharma[2]***

Abstract.
The current world is information world; without this information can't make due in present stage. This information created more from web- based media; this media information is public information; This public infor- mation did not have well security; so we applying the proposed method and it has 2 steps; 1.Addition property in matrix; 2. Using prime numbers in qua- dratic equations. The proposed method gives well security while comparing with Salsa method.
Keywords. Associative Property, RJB21, Salsa, Encryption, Decryption.

1. INTRODUCTION

The current world is information world; without this information can't make due in present stage. This information created more from web-based media; this media information is public information; This public information did not have well security; so to conquer this matter we apply the Salsa strategy. This strategy effectively hack the information from the programmers.The additional rotations XOR for ChaCha is fault attack [1]. This author is used new hash concept for key guessing and halting condition [2]. Author was introduced thw bricklayer attack for analysis of ChaCha [3]. They mainly focuse the security for Double A [4]. They made new design for secure fast and flexible algorithm [5]. SRB18 method used to give security for data [6]. SRB21 method used to give security for data [7]. CBB21 method used to provide security for data [8]. CBB22 method used to provide security for data [9]. Introduced the new method RJB21(Rajaprakash Jaichandran and Bagath Basha) 21 for this problem.

2. METHODS

Associative property of addition (CP): This property discuss in Table 1 and Table 2.

3. ENCRYPTION

"A is analyzed matrix"; and "B is secret matrix". [10]

"Equation (1)"

$$A=\begin{pmatrix}21 & 22 & 23\\ 24 & 25 & 26\\ 27 & 28 & 29\end{pmatrix} B=\begin{pmatrix}32 & 34 & 33\\ 35 & 36 & 31\\ 37 & 39 & 38\end{pmatrix} C=\begin{pmatrix}49 & 47 & 48\\ 46 & 44 & 45\\ 42 & 43 & 41\end{pmatrix}$$

$$AP=\begin{pmatrix}21+32 & 22+34 & 23+33\\ 24+35 & 25+36 & 26+31\\ 27+37 & 28+39 & 29+38\end{pmatrix}+\begin{pmatrix}49 & 47 & 48\\ 46 & 44 & 45\\ 42 & 43 & 41\end{pmatrix}$$

$$AP=\begin{pmatrix}53 & 56 & 56\\ 59 & 61 & 57\\ 64 & 67 & 67\end{pmatrix}+\begin{pmatrix}49 & 47 & 48\\ 46 & 44 & 45\\ 42 & 43 & 41\end{pmatrix}$$

$$AP=\begin{pmatrix}53+49 & 56+47 & 56+48\\ 59+46 & 61+44 & 57+45\\ 64+42 & 67+43 & 67+41\end{pmatrix} AP=\begin{pmatrix}102 & 103 & 104\\ 105 & 105 & 102\\ 106 & 110 & 108\end{pmatrix}$$

"Equation (2)"

"p=2,q=3, r=7"

"EM=36855654"

"Pairs (3, 6), (8, 5), (5, 6) and (5, 4)."

"Pair-1(3, 6)"

$$EM=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 102\\ 105 & 110 & 108\end{pmatrix}$$

"Pair-2(8, 5)"

$$EM=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 108\\ 105 & 110 & 102\end{pmatrix}$$

"Pair-3(5, 6)"

$$EM=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 105\\ 108 & 110 & 102\end{pmatrix}$$

TABLE 1. RJB21 Secure Encryption

STEPS	RJB21 SECURE ENCRYPTION
i	"The data analyzed from social data".
ii	"The data will form a matrix".
iii	"The associative property (AP) is applied in the matrix AP "$AP = A + (B + C) = (A + B) + C$" **(1)**
iv	"$EM = (-p \pm \sqrt{(p^2) - 4qr})/2q$. where EM is encrypted matrix" **(1)**
v	" To form a single row for merged numbers".
vi	"To form a pair from left to right from Step 4".
vii	"All pair could be swapped cell values from given matrix".

TABLE 2. RBJ21 Secure Decryption

STEPS	RJB21SECURE DECRYPTION
i	"To analyse theprime in the given matrix".
ii	"$DM2 = (-p \pm \sqrt{(p^2) - 4qr})/2a$. where DM2 is decrypted matrix 2" **(3)**
iii	"To form a single row for merged numbers".
iv	"To form a pair from right to left from Step 3".
v	"All pair could be swapped cell values from given matrix".
vi	"Minus the secret key matrixes C and B with the matrix DM1". $DM\ 2 = DM\ 1 - C$ **(4)** where DM2 is Decrypted Matrix 2 $DM\ 3 = DM\ 2 - B$ **(5)** where DM3 is Decrypted Matrix 3

"Pair-4(5, 4)"

$$EM = \begin{pmatrix} 102 & 103 & 104 \\ 106 & 105 & 105 \\ 108 & 110 & 102 \end{pmatrix}$$

4. DECRYPTION

"Equation (3)"
"p=2,q=3, r=7"
"DM2 = $(-3 \pm \sqrt{(32)} - 4 * 2 * 7)/2 * 2$"
"DM2=$(-3 \pm \sqrt{9 - 56})/4$"
"DM2 = $(-3 \pm \sqrt{47})/4$"
"DM2 = $(-3 \pm 6.85565)/4$"
"DM2 = 36855654."
"Pair of numbers (4, 5), (6, 5), (5, 8), and (6, 3)."

