The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 1, February 2025
https://doi.org/10.33022/ijcs.v14i1.4660

Control the Sensitivity of the Encryption Key to Ensure the Security of Big Data

Wafaa Ali[1], Walaa Alajali[2], Abdulrahman D. Alhusaynat[3]
wafaa-a@utq.edu.iq[1], walaakhshlan@utq.edu.iq[2], rahmandakhil2@gmail.com[3]
[1,2] Thi-Qar University, Education College for Pure Science, Nassiriya, Thi-Qar , 64001, Iraq.
[3] Thi- Qar Education Directorate, Nassiriya, Thi-Qar, 64001, Iraq.

Article Information

Received : 22 Jan 2025
Revised : 31 Jan 2025
Accepted : 7 Feb 2025

Keywords

Big data, Encryption, Key sensitivity, Data security.

Abstract

With the increasing technological development that has led to the complexity of big data systems, the importance lies in the challenge that ensures the security of sensitive information. Encryption is one of the basic methods used to protect data, hence the importance of the encryption key and its sensitivity, which play a vital role in the strength of encryption. Encryption sensitivity is the simple change in the encryption key that produces a very different encrypted text. This study is concerned with methods of controlling the sensitivity of the encryption key and its effect on the strength of encryption of big data. This context is in line with the nature of cloud data and the focus on the attacks that this data suffers from, such as brute-force attacks and statistical attacks. The research discusses the components that make up the encryption key, logistics maps, and chaos. The results reached by the study proved the merit of the research in terms of accuracy 10^{15} and appropriate key sensitivity 2^{128}. This study discussed future challenges and the possibility of using artificial intelligence algorithms and adaptive security algorithms and solving quantum encryption problems.

A. Introduction

In the era of big data and the expansion of data in terms of volume, speed and type, challenges have arisen in the security of big data. With the increasing use of data in all fields of military, health and communications, cyber-attacks pose a major threat to the confidentiality and availability of data. Hence, encryption is considered an important and effective defense to prevent unauthorized access or theft of sensitive data, and plays an important role in protecting big data. Complex algorithms in encryption are not enough, and the strength of the algorithm is not limited to its complexity, but the sensitivity of the encryption key plays a fundamental role in the complexity of encryption. Strong and effective algorithms are useless if the encryption key is compromised or has little protection [1].

The sensitivity of the encryption key depends on the security of the encrypted data and its degree of sensitivity determines the degree of complexity of the encryption process and the integrity and confidentiality of sensitive data depends on it. In the context of big data, there are several stages that data goes through, and at each stage the data is threatened and vulnerable to attack, such as the transmission stage, the distribution stage, the storage stage, the cloud computing stage, and the real-time processing stage. The sensitivity of the encryption key is important at all stages of the big data infrastructure. Traditional technologies may not be scalable at a certain stage or several stages, but they must be impenetrable, especially in environments such as these because they deal with bytes of data that are technically and geographically distributed [2].

Due to the development of information and communication technologies, attackers have become more sophisticated and experienced in exploiting vulnerabilities in confidential data, so many attacks have become dangerous such as side-channel attacks, brute force attacks, and key reuse attacks. Hence, the need to design advanced encryption strategies and enhance the sensitivity of keys to confront and withstand attacks. This type of development requires advanced methods for generating keys and distributing them throughout the data flow and their rotation, with encryption methodologies that adapt to changes in encryption keys and respond effectively to attacks in real time [3].

In this paper, the role of encryption key sensitivity and its impact on securing sensitive data in term of big data are explored. It works to improve a new strategy for controlling the key, and organize encryption in a new and effective way. The problem statements that this study relies on are the weakness of traditional encryption techniques and the development of the concept of encryption among attackers. As well as the development of the infrastructure of big data and its handling of data acquisition in real time, in addition to the diversity in data transmission through the stages of big data such as cloud storage, topographic distribution of data and data collection, all of which called for a major challenge in designing a highly sensitive key to encrypt data [4]. The inability of some traditional methods to stand up to attacks launched by intruders has put us in front of a new kind of challenge with the development of data science. The main objectives of this study is to develop a method for data encryption that is suitable for the big data environment, in addition to creating a complex encryption key that can be controlled by future variables to be more reliable than before, as well as integrating the encryption method through the evaluation of the results we reach.

Challenges of Big Data Security

Privacy Risks: Big data provides convenience for people who deal with it, but in return, there are harassments they face from intruders. Privacy protection is a requirement that must be provided to users, otherwise the data will be threatened. The data that is protected is not only private, but also viewing and analyzing it allows the counterparty to know its future trends and predictions as well. People's spending methods can be determined and controlled, and certain intellectual tendencies of people can also be known through their stored historical information. In this case, the security of big data is a priority in our daily lives [5].

Big Data Privacy Protection: due to the widespread dissemination of data and its transfer between sites, the lack of technical support, weak supervision and unauthorized access lead to the weakness of the data and thus its exposure to catastrophic attacks. Reducing the value of data leads to a negative impact on individuals and society, which in turn leads to large economic losses.

Data Security Threats: Since the development of big data and the widespread use of the Internet, mobile data terminals have become threatened, and mobile and big data have become a concern for people because of the insecurity of these terminals. Due to the rapid development of smart products, it has caused a great challenge due to the big data terminals being operated by smart devices.

