Research Article

A Multi-layer Security Scheme (MLSS) for Digital Images Contents

Faraj Ali Faraj Alyaqobi [a] and Nor Adnan Yahaya [b]

[a] PhD Candidate, Department of Information Technology, Malaysia University of Science and Technology, Kuala Lumpur, Malaysia

.

[b] Professor of Information Technology, Department of Information Technology, Malaysia University of Science and Technology, Kuala Lumpur, Malaysia

Abstract: Digital images and their contents are increasingly being utilized in numerous applications, especially in the context of the Internet of Things (IoT). The rapid growth of IoT has facilitated the sharing and transmission of vast amounts of data in today's modern world. Consequently, various applications relying on images are now generating a substantial volume of data that requires extensive processing, including the manipulation of images and associated digital elements. Protecting sensitive information within these digital images is of utmost importance, particularly for applications that store critical data. The exposure of such data to the public would pose significant risks to numerous applications and systems. However, despite the advantages offered by IoT, devices and resources connected to this network still face substantial security challenges. In this research, we propose a multi-layer security scheme (MLSS) that employs a diverse range of security procedures applicable to various forms of information, including images. The MLSS consists of three key processes, aimed at preserving information integrity, confidentiality, and accessibility. An evaluation of this scheme has demonstrated its effectiveness, safety, and with a very low range of data loss.

Keywords: Confidentiality, Digital Images, Information Security, Integrity, Digital Contents Security

1. Introduction

Nowadays, it has become prevalent that digital systems are governed by granting connected users the ability to remotely engage with each other, thereby enabling interaction for both parties involved (Ain, Vaia, DeLone, & Waheed, 2019; Nourani, Kabir, Mohseni, & Ragan, 2019; Tavakoli, Carriere, & Torabi, 2020). As a direct consequence of this, protecting the security of the linked content will be of the utmost importance (Sollins, 2019), where it is essential to ensure reliable availability of some information through verification (Hang & Kim, 2020; Hofer-Schmitz & Stojanović, 2020), authentication (Khalid et al., 2020), and secrecy security methods (Nashwan, 2021; Nizzi, Pecorella, Esposito, Pierucci, & Fantacci, 2019).

An emerging scenario that requires protection of data is due to increasing communications between equipment in smart homes and their service providers (Isaak & Hanna, 2018; Wachter & Mittelstadt, 2019). When this phenomenon becomes more prevalent, a private communication channel between these various persons and organizations will have been set up so that they may only communicate with one another and share information in a risk-free and protected manner (Atlam & Wills, 2020; Golec, Gill, Bahsoon, & Rana, 2020; Puthal et al., 2022).

There are a number of earlier studies that have been conducted on this subject that are found in the literature. One proposed security system has provided a key setup method that takes advantage of a mechanism found in the application layer. To accomplish this goal, a security process that is applied to intelligent applications and data systems has been carried out, and subsequent information is then collected. The methodology presented in (Shin et al., 2019) aims to achieve the development of a secure and confidential security architecture, as discussed in reference (Yao et al., 2021). In order to verify and validate the information and obtain a high level of security, it advised employing two distinct layers of authentication (Dhar, Khare, & Singh, 2022; Li, Zuo, Song, & Lv, 2021; Pavlović et al., 2022).

There are a variety of research that have been done on multi-layer security systems that can be incorporated into data application systems. Generally, the goal of the solution is to provide protection for all layers of the system where data are processed. This multi-layer protection is required to prevent any data from being exposed in any way (D. N. Gupta & Kumar, 2021; Khan et al., 2022), prevent any possible danger (Alterazi et al., 2022; Shurman, Khrais, & Yateem, 2019), and shut any vulnerabilities associated to data systems (He, Yu, Li, Chan, & Guizani, 2022; Raghuvanshi, Singh, & Joshi, 2022). One of the techniques for protection is to provide a security layer that protects against denial-of-service attacks (Bhardwaj, Mangat, Vig, Halder, & Conti, 2021; B. Gupta, Chaudhary, Chang, & Nedjah, 2022; Tukur, Thakker, & Awan, 2019).

