NTU Journal of Engineering and Technology (2024) 3 (4) : 1-6
DOI: https://doi.org/10.56286/ntujet.v3i4.919

IRAQI Academic Scientific Journals

P-ISSN: 2788-9971 E-ISSN: 2788-998X
NTU Journal of Engineering and Technology
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JET/index

Empowering Paperless Workflows: Networked UDC-Based EDMS for Enhanced Efficiency and Data Security

Salar Jamal Rashid[1]
1. Electronic Technologies Department, Northern Technical University, Iraq

Article Informations

Received: 11-03- 2024,
Revised: 12-10-2024,
Accepted: 11-11-2024,
Published online: 20-12-2024

Corresponding author:
Name: Salar Jamal Rashid
Affiliation : Northern Technical University
Email: salar.jamal@ntu.edu.iq

Key Words:
UDC,
EDMS,
QR,
Cloud,
Encryption.

A B S T R A C T

The Internet enables global virtual communication. Ubiquitous Device Connectivity (UDC) aims to facilitate communication between any physical devices regardless of their location or networking technology. In this paper, smart electronic documentation and authentication are implemented. Transitioning to Electronic Document Management System (EDMS) Implementing UDC will bring advantages to a business by reducing working hours and storage space, thus enhancing the efficiency of the business enterprise plant's operation. A UDC service consists of a camera as an acquisition device, QR codes, encryption, and cloud are used in the system. It will also facilitate paperless documentation for Quality Assurance (QA), Human Resources (HR), and other departments. The implemented system efficiently collected and requested data, allocating it to only authorized persons, and quickly submitted a file for examination and verification. It prevents data duplication and loss, organizes information through historical tracking, and utilizes digital filtering.

Introduction

Ubiquitous device connectivity (UDC) is the upcoming advancement that offers a wide range of services in various sectors such as education, healthcare, smart grids, automotive engineering, manufacturing, security, and consumer electronics. Most of these systems currently have an online presence but primarily utilize protocols that are not reliant on the web [1].

The UDC concept became famous in 1999 due to MIT's Auto-ID Center [2]. Kevin Ashton, a co-founder of the Auto-ID center, viewed Radio-frequency identification (RFID) as essential for the universal data center, enabling things in daily life to be tagged with identifiers for computerized management and inventory purposes [3, 4, 5]. In addition to RFID, items can be tagged using Quick Response (QR) codes, barcodes, or Near Field Communication (NFC) technology [6, 7, 8].

UDC could examine contextual data from vast amounts of information. Previously, there were limitations in storage capacity and speed of information retrieval, so cloud-based servers offer immediate storage, abundant capacity, and strong computational capabilities by integrating storage methods with automated systems [9, 10].

The management must exert significant effort to secure those files. It is vulnerable to destruction from fire, insects, floods, and earthquakes, and keeping track of record monitoring can be time-consuming. Therefore, the precision of file searching is in danger. Verification of previous order details is required in certain instances. Ultimately, this system will require time to finish. Implementing UDC in an Electronic Document Management System (EDMS) will bring benefits by streamlining business processes, reducing working hours and storage space, and enhancing the effectiveness of the company's operations [11].

On the other hand, the data in these systems must be secured from unauthorized access using encryption methods. The length of the encryption key used typically indicates the encryption's level of security. Encryption key length follows a "larger is superior" approach: longer keys result in more robust encryption. Encryption methods can be discussed in two ways: through the application and the algorithm. When using the application, the variations usually concern the sharing of encryption and decryption keys among individuals encrypting and decrypting messages. The variations are determined by the encryption method used to obfuscate the encrypted message or data in terms of algorithms. Both are interdependent; however, both factors must be considered when analyzing encryption complexity in terms of bits [12].

Recent studies have explored the integration of advanced encryption techniques in EDMS. For instance, [13] investigated the application of homomorphic encryption in securing sensitive patient data within a healthcare EDMS. Similarly, [14] proposed a blockchain-based approach to enhance data integrity and auditability in EDMS. While this paper focuses on Feistel and XOR algorithms for their simplicity and ease of implementation, future research could delve into more modern encryption techniques like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) to compare their performance in terms of speed, accuracy, and reliability

System Design

As shown in figure 1, the proposed system can be broken down into a single documentation unit and a large number of authentication units individually. Decoding the QR Code is required in every unit, either for the purpose of uploading the document to the cloud or for the purpose of accessing it for verification based on machine-to-machine interaction (M2M). There are four components that can make up the system.