Supervision of Social Network Data: The media created in the era of big data have priority in interpersonal communication. The excessive sharing of data in social media creates a vulnerability for big data by exploiting unauthorized access to tamper with data security. In order to reduce this security vulnerability, we must increase the supervision and management of security data to deprive criminals of the opportunity and minimize losses. People's technological awareness plays an important role in self-prevention of potential attacks.

Characteristics of Big Data

Big data is a term that refers to the huge volume of data that comes from different sources. Traditional techniques fail to manage, analyze and process it. There are specific characteristics of big data through which it can be managed and dealt with properly [6]. We can only understand big data by studying these characteristics and taking them into consideration to be able to deal with it effectively. These characteristics can be summarized as follows:

Volume

The term big data alone refers to the enormous volume of data that is created and stored. This volume continues to grow and increase dramatically as a result of dealing with modern digital devices, Internet of Things devices, and various applications. The volume of data in organizations today is dealing with petabytes or Exabyte and sometimes reaches zettabytes of data, all of which requires distributed databases or cloud storage to store the data. The challenge here is managing this data in real time because traditional methods cannot handle this amount of data.

Velocity

It refers to the speed at which data is generated, processed, and analyzed. Due to the emergence and development of real-time applications such as social media and financial markets trading, which care more about time than anything else, real-time data analysis is required. The challenge is the speed of data generation, which requires effective frameworks that can accommodate this amount of data, such as Apache Kafka and Apache Flink, which aim to make decisions in real time for fraud detection and predictive maintenance.

Variety

It represents the types and formats of different data that come and are generated from several sources. Previously, data is mostly structured and can be formatted and stored in a precise manner in relational databases as rows and columns. However, for big data, it comes in several forms: unstructured, semi-structured, or structured.

- Unstructured data is free and distributed in an irregular manner, such as video, text, audio, and social media data.

- Semi-structured data does not have a fixed and often variable form, such as records and JSON or XML files.

- Structured data is data that is stored in advance and in a specific order, such as tables and databases.

In this case, the challenge is to manage these different formats and integrate them into a unified framework. Therefore, the data must be organized first before merging it.

Veracity

It refers to the reliability and accuracy of data as well as its quality. Data diversity results from the large amount of data and is often incomplete or cluttered. Data that is cluttered or of poor quality leads to making decisions that may be incorrect. The challenges lie in coordinating data to ensure data quality is a priority in big data. This process includes advanced practices for data auditing and maintaining its accuracy.

These characteristics reveal the challenges in big data and provide unique opportunities for dealing with this type of data. Dealing with it must combine the special characteristics to develop it and harness all the capabilities to solve the problems facing big data and benefit from making the right decisions. Figure 1 illustrates the most important characteristics related to big data.

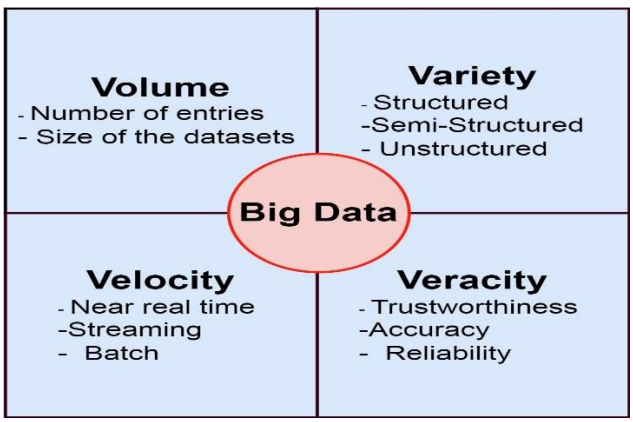

Figure 1. Characteristics of Big Data

As systems and applications that generate big data continue, information security has become a priority that we must consider here. The main source of information security is encryption, and we can consider the sensitivity of the key to be the heart of the encryption process. Any change, even a small one, leads to a completely different encryption, and this has the advantage that even 95% knowledge of the key cannot decrypt it. There are different encryption algorithms such as AES and RSA, and these algorithms show high sensitivity to encryption, which is important in preventing attacks [7]. Due to the huge size of data, its distribution, and the nature of information transmission in it, key sensitivity has become very important.