Another solution that has been proposed with the intention of preventing attacks from taking advantage of vulnerabilities in a data system has taken into consideration the possibility of combining two distinct security processes, specifically security testing and security event detection. This solution was presented with the intention of preventing attacks from taking advantage of vulnerabilities in a data system (Lai, Leu, & Chu, 2014; Yahyaoui, Abdellatif, Yangui, & Attia, 2021). It has implemented the security measures in a hierarchical structure with several layers (Karras, Karras, & Sioutas, 2022). This combination of several security layers has helped to lessen the danger of data security that was confronted by personal data (Haque, Bhushan, & Dhiman, 2022; Ni, Cang, Gope, & Min, 2022).

The two-layer security systems may be vulnerable to attacks in the future. For this reason, additional safety and protection measures for the data need to be considered (Hasan & Hasan, 2022). This indicates that a data system with a greater number of security layers added to it may function more effectively than other data systems with fewer security levels (Bohli, Langendörfer, & Skarmeta, 2022; Mohiyuddin et al., 2022). Hence, the purpose of this paper is to enhance the number of layers of security in order to better safeguard the data.

Several security-related processes and protocols have been put in place to improve the level of data protection offered by this paper. This paper hypothesizes that the data that is being encrypted may be subjected to more than one attempt using a variety of methods and/or mechanics to apply a disclosure procedure that, in the end, comprehends what the concealed message is or what the embedded contents are. This is based on the supposition that a disclosure procedure may be applied. As a result, the method that has been developed has included a number of security layers, which safeguard contents throughout many stages of encryption and decryption, as well as over multiple periods of time. These stages are performed by the sender and the receiver, respectively.

In this setting, the data may be protected on several fronts using a wide range of security measures. In order to verify that the authorized user or party has received the intended contents in a secret way, a number of security layers will be applied to the original data during the encryption phase, and a comparable number of verification methods will be used during the decryption phase. Using security measures during encryption is intended to ensure the integrity and reliability of the original content provided from a trusted source. If the contents are secure against tampering, it means that they can be relied upon to provide the desired results without being compromised. The suggested measures are carried out in synchrony.

This paper is organized as follows. Section 2 presents high-level view of our proposed Multi-Layer Security Scheme (MLSS). Section 3 is devoted to providing details and the main algorithmic steps applied in the proposed MLSS. In the next section (Section 4), MLSS is analysed and evaluated, and its results and findings will be discussed and explained. Section 5 presents our concluding remarks.

2. The Proposed Multi-Layer Security Scheme (MLSS)

There are several processing steps that are involved in using the proposed MLSS. First, the digital contents as an input will be initialized and pre-processed. Then, post-processing will be done on the content where the necessary information will be extracted. This step essentially serves as the beginning of the use of the MLSS. In the subsequent step, the previously processed data will be transformed into scrambled form. In addition, the content will also be changed to make the data more ambiguous and to increase the level of security. The next step is to use an encryption system on the data that has been changed and scrambled. Using a QR code technique-based encryption scheme, the encrypted data will then be safely wrapped up. Finally, the digital contents will be ready to be transferred to the other party via an IoT medium. The high-level view of MLSS is shown in Figure 1.