"Pair-1(4, 5)"

$$DM1=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 105\\ 108 & 110 & 102\end{pmatrix}$$

"Pair-2(6, 5)"

$$DM1=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 108\\ 105 & 110 & 102\end{pmatrix}$$

"Pair-3(5, 8)"

$$DM1=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 102\\ 105 & 110 & 108\end{pmatrix}$$

"Pair-4(6, 3)"

$$DM1=\begin{pmatrix}102 & 103 & 104\\ 105 & 105 & 102\\ 106 & 110 & 108\end{pmatrix}$$

"Equation (4)"

”DM2 = DM1 − C”

$$DM2=\begin{pmatrix}102 & 103 & 104\\ 105 & 105 & 102\\ 106 & 110 & 108\end{pmatrix}-\begin{pmatrix}49 & 47 & 48\\ 46 & 44 & 45\\ 42 & 43 & 41\end{pmatrix}$$

$$DM2=\begin{pmatrix}102-49 & 103-47 & 104-48\\ 105-46 & 105-44 & 102-45\\ 106-42 & 110-43 & 108-41\end{pmatrix} DM2=\begin{pmatrix}53 & 56 & 56\\ 59 & 61 & 57\\ 64 & 67 & 67\end{pmatrix}$$

"Equation (5)"

"DM3 = DM2 − B"

$$DM3=\begin{pmatrix}53 & 56 & 56\\ 59 & 61 & 57\\ 64 & 67 & 67\end{pmatrix}-\begin{pmatrix}32 & 34 & 33\\ 35 & 36 & 31\\ 37 & 39 & 38\end{pmatrix}$$

$$DM3=\begin{pmatrix}53-32 & 56-34 & 56-33\\ 59-35 & 61-36 & 57-31\\ 64-37 & 67-39 & 67-38\end{pmatrix} DM3=\begin{pmatrix}21 & 22 & 23\\ 24 & 25 & 26\\ 27 & 28 & 29\end{pmatrix}$$

5. CONCLUSION

Prediction of an environmental parameter is possible using sensing [16-20] or IoT [21-23] mechanism but prediction of security is based on features of data or Big Data[24,25]. Different kinds of prediction possible using various techniques including ML [26,27].

The current world is information world; without this information can't make due in present stage. This information created more from web-based media; this media information is public information; This public information did not have well security; so we applying the RJB21 method and it has 2 steps; 1.Ad- dition property in matrix; 2. Using prime numbers in quadratic equations. The RJB21 method gives well security while comparing with Salsa method.

REFERENCES

[1] P. A. BABU AND J. J. THOMAS: *A PRACTICAL FAULT ATTACK on ARX-like Ciphers with A CASE Study on CHACHA20*, Wo. on Fa. Di. and To. in Cr. (2017), 33-40.

[2] S. V. D. KUMAR, S. PATRANABIS, J. BREIER, D. MUKHOPADHYAY, S. BHASIN, A. CHATTOPADHYAY, AND A. BAKS: *Freestyle, A RANDOMIZED version of CHACHA for resisting offline brute-force AND DICTIONARY ATTACKS*, IE. tr. on In. Fo. and Se. (2018).

[3] A. ADOMNICAI, J. J. A. FOURNIER, AND L. MASSON: *BRICKLAYER ATTACK: A Side- CHANNEL ANALYSIS on the CHACHA QUARTER Round*, Pr. in Cr. In., Le. No. in Co. Sc., Sp. 65-84.

[4] B. MAZUMDAR, S.K. S. ALI AND O. SINANOGLU: *Power ANALYSIS ATTACKS on ARX: An APPLICATION to SALSA20*, On-. Te. Sy. IE. (2015), 40-43.

[5] C. WATT, J. RENNER, N. POPESCU, S. CAULIGI, AND D. STEFAN: *CT-WASM: Type- Driven Secure CRYPTOGRAPHY for theWeb Ecosystem*, Pr. ACM Pr. La. PO. (2019), 77:1-77:29.

[6] C. BAGATH BASHA, S. RAJAPRAKASH: *ENHANCING The Security Using SRB18 Method of Embedding Computing*, Mir. and Mic 103125, (2020).

[7] C. B. BASHA, S. RAJAPRAKASH: *Securing Twitter DATA Using Srb21 PHASE I Method- ology*, Int. Jou. of Sci. and Tec. Res. **8**(12) (2019), 1952–1955.

[8] C. B. BASHA, S. RAJAPRAKASH: *Applying The CBB21 PHASE 2 Method For Securing Twitter ANALYSED DATA*, Adv. In Mat. : Sci. Jou. **9**(3) (2020), 1085-1091.