Many studies have taken into account data security in big data and have been summarized by a number of researchers [8,9,10]. Other studies have focused on data security in general and the encryption methods used in data, whether traditional or massive. A study showed that traditional encryption keys face difficulty in expanding with big data, as many keys must be dealt with to keep pace with the expansion of the data [11]. In the cloud environment, where data is stored in a logical way more than in a physical way, a study is presented on the importance of the encryption key in data security and the difficulty of maintaining it [12]. A study emphasized the importance of the encryption key and its role in bridging security gaps, especially in the physical layer of communications, and how to make controls for key sensitivity [13]. A study developed homogeneous encryption to suit big data and to perform complex mathematical operations without decryption to ensure the complexity of the encryption key [14]. A study emphasized the cost of encryption operations that lack a sensitive encryption key and the extent to which big data affects the workflow in data expansion across the network [15].A new concept that has proven its worth in big data encryption operations is quantum computing. The study emphasized quantum-resistant encryption and its difference from traditional network-based methods and how to protect data from classical and quantum attacks [16]. In a study, quantum key distribution (QKD) was considered as an important and future technology in securing encryption keys and taking advantage of quantum mechanics to detect breaches in networks [17].A study investigated the difference between data security in watermarking and stenography as techniques that can be dealt with in big data but in a different way than with traditional data [18,19]. A study emphasized the importance of using artificial intelligence and its algorithms in maintaining data security because the main goal of data security is to predict and detect attacks and then complicate the encryption solution [20]. Machine learning has been used to improve encryption algorithms in dynamic environments. Encryption requires isolation and classification of the most sensitive data, which is why machine learning has been successful in encryption [21]. Deep learning algorithms have been used to encrypt data in real time and then adjust the sensitivity of the encryption key to withstand potential threats [22].

There are many methods that have been suggested in the literature, and those that are closely related to our study have been presented. In Table 1, we show the most important methods that had an impact through the results reached by the known encryption methods.

Table 1. The Most Important Methods Deal with Big Data and its Applications

Author years	Considerations	Scope	References
2022, 2024	combining cipher-text policy attribute-based encryption (CP-ABE) and advanced encryption standard (AES)	Big data transition and manipulation	[23] [24]
2022	AES is that it uses the same key for both encryption and decryption	Big data within clouding	[25]
2020,2024	Hadoop Distributed File System (HDFS) storage and Attribute Based Honey Encryption (ABHE)	security within physical layer in big data	[26][27]
2024	Advance encryption algorithm without changing key (implicit) AES-SM2 Hybrid Encryption	Moving data within network transection	[28]
2024	Achieving both efficiency and security by Triple Data Encryption Standard (3DES).	Distributed data in warehousing, BIG data and CLOUD computing	[29]
2023	quantum image encryption algorithms based on complex scrambling	Images in big data	[30]
2022	Improve Chaos Encryption (ICE) for complex randomness	Health medical image in the clouding	[31]

B. Research Method

In data security, the main process performed on data is encryption, which converts plain text into unreadable encrypted text. This method ensures data confidentiality in the best possible way. The encryption key plays the main role in this process, which requires confidentiality of changes to the encrypted text. Data comes from different sources, it is generated from applications, sensors or specific storage areas and is transmitted through the network to the destination. During these movements, the data is encrypted. Figure 2 illustrates the structure of data movement through the concept of big data.

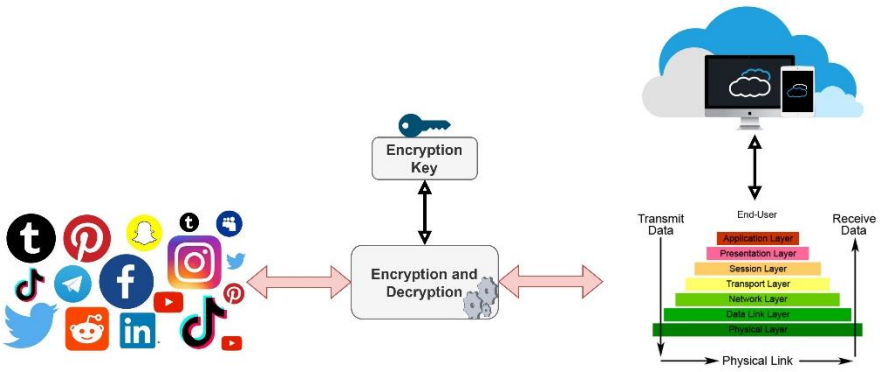

Figure 1. Structure of Big Data Throw Network

Encryption includes two basic operations: confusion and diffusion. The first works to change the positions of letters or words, and the second works to change the value of the bits that make up the letters or words.
First, data samples are taken in equal serial sizes of 2^8 and stored in a vector. The second sample is taken and stored in another vector, and so on until we achieve a 2D matrix. This stage is considered the first, as the even rows are replaced with the odd rows, starting from top to bottom. When finished, work begins on replacing the even columns with the odd columns, from right to left. As illustrated in equation.

$$A_{i,j} = B_{i,(n-j+1)} \quad for\ i = 1 \dots n, j = 1 \dots m \tag{1}$$

Where A is resulting matrix from original matrix B, and can show the process in Figure 3.

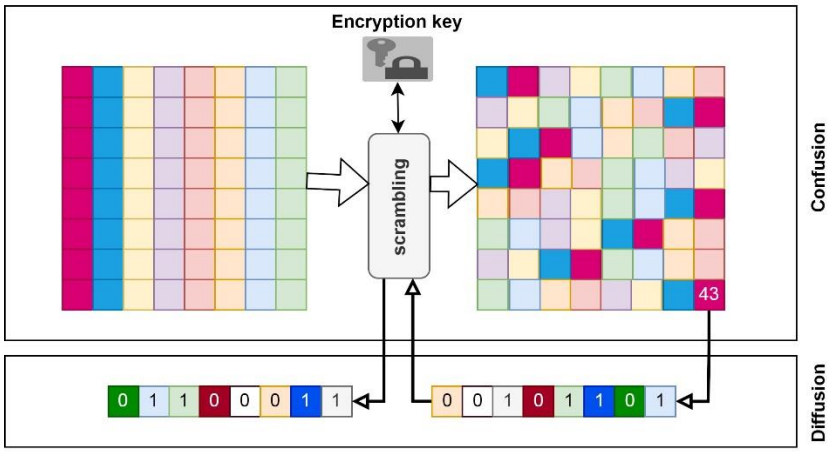

Figure 2. General Encryption Process

Each cell of the matrix consists of one character, and this character is in turn converted to the ASCII system, and then converted to the binary system to be stored in the format 0 and 1 with a size of 28. The bits are also scrambling in