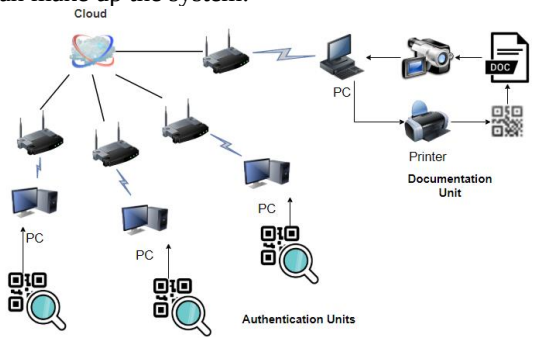

Figure 1. Documentaion and Authenticaion Systems

A. QR codes

The widely used 2D optical standard is the QR code. The popularity of the QR code standard is closely linked to the widespread availability of its reader, which is a feature of the high-resolution camera present in all contemporary smartphones. An image-processing approach is used to extract and decode a QR code from a scene, resulting in a number, text, or URI.

B. Network Connection

Once data is collected by cameras, the following step is to transmit it across the communication network. cameras are linked to a networking environment by technologies such as Bluetooth/Wi-Fi. Facilitating connections to a vast number of devices is a significant concern.

C. Encryption

Two encryption algorithms are utilized for encrypting photographs prior to uploading to a cloud service. The first encryption method used relies on the Feistel algorithm using a 64-bit cypher key, while the second approach employs XOR operation.

D. Cloud

Dropbox is a cloud storage service that allows users to store and exchange files online. It enables convenient access from any location, such as a home computer, business computer, or mobile device. The files are stored on Dropbox's servers and can be synchronized across all your devices. The used standard Dropbox service is complimentary, but you have the option to pay for an enhanced version that offers increased storage capacity and extra functionalities.

Implementation

A series of QR codes are generated and printed for each document; each code holds a name, number, and date, which provides a unique ID for the document. Then, that QR sticker is placed on a document, and the whole document will be captured by camera. After capturing the document, it will be transferred over the communication network to the connected computer through WiFi. The QR code is extracted and decoded at the computer from a scene using image-processing techniques, yielding the document's name, number, and date. The captured document will be uploaded to a specific Dropbox folder (synchronized with the cloud) and stored under the extracted QR code information. Figure 2 shows four documents stored in the Dropbox. Figure 3 shows the steps of the documentation unit.

