Empirical Research Press Ltd.
London, United Kingdom

International Journal of Engineering and Applied Computer Science

Volume: 04, Issue: 02, March 2022 ISBN: 9780995707542

A Secured Text Encryption with Near Field Communication (NFC) using Huffman Compression

Adeniji Oluwashola David[1], Akinola Olaniyan Eliais[2]

[1, 2] Department of Computer Science, University of Ibadan, Nigeria

10.24032/IJEACS/0402/002

Volume: 04, Issue: 02, ISBN: 9780995707542, March 2022

A Secured Text Encryption with Near Field Communication (NFC) using Huffman Compression

***Abstract*—There are a lot of Challenges raised over the security of information written to the Mifare classic 1k a Radio Frequency Identification card due to the vulnerability status of this card. The card's information can be traced to another card or an electronic device. These issues allow for unauthorized access to the data on the Mifare classic 1k-enabled device data which are transmitted between the device and reader. The information produced by a Mifare classic 1k enabled credential system for a stated status is also a concern. The focus of the study is to develop an algorithm to secure information written to the Near Field Communication tag. The performance of the system shows that when n=50, with elapse time of 1.2ms the unique character was 64, likewise at optimal when n=200, the elapse time was 1ms with the unique character of 62. This result shows a decline of the symbol-by-symbol restriction with elapses time which can secure the information of the unique character.**

Keywords- RFID, Compression, Encryption, Huffman, Security.

I. INTRODUCTION

Radio Frequency Identification systems operate in three modes which are low frequency (LF), high frequency (HF), and ultra-high frequency (UHF) bands. The frequencies band are opposite to each other due to the advantages and disadvantages related to the frequency band. The operation of a low frequency creates a laggard read rate with an enlarged capacity for reading neighboring, metallic, or liquid regions. The procedure of implementation of a higher frequency will result in quicker data transfer rates with longer ranges. The LF band frequency is between 30kHz-300 kHz with lengthy wavelengths of around 2,400 meters. LF RFID systems are simply allowed to use the small range between 125kHz –134 kHz. The High-Frequency scheme operates within the 3 MHz to 30 MHz limit and renders reading distances of 10 cm - 1 m.

Higher frequency, equal to low frequency, utilizes magnetic coupling to intercommunicate between the tags and RFID reader/antenna. HF motion can pass directly in most materials excluding water and compact metals. Compressed metals, like aluminum, can still be labeled with HF tags and perform normally. HF labels trust magnetic connection for power source, so they endeavor to improve the lifespan of the application unless damaged by wear and tear of the tag end. Within the higher frequency set of the RF range, near-field connection, or NFC, is a communication code of behavior licensed by the International Organization of Standardization. The ultra-higher frequency (UHF) set inside the RF range ranges from 300 MHz to 3 GHz; however, most UHF RFID systems operate between the 860 – 960 MHz bands.

The essential exceptions are RFID arrangements that operate at 433 MHz and 2.45 GHz. In real-world applications, the type of RFID to be used depends on the use case, cost, maintainability, regulations, environmental factor, and other requirements. This has made the world of RFID-based identification systems a little bit complicated. A typical RFID system consists of tags, a reader, an information system, and materials. The information system consists of data storage, infrastructure, software applications, and middleware. RFID system usually requires a form of middleware application that handles the translation of the RFID data to an intelligible form that the information system can understand. This is important because, rarely is an information system built from scratch based on RFID, usually; RFID is introduced to augment the current identification system which usually has been built already. The ease of integration to an existing system usually makes an RFID system a go-to for RFID-based identification systems. This also means that a new system can be built without incorporating the essence of RFID into the core of the system.