a way called diffusion. Encryption methods work on the basis of complex randomness. Randomness is in the form of randomly generated numbers ranging between 0 and 1. This randomness needs to be improved over previous studies, which increases the sensitivity of the key, which is the basis of encryption methods.

The encryption key generates random numbers equal to the number of numbers to be encrypted. The numbers are stored in vectors in the form of a matrix identical to the plaintext matrix. These random numbers are combined with the previously scattered numbers by XOR to generate the plain text. Figure 4 shows the following process for the scrambling process.

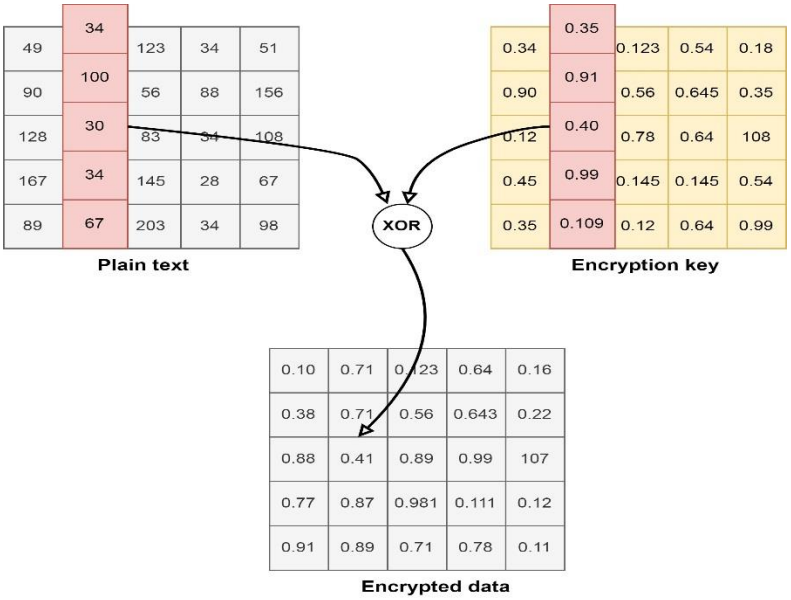

Figure 3. Generated Cipher Data within Encryption

The contribution of this study is in two stages. The first is the scrambling stage, which works on replacing columns and rows. The replacement is in the data locations and the bit locations of the information itself. The second stage is the complexity of the encryption key and increasing its sensitivity by integrating the Henon mapand the logistic map. The complexity of the work on the encryption process works to increase the strength of the encryption. Figure 5 illustrate the contribution to increase key sensitivities.

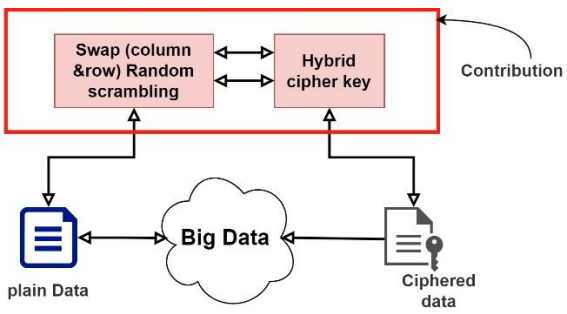

Figure 4. Contribution within Proposed System

In the following section, the results will be explained in detail along with the methods that led to these results. Taking into consideration the difference that the contribution made to this study and its impact on the results.

C. Result and Discussion

Correlation and histogram

In this section, we will list the results and the effect of the proposed method on the result in data encryption. In the confusion part, the goal is to reduce the correlation to the minimum possible between the pixels in the image, and breaking the correlation is done by redistributing the data items and distributing them in the cipher data in a chaotic way.

One of the most successful methods in attacks is the statistical method, and in order to resist this attack, the encryption method must be good. To ensure a good encryption method, the horizontal, vertical, and diagonal data correlation must be calculated in the plain and encrypted data, and the correlations are calculated according to the following equations.

$$Cor = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (2)$$

$$\text{Such as : } D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - x')^2 \quad (3)$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - y')^2 \quad (4)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - x')(y_i - y') \quad (5)$$

Where *(x,y)* is the data item in plain matrix position and (x', y') is the next position in cipher matrix. The confusion step reduces the correlation between adjacent data item in the image as shown in the Table 2 while the entropy will not be affected due to the change in the location.