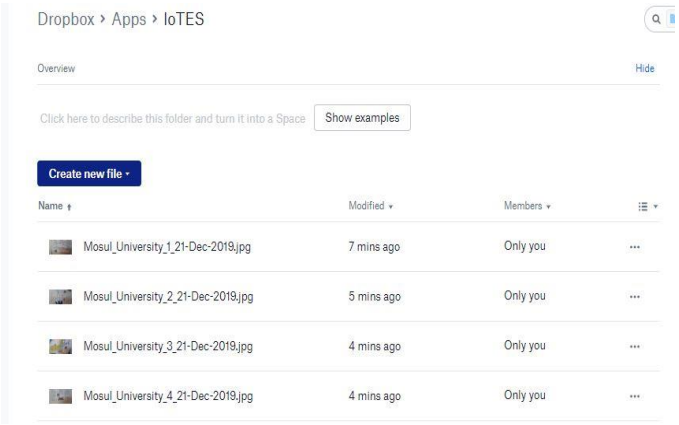

Figure 2. Stored Captured Documents in the Dropbox

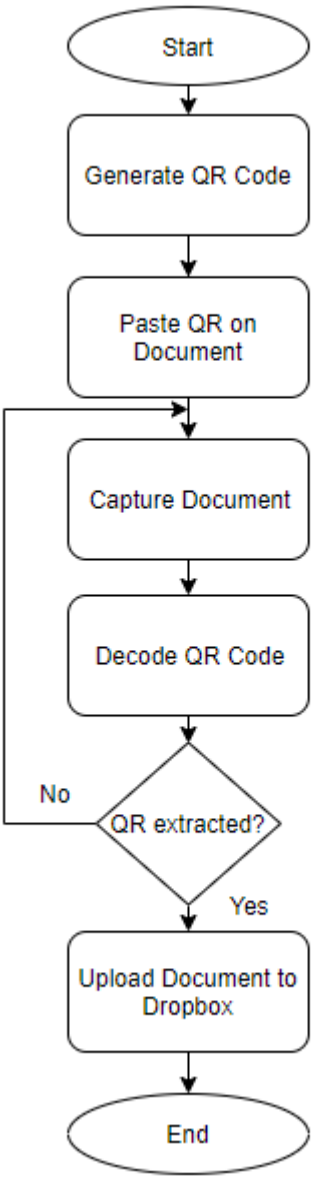

Figure 3. Documentaion Process Flowchart

On the other hand, figure 4 illustrates the authentication procedure. The authentication unit will utilize the QR code to access the cloud URL in order to verify the documents. Dropbox access tokens are utilized for the purpose of granting authorization for devices to access the cloud as part of the verification process.

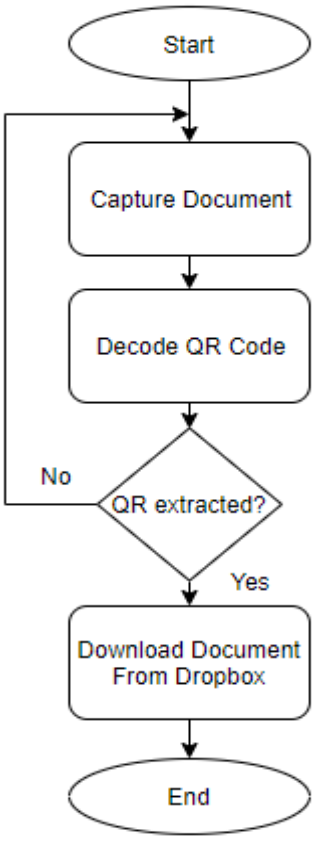

Figure 4. Verification Process Flowchart

The architecture of the cipher algorithm used to encrypt documents during documentation units provides a simple approach suitable for implementation in a software environment; two separated algorithms are used in the system: Feistel and XOR.

A. Feistel Algorithm

Figure 5 shows the flowchart of the encryption operation of the Feistel algorithm. The most essential component in the encryption and decryption operations of this algorithm is the key. The encryption/decryption operations of the algorithm consist of five round stages; therefore, it needs five unique keys to complete the ciphering operation. So, the key expansion unit is designed for this purpose.

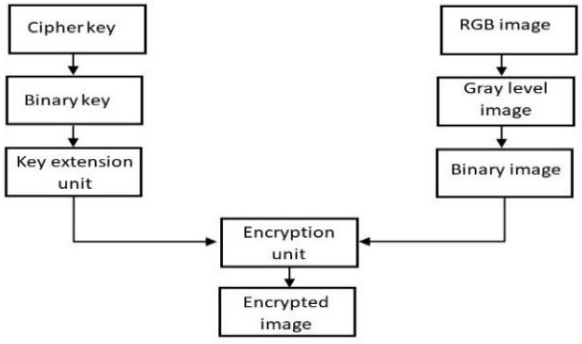

Figure 5. Data encryption process

In this algorithm, the cipher key length is a (64-bit), which means it requires a (64-bit) key to encrypt data of length (64-bit). An input cipher key of 64 bits is specified as input from the user. In the first stage, the cipher key (64-bit) is divided into (4) sets; Each one has a (16-bit) key, as shown in figure 6.