II. LITERATURE REVIEW

The application of RFID in human tracking and identification has many branches, as seen in the work of [1] who proposed the use of RFID based system in the identification of patients and staff. The review in [2] also works on RFID based attendance capturing system. A work by [3] implemented RFID Based Security and Access Control System which works with other information systems. Some research has shown that an RFID system does not always require a full-fledged infrastructure. The study in [4] built an RFID system based on the Arduino microcontroller, which does not require putting network infrastructure or a central database in place. Some privacy developers see RFID's distribution and un-restricted deployment as a kind of crack of doom scenario in which corporate and government involution can pervasively monitor individuals, paving the way for a techno-totalitarian state. Also, each person's movements, associates, and casual acquaintances are cautiously monitored and recorded in futuristic data centers [5]. The security Method will defend it from any sign of vulnerabilities associated with the network such as distributed denial of service (DDoS) attacks [6]. Some systems may even lack a full network-based information system together employing a microcontroller to serve as the logic or decision unit of the information system. The research in [7] on design guidelines and best practices, divides the RFID system into three subsystems; RF Subsystem, Enterprise Subsystem, and inter-enterprise subsystem. The performance analysis of the Huffman code was discussed in [8]. Symmetric Key Block Cipher Algorithms was developed thereby describing the analysis of the cipher algorithm. The significant roles of encryption algorithms are numerous and essential in information security by [9] in Comparative Study of

Symmetric Cryptography Mechanism. Therefore, this strategy attempts to detect only known attacks based on predefined attack characteristics in [10]. It is of very low standard and quality, has little or no integrity, very easy to forge in [11]. The tradeoff between the two protocols can provide a significant impact on the networks.in [12]. AdaBoost Algorithm selects the best set of Haar features and implements it in cascade to decrease the detection time [13].

III. METHODOLOGY

There are three procedures during the implementation with independent solutions which can be extracted and implemented in different devices. The language of implementation was C# which simulates the first stage in the developed model. The first stage is the development of the Information System. The Information System handles HTTP requests, handles database communication, authorization and authentication. The module consists of the Core, infrastructure, and WebAPIs.The core configures the entities and the business rules by ensuring that, the data is securely accessed. Accessing the database, calling an external endpoint, and sending emails were handled by the infrastructure layer whileWebAPIs interface provided the secured information access to the Core through HTTP requests. The card Interactor layer is the second stage which deals with the hardware, it implements and exposes the API to communicate with the card through the interfaces using dependency injection.

The third stage is the Middleware which consists of Logic Base. This handles the Middleware logic, implements the basic checks, and has its logic without having to contact the information system. Southbound. deals with the hardware interface directly through the Card Interactor. Every read and writes operation is handled here while the Northbound deals with communications with the information system. Figure1 below shows the solution map of the developed model.

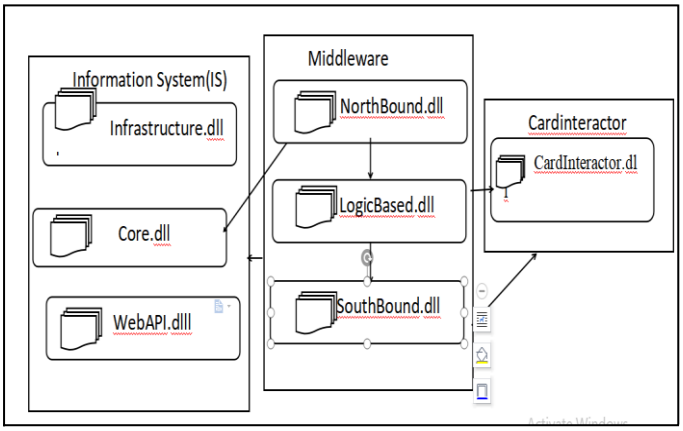

Figure 1. Model Solution Map 1

The Huffman coded information during the simulation using hexadecimal was encrypted before being written to the card. The symmetric encryption key of 6 character long alphanumeric character-set was coded using equation 1 below.

$$C = \{a-z\} \cup \{A-Z\} \cup \{0-9\} \quad \text{.....(1)} \quad \text{And} \quad K \subseteq C \quad \text{Where}$$

K is the Key and C is the characterset

The key was calculated with the entropy of the password. Password entropy predicts how difficult a given password would be to crack through brute force or guessing. Figure 2 shows the developed simulation model on visual studio IDE.