Table 2. Illustrate the Correlation of Adjacent Items in Cipher Data

			Correlation		
Images	**Type**	**Data Size**	**Horizontal**	**Vertical**	**Diagonal**
Data 1	Normal text	17682 Bytes	-0.000569	0.00232	0.000910
Data 2	Complex	12683 Bytes	0.001282	0.00182	0.003093
Data 3	Normal text	13768 Bytes	0.003469	0.00344	-0.000533
Data 4	Normal text	12666 Bytes	-0.000971	0.00034	-0.00584
Data 5	Complex	16322 Bytes	-0.000775	-0.00956	0.000796
Data 6	Normal text	15672 Bytes	0.000788	0.00568	0.00374
Data 7	Normal text	13451 Bytes	0.000982	-0.00457	0.00323
Data 8	Complex	17345 Bytes	0.000342	0.000239	-0.00765

Data 9	Complex	20762 Bytes	0.00892	0.000233	0.00066
Data 10	Complex	21682 Bytes	-0.00026	-0.00098	-0.00261

In plain text is divided into items, and each item is a word separated from the other by a space. The size of each text varies according to the matrix divisions that are determined in advance by the 2^N, and the numbers that affect the result as well. If the number of numbers exceeds 100 bytes, it is called complex.

Chaotic

Chaos is known to be a widespread phenomenon in most nonlinear systems and is highly sensitive and random in behavior. The logistic map is a quadratic boundary that has been used in cryptography due to its simple application and complex result and can be described in the equation.

$$X_{n+1} = r\mathrm{X_n}(1-\mathrm{X_n}) \quad (6)$$

Consider *r* the control parameter such as $r \in (0,4)$ and *n=1,2,3,... . X1* represent initial condition (seed value) occur ($0< X_1 <1$). And the chaotic will be in value of (between 3.5699 and 4) as shown in Fig. 6.

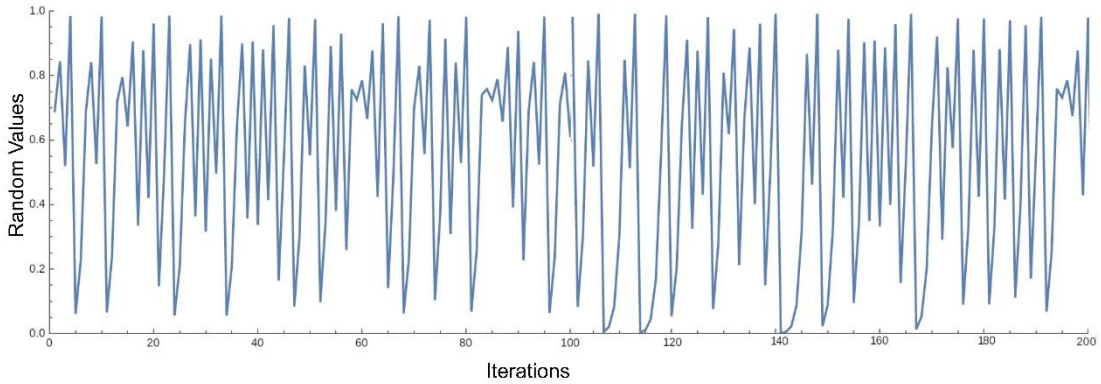

Figure 6. Logistic Map Behavior

In term of cobweb diagram easy can draw the chaotic logistic map as in Fig. 7. The behavior in the form is based on the chaos in the encrypted image, which depends on the method used. The more chaos there is, the more impossible it is to decrypt without the encryption key. Image encryption is considered complex due to the limited dimensions of the image to be encrypted and thus the limited data. But when repeating the training process with many iteration on different data size, we reach a stage where the chaos is almost impossible in order to transfer the data to the other party safely.

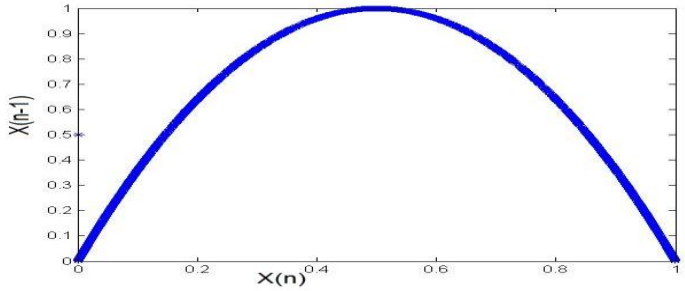

Figure 7. Cobweb Behavior of Complex Chaotic

The main goal of this study is to design a high-level encryption system to ensure the security of data. In order to achieve this goal, the statistical properties of the data, represented by the correlation, must be eliminated. Since the encryption goes through iterations during training process, the complexity can be increased by a good amount without losing the information in the data. Any process that includes training procedures achieves the highest desired result because the encryption process that simulates the best of what was entered as the final result is at a high level of accuracy, as shown in the Fig. 8.