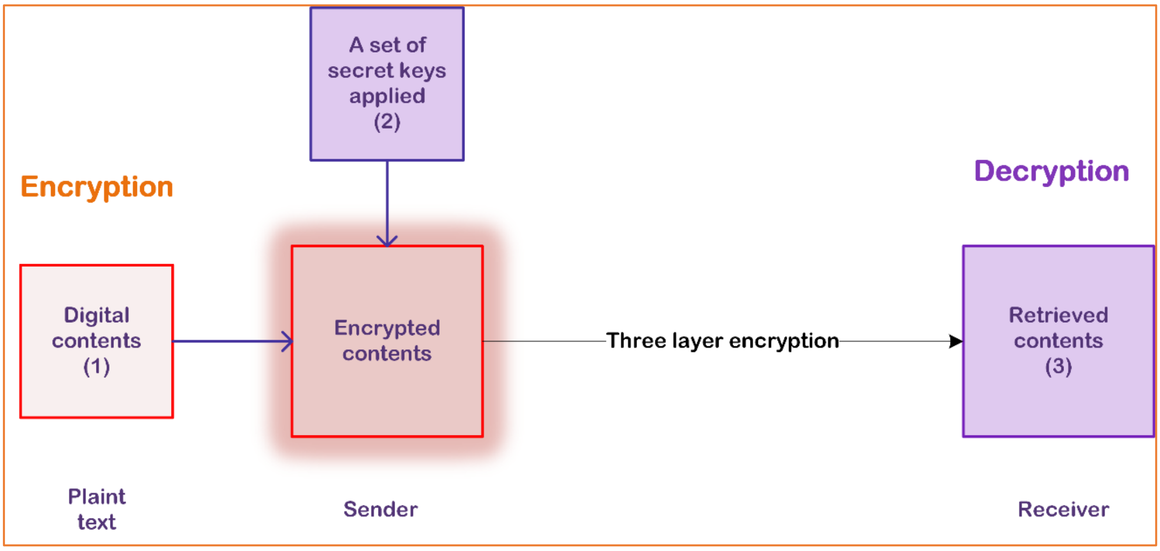

Figure 1. High-level View of Multi-Layer Security Scheme (MLSS)

This diagram shows that there are three steps, the first of which is an encryption phase. At this stage, three layers are used to protect the original data and digital contents. In the first phase, a number of different MLSSs will be used to make sure the content is safe. These MLSSs will result in the contents being at most encrypted, and data will be concealed and incomprehensible. The transmission of confidential information will take place during the second phase. Decryption of the secure data takes place during the third step of the process.

In order to increase the level of protection provided to the original data and content, the first step of the process entails the implementation of three main levels of security, each of which is made up of more than one security layer. At each layer, for instance, there will be a process of converting original data from one form to another one. This will occur at each level. The encrypted material is decrypted using three primary security levels in the third step of the process. There will be three different verification mechanisms in place so that the three different security goals of availability, integrity, and secrecy can be verified. A detailed presentation of the primary and secondary levels of security shall be provided in Section 3. Figure 2 shows the flowchart for multi-layer encryption process for the proposed MLSS.