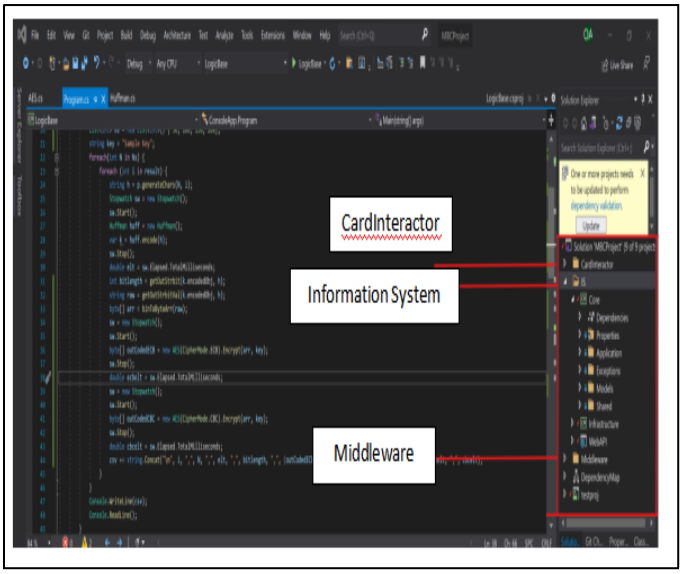

Figure 2. Simulation in Visual Studio IDE

The simulation was tested to detect Mifare standard 1k with active protocol as shown in Figure 3 below.

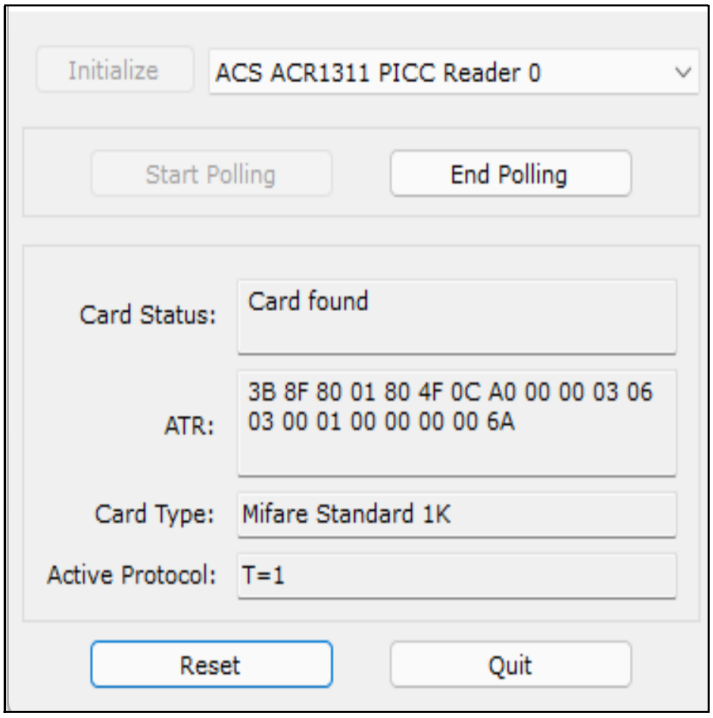

Figure 3. Interface Showing Card interactor window (card detected)

IV. RESULT AND DISCUSSION

The results from the model consist Huffman Time function which was used to identify if symbols are not independent and identically distributed because Huffman is based on the desired approach to get the optimal compression, so the study uses the shared complexity of symbol-by-symbol coding. For a given message of byte N, where n is the total number of unique characters, there is less compression achieved as n increases. The maximum compression ratio is achieved when n = 1 for the same value of N. There is a clear correlation between the number of unique characters n and how deep the tree is, which in turn affects time performance during the simulation as shown in Figure 4.1, 4.2, 4.3 and 4.4 below.