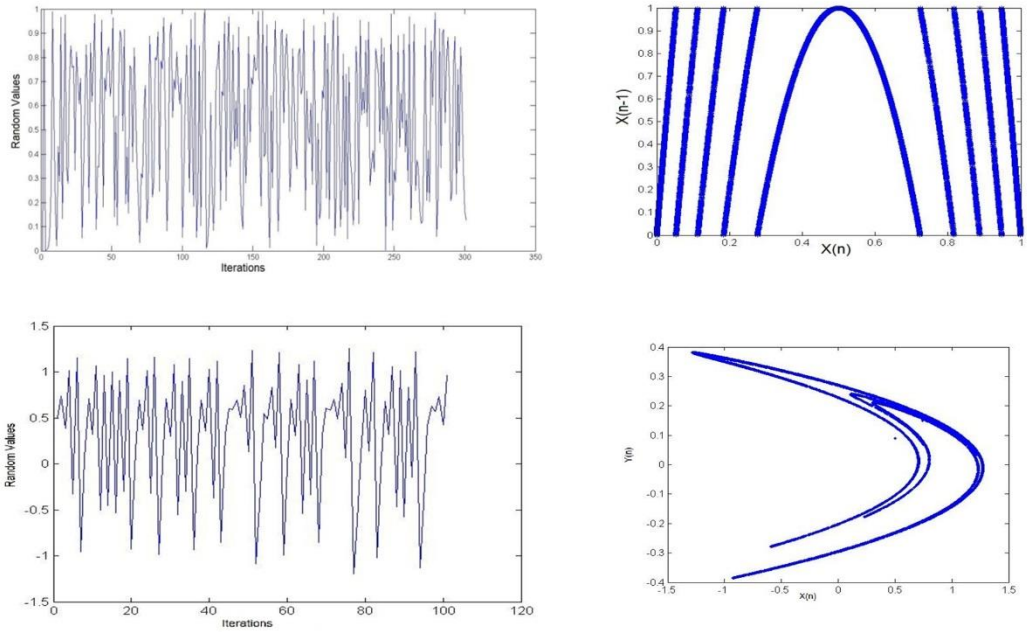

Figure 8. Behavior of Chaos in Proposed Method

Entropy

The change from the degree of certainty can be measured by entropy. Entropy is often defined as the degree of randomness or disorder of the system. Hence, entropy came as a standard to measure the degree of randomness in the encrypted data. In the case of the closeness of the items in different size, the entropy is close or most likely = 8, and even in the case of the big data, when the data value reach to the maximum, the entropy = 8, so the entropy of the encrypted data is 8, and this is what the proposed method did, which relied on the number of training times to get the best result. Entropy can find by this equation:

$$H(m) = \sum_{i=0}^{M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (7)$$

Considering *M* is the total number of items (word), $P(m_i)$ is the possibility of occurrence symbol m_i in binary mode. Then the perfect of entropy in data encryption is 8. In Table 3 shows some encrypted data with their entropy.

Table 3. Entropy with Different Iterations and Complex Data

Images	Image Size	Entropy
Data 1	2^{512}	8
Data 2	2^{128}	8
Data 3	2^{256}	8
Data 4	2^{128}	8
Data 5	2^{128}	8
Data 6	2^{512}	8

From here we know that the encryption system is important in securing data and also depends on the method used. The data from the dataset is encrypted and also produces a cipher text and is sent to the other party and at the other party it starts reversing the encryption method to form and return the original image as in the Figure 9.

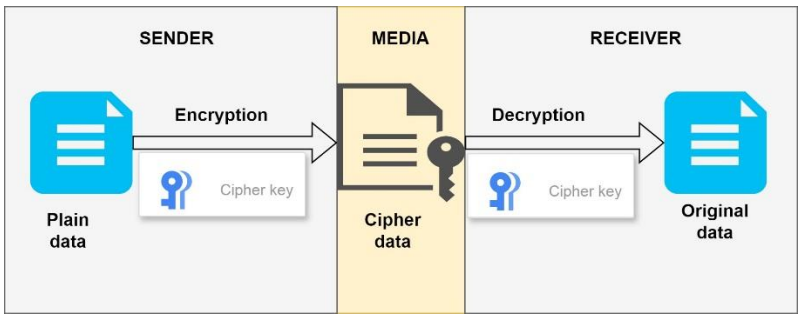

Figure 9. Encryption Strategy

Analysis of key space

The ideal use of key generators for encryption requires a large key space to make attacks impossible, including brute force or exhaustive attacks. A small space size such as 2^{128} or less is insecure. In this study, several chaotic maps are used for the security of the key generator and the precision is equal to (10^{15}). To illustrate how to calculate the key space, we consider Table 4.

Table 4. Key Space Used in This Study

Chaotic Map	Initial Values Number	Key Space in Decimal	Key Space in Binary
Henon	2	10^{30}	$2^{99.6}$
Amended Beroulli	2	10^{30}	$2^{99.6}$
Tinkerbell	2	10^{30}	$2^{99.6}$
Burger	2	10^{30}	$2^{99.6}$
Ricker	1	10^{15}	$2^{49.8}$

Total	9	10^{135}	2^{448}

In this study, the key space length is 2^{448} which is considered the possible key set. This value is very large and therefore the proposed method can withstand brute force attacks and it is impossible to break this encryption method. In the initial state, Henon map is used as an input to encrypt the method in addition to other methods and from it the control sets of keys are increased.