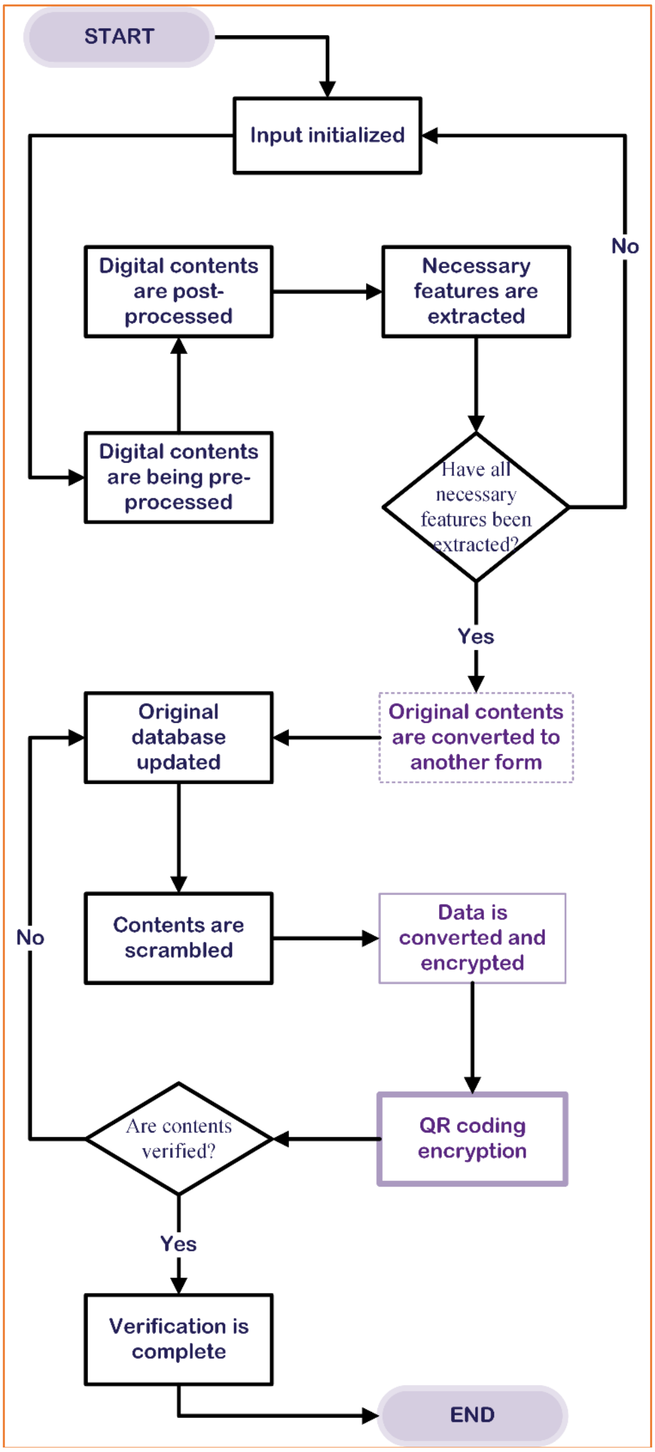
START
Input initialized
Digital contents are post-processed
Necessary features are extracted
No
Digital contents are being pre-processed
Have all necessary features been extracted?
Yes
Original database updated
Original contents are converted to another form
Contents are scrambled
Data is converted and encrypted
No
Are contents verified?
QR coding encryption
Yes
Verification is complete
END

Figure 2. Flowchart of multi-layer encryption process

The flowchart shows the main steps involved to implement the multi-layer encryption process in the proposed scheme. A brief explanation of these important components is given in the sequel.

The digital contents will be set to their default values, and a particular category of data will be chosen for further processing. The image file will then be imported as an input at this point. After that, the image will be subjected to pre-processing, during which its details will be evaluated to determine whether or not to retain a subset of significant features and whether or not to remove irrelevant details from the image. The next step is to do some kind of post-processing on the image that was created, during which the essential aspects of the image will be brought out and preserved. The next step is an image information and features extraction technique, which comes after this step. After that, the image that has been processed will be changed into a new form of digits, and then values that correspond to the original color intensities will be derived from those digits. The image will then be transformed into a two-dimensional array when this step is complete (2DA). The associated two-dimensional array (2DA) will be transformed into a one-dimensional array (1DA) with a defined length throughout the formalization process. The length of 1DA, its shape, and its values are completely different to those of 2DA. The 1DA will be encrypted using the first method that will be implemented. Following that, a different encryption method scheme will be employed in order to further enhance the level of security afforded to the original data. In the end, the data in its encrypted form will be displayed in a format that is distinct from the information it originally had, either in the form of a textual representation or an image-based representation. After data has been encrypted, it is then possible to transmit it.

2.1. Multi-layer decryption process

The decryption phase is crucial for ensuring image data security and integrity. This phase involves converting encrypted image data back to its original readable format using a decryption key. To maintain security, it is vital to keep the decryption key confidential and prevent unauthorized access. Robust encryption algorithms and secure key management practices are employed to achieve this.

Multi-factor authentication is commonly used to enhance decryption phase security. This method requires users to authenticate their identity through multiple means, such as biometric verification (e.g., fingerprint or facial recognition) and password authentication. Implementing multi-factor authentication adds an extra layer of protection to the decryption key.