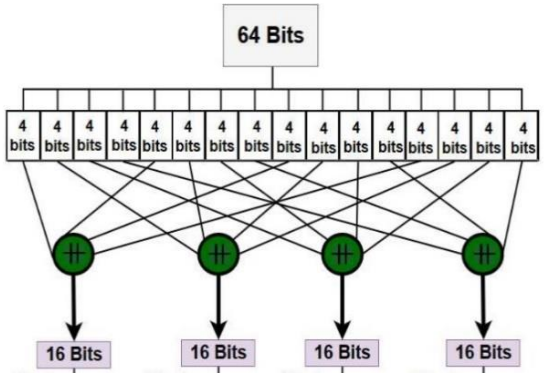

Figure 6. Dividing Cipher Key into Four Sets.

where (#) refers to the concatenation operation. The cipher key is used as an input to the key expansion unit. This unit generates five unique (16-bit) round keys; four of them are generated using internal linear combinations and a lookup table, and the fifth key is obtained by performing an XOR operation among the four round keys, as shown in Figure 7. These keys are used in the encryption/decryption operations.

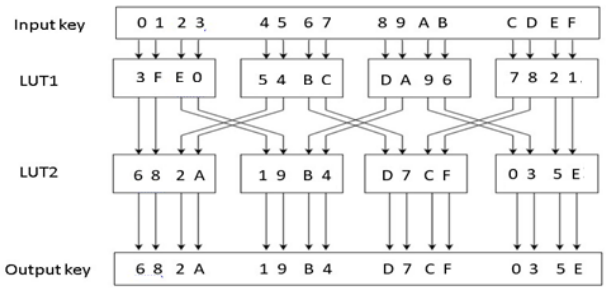

Figure 7. LUT and Linear Combination for Generating Round Key

The encryption process includes some basic logical operations, decomposition of data, and exchanging. At first, the input data of (64-bit) is divided into four sets of (16-bit) lengths each. The entire data is passed through five stages of the same logical operations (XOR, XNOR, shift operation, and exchanging), and each stage has its private round key, as shown in Figure 8. Finally, these sets are concatenated together to get the encrypted data.

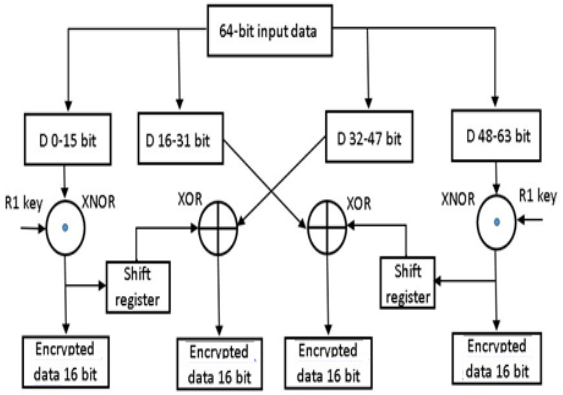

Figure 8. Data Encryption Process.

B. XOR Algorithm

XOR encryption is a method that involves performing XOR operations between an input image and an encryption key to produce an encrypted image. The encryption key is derived by algorithms that produce consistent random values for each iteration. XOR encryption is significantly more secure when the key is random and at least as long as the data, compared to when there is key repetition inside the data. A stream cypher is produced when a pseudo-random number generator creates the key stream. Using a genuinely random key enhances security, making it theoretically unbreakable.

Decryption is achieved by applying the XOR operation between the original random key used during encryption and the encrypted image, resulting in the decrypted image, as illustrated in figure 9.

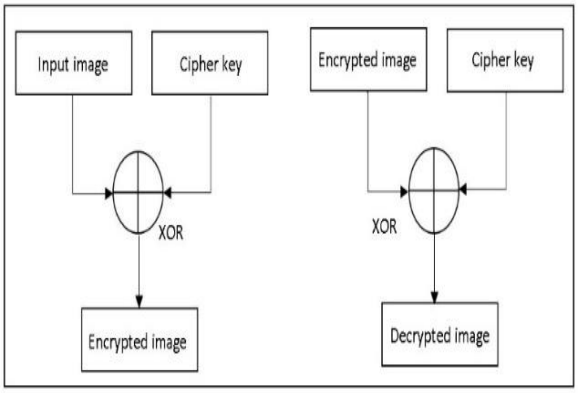

Figure 9. Block Diagram of XOR Encryption/Decryption

Results

The two encryption algorithms are simulated using MATLAB software, figure 10 and figure 11 illustrate the results that are obtained by performing (64-bit) cipher algorithm and XOR encryption respectively.