One of the signs of a successful encryption method is that the changes in the initial key are small, reaching one bit to produce the cipher text. In this study, the key space is a combination of several conditions and its accuracy is equal to $10^{\wedge 15}$. To check the sensitivity of the key, we will choose a specific text and a slight change will be made to each of the initial conditions. After encryption, the change in the conditions will be measured and this process will be repeated several times (9) to ensure the sensitivity of the encryption key. After analyzing the text, we will see the slight change in the sensitivity of the key with each use.

Analysis of sensitivity

To perform key sensitivity analysis, at the beginning choosing of plain text with size of 143522 Bytes will done, then initiate condition will be as:

Henon with 1st initial condition of = 0.700000000000000
Henon with2nd initial condition of = 0.500000000000000
Tinkerbell 1st initial condition of = 0.100000000000000
Tinkerbell 2nd initial condition of = 0.500000000000000
Amended Bernoulli with 1st initial condition of = 0.950000000000000
Amended Bernoulli with 2nd initial condition of =0.070000000000000
Ricker with initial condition of = 0.100000000000000
Burgers with 1st initial condition of = 0.100000000000000
Burgers with 2nd initial condition of = 0.100000000000000

Through the initial conditions and circumstances, the cipher text is re-executed using the proposed method with slight differences in the conditions to evaluate the key sensitivity and also evaluate the correlation coefficient. Fig. 10 represents the plain text and the cipher text with the best possible sensitivity key.

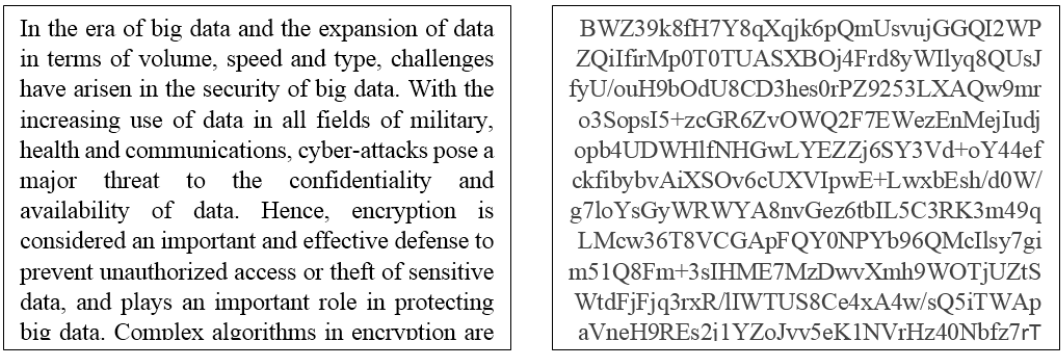

Figure 10. Encryption Example with Key Sensitivity

D. Conclusion

Ensuring data security in a big data environment is of paramount importance. Key sensitivity is a critical issue that has priority in maintaining data security. Controlling the sensitivity of the encryption key helps to increase the strength of the encryption. The purpose of increasing the sensitivity of the encryption key is the basis for resisting brute force attacks and statistical attack threats. Chaos, randomness and logistic maps provide a mechanism for the strength of the encryption key.

With the increasing volume and variety of big data, challenges related to cryptographic key sensitivity have become increasingly important. The big data cloud environment requires secure key storage and encryption methods to avoid hacking and unauthorized access. The current study has proven its worth in encryption strength through evaluations and according to the followed standards, as it achieved an accuracy of 10^{15} as well as an encryption key sensitivity of 2^{128}, which is considered a very good result in the context of encryption, especially for big data.

As big data is rapidly expanding and the work on data processing is increasing, future research is necessary to develop mechanisms to enhance the sensitivity of encryption keys to ensure the security of sensitive data. One of the future areas is quantum-resistant encryption, which is important for quantum computing. Also, machine learning and deep learning techniques are promising algorithms that can be used to improve the sensitivity of encryption keys by predicting the best information to make encryption strong. Addressing future areas related to big data ensures that the encryption strength remains flexible in the face of threats and technological advances.

E. References

[1] Srihith, I. D., Donald, A. D., Srinivas, T. A. S., Thippanna, G., & Anjali, Locking down big data: "*a comprehensive survey of data encryption methods*". International Journal of Advanced Research in Science, Communication, and Technology, 3(2), 84-93, 2023

[2] Balamurugan, V., Karthikeyan, R., Sundaravadivazhagan, B., & Cyriac, R., "*Enhanced Elman spike neural network based fractional order discrete Tchebyshev encryption fostered big data analytical method for enhancing cloud data security*". Wireless Networks, 29(2), 523-537, 2023.

[3] Wong, M. L., & Arjunan, T.," *Real-Time Detection of Network Traffic Anomalies in Big Data Environments Using Deep Learning Models*". Emerging Trends in Machine Intelligence and Big Data, 16(1), 1-11, 2024.

[4] Duan, X., Li, Y., Liu, C., Li, X., Liu, W., & Li, G., " Research on the method of selecting the optimal feature subset in big data for energy analysis attack". In *International Conference on Digital Forensics and Cyber Crime* (pp. 109-126). Cham: Springer International Publishing, 2021.

[5] Tiwari, A., Sharma, N., Kaushik, I., & Tiwari, R. ," Privacy issues & security techniques in big data". *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 51-56). IEEE, 2019.