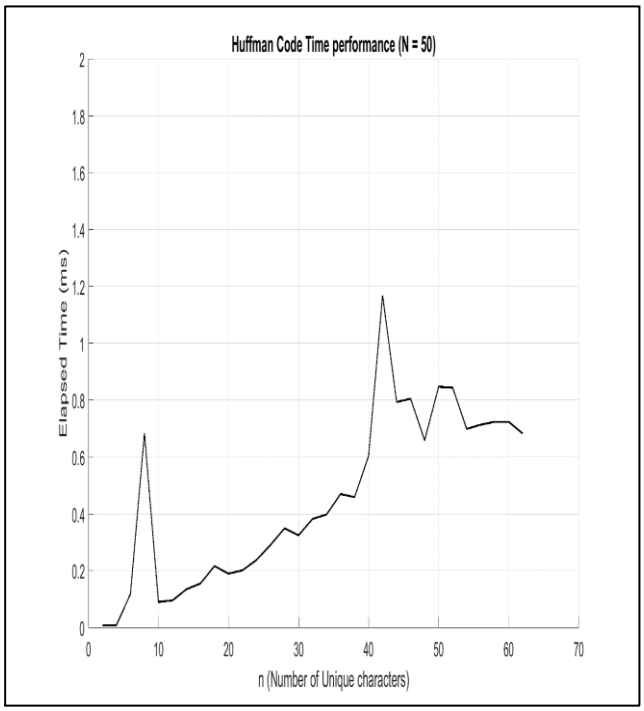

Figure 4.1. Graph of Time performance when N=50

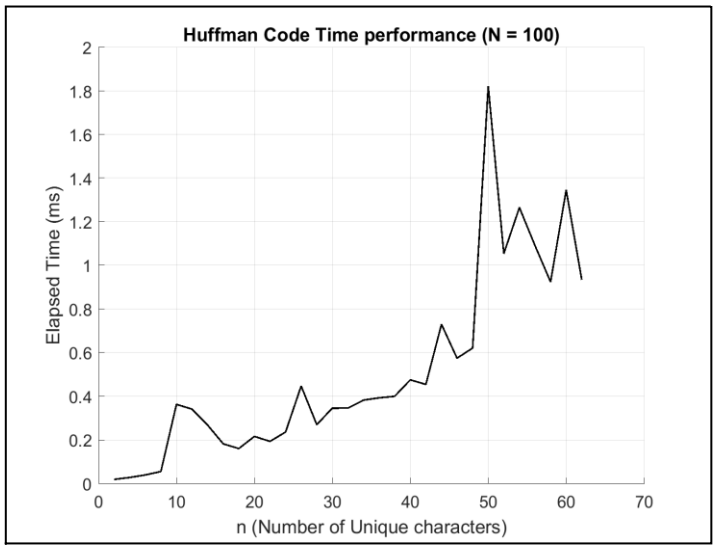

Figure 4.2. Graph of Time performance when N=100

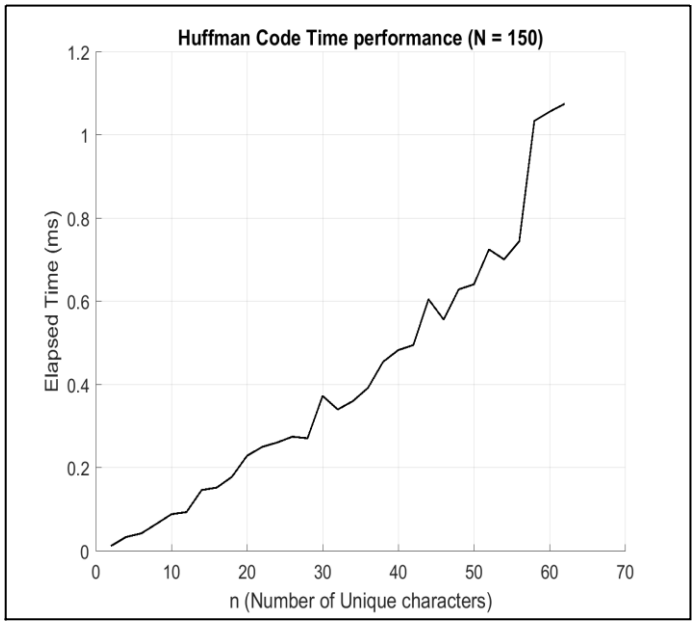

Figure 4.3. Graph of Time performance when N=150

The results of Huffman code time performance during the simulation when n=50, n=100, n=150, and n= 200 are depitched to confirm that the result of the graph presents the elapsed time against the number of unique characters. These results present the desired approach to get the optimal compression when n=50 with elapse time of 1.2ms when the unique character was 64 in Figure 4.1.

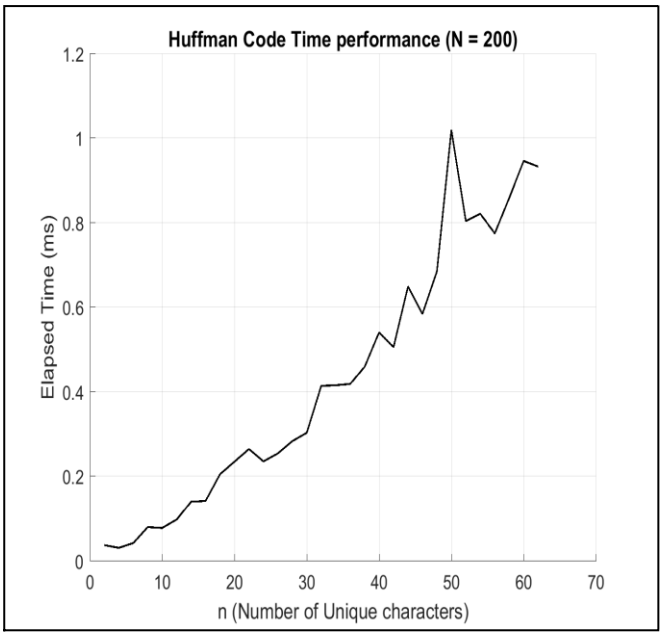

Figure 4.4. Graph of Time performance when N=200