[9] C. B. BASHA, S. RAJAPRAKASH, V. V. A. HARISH, M. S. KRISHNA, K. PRABHAS: *Securing Twitter ANALYSED DATA Using CBB22 Algorithm*, Adv. In Mat. : Sci. Jou. **9**(3) (2020), 1093-1100.

[10] C. B. BASHA, K. SOMASUNDARAM: *A COMPARATIVE Study of Twitter Sentiment ANAL- ysis Using MACHINE LEARNING Algorithms in Big DATA*, Int. Jou. of Rec. Tec. and Eng. **8**(1) (2019), 591-599.

[11]Somasekar, J. & Sharma, A. & Reddy, N. & Reddy, Y.. (2020). IMAGE ANALYSIS FOR AUTOMATIC ENUMERATION OF RBC INFECTED WITH PLASMODIUM PARASITES-IMPLICATIONS FOR MALARIA DIAGNOSIS. Advances in Mathematics: Scientific Journal. 9. 1221-1230. 10.37418/amsj.9.3.48.

[12] A. SHARMA1 AND J. SOMASEKAR "Contrast Image Construction Technique for Medical Imaging" published in Advances in Mathematics: Scientific Journal (Adv. Math., Sci. J.) vol-9-no-6-2020 (pp 3325–3329)

[13] *Rohini Goel, Avinash Sharma, and Rajiv Kapoor,* "Object Recognition Using Deep Learning" published in Journal of Computational and Theoretical Nanoscience Vol. 16, 4044–4052, 2019

[14] Santosh, Mamta & Sharma, Avinash. (2019). A Proposed Framework for Emotion Recognition Using Canberra Distance Classifier. Journal of Computational and Theoretical Nanoscience. 16. 3778-3782. 10.1166/jctn.2019.8250.

[15] Mamta Santosh, Avinash Sharma, "Facial Expression Recognition using Fusion of LBP and HoG Features" published in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019

[16] Varsha, N. Kumar, Energy Efficient TABU Optimization Routing Protocol for WSN, Ingeniería Solidaria, Universidad Cooperativa de Colombia, Issue- 33, July 2020.

[17] G.Arora, A.Kumar, Versha, N.Kumar, "Swarm Intelligence based QoS optimized routing in WSN", Test Engineering & Management, Vol.-82, 2020. pp-12880-12885.

[18] Varsha, M. B., Kumar, M., & Kumar, N. Hybrid TABU-GA Search For Energy Efficient Routing In WSN. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019. P.-3250-3256.

[18] Varsha, M. B., Kumar, M., & Kumar, N. Development of QoS optimized routing using Artificial bee colony and TABU-GA with a mobile base station in Wireless Sensor Network, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November 2019.

[19] Awadhesh Kumar Maurya,Varsha, Neeraj, Ajay Kumar, Neeraj Kumar, "Improved chain based cooperative routing protocol in wsn", FEST, Journal of Physics: Conference series, IOP Publishing, 1478,1-8, 13/05/2020.

[20] N. Kumar, A. Agrawal, R. A. Khan, "METHWORK: An Approach for Ranking in Research Trends with a Case Study for IoET, Recent advances in Computer Science and Communication (formerly Recent Patents on Computer Science), 2019.

[21] Neeraj Kumar; Paresh Goyal; Gayatri Kapil; Alka Agrawal; Raees A Khan, "Flood Risk Finder for IoT based Mechanism using Fuzzy Logic", Materials Today: Proceedings, Elsevier, 2020.

[22] Kumar, Neeraj, Alka Agrawal, and R. A. Khan. "Cost estimation of cellularly deployed IoT-enabled network for flood detection." *Iran Journal of Computer Science* , issue 2, no. 1 (2019), Springer Nature: 53-64.

[23] V. Velvizhi; Satish R Billewar; Gaurav Londhe; Pravin Kshirsagar; Neeraj Kumar, "Big Data for Time Series and Trend Analysis of Poly Waste Management in India", Materials Today: Proceedings, Elsevier, 2020.

[24] G. Arora, A. K. Maurya, N. Kumar, A. K. Mishra, "Application of big data generated by IoT environment for HealthCare using Voice Recognition", International journal of research in engineering, IT and Social Sciences, vol.-08, issue-11, November 2018, page. 132-136.

[25] Manoj Diwakar, Amrendra Tripathi, Kapil Joshi, Minakshi Memoria , Prabhishek Singh, Neeraj kumar, "Latest Trends on Heart Disease Prediction using Machine Learning and Image Fusion", Materials Today: Proceedings,Elsevier, 2020.

[26] Parth Wadhwa; Aishwarya; Amrendra Tripathi; Prabhishek Singh; Manoj Diwakar; Neeraj Kumar, "Predicting the Time Period of Extension of Lockdown due to Increase

in Rate of COVID-19 Cases in India using Machine Learning", Materials Today: Proceedings Elsevier, 2020.