Creating a secure decryption environment further strengthens security during the decryption phase. This can involve using a dedicated and secure computer or network solely for the decryption process, limiting access to authorized personnel. By isolating the decryption environment, the risk of unauthorized access to the decryption key is significantly reduced.

3. Algorithmic steps

3.1. Initialization process

3.1.1. Step 1: Input initialization

The first step is to load the first image into the working environment of the program. C++ is the programming language that has been used for the software environment. The image has to be pre-processed in order for any treatments to be carried out successfully.

3.1.2. Step 2: Contents' pre-processing

During this stage of the process, the image is changed to a different color mode in order to begin the pre-processing phase of the procedure. The goal of this phase is to preserve the image's essential characteristics while excluding its fewer essential ones. In order to carry out this procedure, you will need to make use of a certain mathematical formulation, which can be found in Equation (1):

$$f(x,y) = (0.29 \times r) + (0.58 \times g) + (0.11 \times b) \tag{1}$$

where:

- $f(...)$ yields values that indicate the intensities of the pixels involved in the production of grey color.
- x and y are used to indicate the positions of the pixel that is now being processed in the 2D image.
- r is the value of the RED color that was taken from the image with the coordinates (x,y) and assigned to the pixel that was positioned at the x^{th} row and the y^{th} column.
- g denotes the GREEN color value that was derived from the $f(x,y)$ for the pixel that is positioned at the x^{th} row and the y^{th} column.
- b stands for the BLUE color value that was taken from the image with the coordinates (x,y) and assigned to the pixel that was positioned at the x^{th} row and y^{th} column.

3.1.3. Step 3: Post-processing

3.1.3.1. Removal process

During this sub-process, a large number of the features that are situated inside the limits of the objects will be removed. This technique is used to the interior and textural elements, neither of which are very significant. That is to say, the procedure of removing such unimportant elements will not have any impact on the borders of the objects in the image. The recommended pseudo-code will be shown in Algorithm 1.

Algorithm 1: Unwanted details removal process

```
1:   START
2:   For (i=0;i<max(img_h);i++)
3:       For (j=0;j<max(img_w);j++)
4:           If(f(i,j)∈img_f_grnd)
5:               j++;
6:           Else
7:               f(i,j)=0;
8:           END if
9:       END For j
10:  END For i
```

The primary objective of Algorithm 1 is to emphasize the goal of the removal stage, which is to concentrate on the deletion of features in such a way that the image is not negatively impacted by their absence.

Every location and the value of each pixel will be considered in Algorithm 1. If the pixel has a value that belongs to the foreground region and also to the edges of objects or the borders between regions, this means that the pixel is important and that removing it will change what the image means. If the value is in the background, it means it isn't important and doesn't belong to any important parts of the image or the edges of anything. Additionally, it is not a part of any item's edges.

If the criterion is met in line 4 of Algorithm 1, it means that the details are important and shouldn't be removed. If the criteria aren't met, the elements may be moved to the background, which means they aren't important and can be taken away.

3.1.3.2. Necessary details preservation process

The method starts by moving from left to right and then from top to bottom to look at the intensity of each pixel and its position, which is represented by I and j. Algorithm 2 shows the pseudo-code.

Algorithm 2: Necessary details preservation process

```
Initialization:
    Get f(i,j);
Process:
    while ((i<=max(img_h)) AND (j<=max(img_w))) {
        If ( f(i,j) )
            If ( $N_4$(f(i,j)) != f(i,j)  AND $N_8$(f(i,j)) != f(i,j) )
                {
                    j++;
                    f(i,j)=0;
                }
            End If
        End If
        update_location(i,j);
        }
Output:
For (i=0;i<max(img_h);i++)
    For (j=0;j<max(img_w);j++)
        If (f(i,j)!=0)
            display f(i,j);
        else
            location++;
        End if
    End for j
End for i
```