[6] Ghasemaghaei, M., & Calic, G.,"*Assessing the impact of big data on firm innovation performance: Big data is not always better data*". Journal of business research, 108, 147-162, 2020.
[7] Ramachandra, M. N., Srinivasa Rao, M., Lai, W. C., Parameshachari, B. D., Ananda Babu, J., & Hemalatha, K. L.," *An efficient and secure big data storage in cloud environment by using triple data encryption standard*". Big Data and Cognitive Computing, 6(4), 101, 2022.
[8] Attaallah, A., Alsuhabi, H., Shukla, S., Kumar, R., Gupta, B. K., & Khan, R. A., "*Analyzing the Big Data Security Through a Unified Decision-Making Approach*". Intelligent Automation & Soft Computing, 32(2), 2022.
[9] Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H.," *Application of big data and machine learning in smart grid, and associated security concerns*": A review. *Ieee Access*, *7*, 13960-13988, 2019.
[10] Singh, A., Kumar, A., & Namasudra, S. DNACDS*:" Cloud IoE big data security and accessing scheme based on DNA cryptography*". Frontiers of Computer Science, 18(1), 181801, 2024.
[11] Xiong, Q., Zhang, X., Liu, W., Ye, S., Du, Z., Liu, D., ... & Yao, X.," *An efficient row key encoding method with ASCII code for storing geospatial big data in HBase*". Isprs International Journal of Geo-Information, 9(11), 625, 2020.
[12] Sandhu, A. K.," *Big data with cloud computing: Discussions and challenges*". Big Data Mining and Analytics, 5(1), 32-40, 2021.
[13] Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A.," *A survey of IoT security based on a layered architecture of sensing and data analysis*". *Sensors*, *20*(13), 3625, 2020.
[14] Hamza, R., Hassan, A., Ali, A., Bashir, M. B., Alqhtani, S. M., Tawfeeg, T. M., & Yousif, A.," *Towards secure big data analysis via fully homomorphic encryption algorithms*". Entropy, 24(4), 519, 2022.
[15] Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., ... & Gupta, A.," *Big data architecture for network security*". Cyber Security and Network Security, 233-267, 2022.
[16] Käppler, S. A., & Schneider, B., "*Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms*". Proceedings of the Society, 84, 61-71, 2022.
[17] Chennam, K. K., Aluvalu, R., & Uma Maheswari, V.,"Data encryption on cloud database using quantum computing for key distribution. In *Machine Learning and Information Processing": Proceedings of ICMLIP 2020* (pp. 309-317). Springer Singapore, 2021.
[18] Fadhil, A. M., Jalo, H. N., & Mohammad, O. F.," *Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation*". International journal of electrical and computer engineering systems, 14(1), 73-81, 2023.
[19] Fadhil, A. M.," *Bit inverting map method for improved steganography scheme*". Diss. Universiti Teknologi Malaysia, 2016.
[20] Suraj, M. V., Singh, N. K., & Tomar, D. S., " Big data Analytics of cyber attacks*"*: a review. *IEEE international conference on system, computation, automation and networking (ICSCA)* (pp. 1-7), 2018.

[21] Liu, L., Gao, M., Zhang, Y., & Wang, Y., " *Application of machine learning in intelligent encryption for digital information of real-time image text under big data*". EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[22] Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., ... & Imran, M., " *Deep learning and big data technologies for IoT security*". Computer Communications, 151, 495-517, 2020.

[23] Mohanraj, T., & Santhosh, R., " *Hybrid encryption algorithm for big data security in the Hadoop distributed file system*". Computer Assisted Methods in Engineering and Science, 29(1–2), 33-48, 2022.

[24] Koppaka, A. K., & Lakshmi, V. N.," *An Efficient and Secured Big Data Storage in a Cloud-based Environment Using Hybrid Cryptography Algorithm and Rivest, Shamir, Adleman Algorithm*". International Journal of Intelligent Engineering & Systems, 17(1), 2024.

[25] Sharma, K., Agrawal, A., Pandey, D., Khan, R. A., & Dinkar, S. K.," *RSA based encryption approach for preserving confidentiality of big data*". Journal of King Saud University-Computer and Information Sciences, 34(5), 2088-2097, 2022.

[26] Kapil, G., Agrawal, A., Attaallah, A., Algarni, A., Kumar, R., & Khan, R. A., "*Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective*". *PeerJ Computer Science*, *6*, e259, 2020

[27] Siyal, R., & Long, J., " *Secure Cloud Data with Attribute-based Honey Encryption*",2024.

[28] Huang, P., Liao, G., & Ren, J.," *The Application of AES-SM2 Hybrid Encryption Algorithm in Big Data Security and Privacy Protection*". International Journal of Advanced Computer Science & Applications, 15(6), 2024.

[29] Deshmukh, P. N., & Deshmukh, V. H., "*Big Data Storage and Privacy in Cloud Environment by using Triple Data Encryption Standard*". Grenze International Journal of Engineering & Technology (GIJET), 10, 2024.

[30] Ma, Y., "*Research and application of Big data encryption technology based on quantum lightweight image encryption*". Results in Physics, 54, 107057, 2023.

[31] Rashmi, P., Supriya, M. C., & Hua, Q., [Retracted] "*Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare*". Security and Communication Networks, 2022(1), 9363377, 2022.