In a related result when n=100 the elapse time for the Huffman performance was 1.8ms with the unique character of 64 as shown in Figure 4.2. Also, when n=150 the elapse time from the graph was 1.03ms with 64 unique characters, and when n=200 the elapse time was 1ms with the unique character

of 62 as shown in the graph of Figure 4.3 and Figure 4.4 respectively.

The evaluation of the Huffman time performance during the simulation is presented in the graph in Figure 4.5 below.

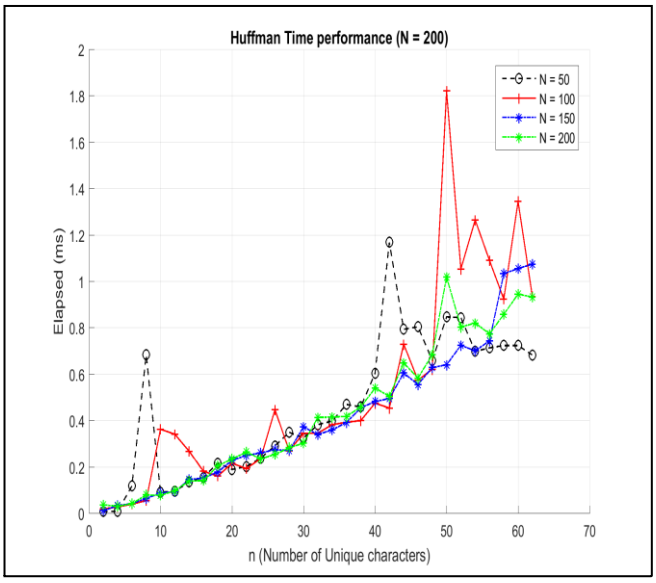

Figure 4.5. Graph of Time performance and compression

This result shows a decline in the symbol-by-symbol restriction which can secure the information of the unique character. The clear correlation between the number of unique characters is a reflection of how deep the tree is, which in turn affects time performance during the simulation.