Figure 10. Encryption Results using (64-bit) Cipher Algorithm.

Figure 11. Encryption Results using XOR Encryption Algorithm

It can be seen that encrypting image using the Feistel algorithm reducing the image size in contrast with implementing XOR operation in which doesn't change the image size. Thus, Feistel algorithm will require less cloud storage area, but it comes at the cost of higher detectability due to the fixed nature of the Feistel algorithm compared to the randomness inherent in XOR key generation.

Further analysis of the results reveals that the Feistel algorithm, while effective in reducing image size, exhibits a deterministic encryption pattern. This predictable nature potentially increases its susceptibility to cryptanalysis compared to the XOR operation, which utilizes random key generation. The impact of both encryption algorithms on system performance was evaluated based on processing time and resource consumption. The XOR operation demonstrated a slight advantage in processing speed due to its simpler logical operations. However, the Feistel algorithm's superior compression capabilities contributed to reduced storage requirements and potentially faster data transmission speeds.

Conclusion

In this paper, a cloud-enabled electronic documentation and authentication system was presented. The system involves the document being scanned with a QR code at the documentation unit and then stored as an image in the Dropbox cloud. The name number and date that are extracted from

the QR code are used as a unique ID for distinguishing between documents. After that, the paper document that has arrived is scanned at the authentication unit, and a comparison is made between it and the copy that is saved in Dropbox for verification purposes. The system that is being presented offers efficient and secured real-time interaction with data, centralized data that is simple to access, and a reasonable price. Additionally, it prevents the waste of human resources and infrastructure devices when operating.

References

[1] R. Want, B. N. Schilit, and S. Jenson, “Enabling the Internet of Things,” Computer, no. 1, pp. 28–35, 2015

[2] Jansen, Maike, et al. "Stop guessing in the dark: Identified requirements for digital product passport systems." Systems Vol. 11, No. 3, 2023.

[3] Cornea, Andreea-Alina. "Technical Analysis of RFID and IoT Technologies Integration in Product Recall Digitalization Process." Proceedings of the International Conference on Business Excellence. Vol. 17. No. 1. 2023.

[4] Wood, Alex. "The internet of things is revolutionizing our lives, but standards are a must." The guardian 31, 2015

[5] "From M2M to The Internet of Things: Viewpoints from Europe". Techvibes. 7 July 2011.

[6] Sristava, Lara. "The Internet of Things – Back to the Future". European Commission Internet of Things Conference in Budapest, 2011.

[7] Wigmore, Ivy. "Internet of things (iot)." TechTarget, June 2014.

[8] Cornea, A. A. "Technical Analysis of RFID and IoT Technologies Integration in Product Recall Digitalization Process". Proceedings of the International Conference on Business Excellence, 17(1), 2023.

[9] Jansen, M., et al. "Stop guessing in the dark: Identified requirements for digital product passport systems". Systems, 11(3) ,2023.

[10] Gupta R., Gupta R. "ABC of internet of things: advancements, benefits, challenges, enablers, and facilities of IoT", Proceedings of Symposium on Colossal Data Analysis and Networking (CDAN) Indore, India, 2016.

[11] Mendoza, Analyn R; Alvarez, Cristina; Castillo, Henriette Mae; Manongsong, Maricel; Andromeda Santiago, "Electronic document management system implementing internet of things (IoT)", International Journal of Advanced Research in Computer Science; Udaipur Vol. 10, No. 2, pp. 10-15, 2019.

[12] Yamini Jain, Ritesh Bansal, Gaurav Sharma, Bhuvnesh Kumar and Shailender Gupta, " Image Encryption Schemes: A Complete Survey ", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.7, pp.157-192, 2016.

[13] Mendoza, A. R., et al. "Electronic document management system implementing internet of things (IoT)". International Journal of Advanced Research in Computer Science, 10(2), 10-15, 2019.

[14] Jain, Y., et al. "Image Encryption Schemes: A Complete Survey". International Journal of Signal Processing, Image Processing and Pattern Recognition, 9(7), 157-192, 2016.