V. CONCLUSION

The information system and the RFID system will be linked together by the means of integration. This essentially ensures that both systems can be built and extended independently without having to redesign the other part of the system. A file database is chosen for this research, this ensures that reliance on the network is obviated reducing the overhead cost of the server and network latency. The developed model in the research due to declination of the symbol-by-symbol restriction will ensure that a brute-force attempt outside this model when guaranteed by a hacker will fail because the system will revert to anti-brute-force to mitigate against guessing the 6-character long key.

ACKNOWLEDGEMENT

The research was conducted at the Department of Computer Science, University of Ibadan, Nigeria. The authors thank the department for their support in this research work.

REFERENCES

[1] Cerlinca, T. I., Turcu, C., Turcu, C., & Cerlinca, M. RFID-based Information System for Patients and Medical Staff Identification and Tracking. InTech.2010

[2] Rjeib, H. D., Salih Ali, N., Al Farawn, A., Al-Sadawi, B., & Alsharqi, H. Attendance and Information System using RFID and Web-Based Application for Academic Sector. IJACSA) International Journal of Advanced Computer Science and Applications, 2018. 9(1).

[3] Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, & Muhammad Usman Asad. “RFID Based Security and Access Control System”. 2014. IACSIT International Journal of Engineering and Technology, 6.

[4] Adak, D., Kumar Pain, M., & Dey, U. K. . RFID BASED SECURITY SYSTEM USING ARDUINO MODULE. International Journal of Scientific & Engineering Research, 2017,8(3).

[5] Ashimi, O. Q., Adeniji, O. D. “Detection and Mitigation of Flood Attacks in IPv6 Enabled Software Defined Networks. *Advances in Research Journal*, 2020, Vol. 21. No. 8. 1-9.

[6] Williams, G. Radio frequency identification. In *Technology for Facility Managers: The Impact of Cutting-Edge Technology on Facility Management* pp. 2018, 75–83.

[7] Konstantinides, J. M., & Andreadis, I. Performance analysis for canonical Huffman coding with fixed window size. Electronics Letters, 2016, 52(7), 525–527.

[8] Mankotia, S., & Sood, M. A Critical Analysis of Some Symmetric Key Block Cipher Algorithms. International Journal of Computer Science and Information Technologies, 2015, .6(1), 495–499.

[9] Logunleko K.B., Adeniji. O.D., Logunleko A.M.” A Comparative Study of Symmetric Cryptography Mechanism on DES, AES, and EB64 for Information Security”. International Journal of Scientific Research in Computer Science and Engineering.2020, Vol.8, Issue.1, .45-51.

[10] Adeniji O.d., Olatunji O.O. “Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security”.International Journal of Computer Science and Information Security (IJCSIS), 2020, Vol. 18, No. 3,111-118.

[11] Eze Chika Victor, Adeniji Oluwashola David,.Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure To Curb Forgery Menace. International Journal of Scientific &Technology, 2014, Vol 3 No 10: 66-70.

[12] Adeniji O. D, Osofisan Adenike Route Optimization in MIPv6 Experimental Testbed for Network Mobility: Tradeoff Analysis and Evaluation. International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 5, pp 2020, 19-28.

[13] Ayorinde Henry Omopintemi, Promise Irebami Ayansola Kehinde Gbemisola Ogundijo Device Synchronization Using a Computerize Face Detection and Recognition System for Cyber security. International Journal of Computer (IJC),2022.ISSN 2307-4523.