The output that was received from the step before this one will serve as the input for the step that follows in this pseudocode, which is represented in Algorithm 2. Every pixel will be checked, and if it has a neighbouring pixel in any of its four neighbours with a value that does not equal to that pixel, then the eight neighbouring pixels will be checked, and if the pixel being processed does not equal to any of the eight neighbouring pixels, then the pixel being processed can then be deleted, and it will be considered to be a part of the noise that already exists in the image. If the condition described above, which is expressed by an if-statement, is found to be true, then the pixel in question will be preserved and taken into account as either belonging to the outlines of objects or being situated on the boundary of an area. It is possible to emphasize and preserve the most crucial aspects of a image by applying this method to each and every pixel in the image. The image that is produced as a result of this procedure will have the edges of the objects highlighted.

3.1.3.3. Feature's extraction

This process is comprised of four distinct sub-processes, which are as described below:

- Emphasis is placed on the most relevant particulars.
- Observation is given to the edges of the items.
- The grayscale image is then transformed into a binary one.
- The intensities of an image's pixels are represented by their corresponding digital integers.

After the preceding process has been applied to the image, the details that are left over will almost always be the important details that keep a portion of the features and information about the image and its objects and regions. Important characteristics that need to be kept for future processing include, but are not limited to, the borders of objects, the boundaries of areas, and the positions of pixels. During this step of the process, these particulars will be brought out and preserved inside the image.

The associated pseudo-code for this procedure is mentioned in Algorithm 3, and it is highlighted as well.

Algorithm 3: Binary image formation process

```
Input:
    define k ← i
    define l ← j
    call pix_int(g(i,j));
Process:
    Do {
        If ( 0<= g(i,j)<= 125 )
            $bin_{op}(k,l)=0;$
        Elseif ( 125<g(i,j)<= 255 )
            $bin_{op}(k,l)=1;$
        else
        {
            update_loc(i,j);
            pix_int(g(i,j));
        }
        End If
        } while ((k<=max(img_height)) AND (l<=max(img_width)));
Output:
    return pix_int($bin_{op}(k,l)$);
```

In this algorithm, g(i,j) will be checked for every pixel. If the values are less than or equal to '125', they will be changed to the '0' value, which corresponds to the '255' number in a binary image. If they are greater than '125', they will be changed to the '1' value, which corresponds to the '255' number in a binary image. Equation (2) gives a mathematical formula that can be used to describe this process (3):

$$bin_{op}(k,l) = \begin{cases} 0, & 0 \le f(i,j) \le 125 \\ 255, & f(i,j) > 125 \end{cases} \tag{2}$$

When this equation is used on a grayscale image, the result is a "binarized" image with only "0" and "1" values.

3.2. Layer 1: Contents scrambling procedure

3.2.1. Original data conversion

There are two used sub-steps in this step. The first step is to turn the binary image into a two-dimensional array (2DA) with the same number of rows and columns as the image. The second one will turn the 2DA into an array with only one dimension. Algorithm 4 contains the proposed pseudo-code that was mentioned earlier.

Algorithm 4: An image conversation process

```
For (a=k; a<=i_h; a++)
    For (b=l; b<=i_w; b++)
    {
    store_values_2DA($f_{2DA}(a,b)$);
    update_loc(a,b);
    }
    End For b
End For a
```

```
    return  $f_{2DA}(a,b)$;
```

At this point, the 2DA contains values that are either 0s or 1s that have been binarized. The next thing that has to be done is to use a look up table to save their positions (indices). The look up table will only hold the locations of values that are a 1 and their values. As soon as all of the locations have been saved, the database will be created. As a result, a lookup table is created in a two-dimensional format.

3.2.2. 2D array alteration

The procedure is broken down into three stages, which are the creation of a database, the transformation of a 2D array into a 1D array, and the insertion of an embedding layer. These three phases are summed up in Algorithm 5, which can be found here.

Algorithm 5: A 2D array conversion process

```
For (a=0;a<img_h;a++)
    For(b=0;b<img_w;b++)
        If ( $f_{2DA}(a,b)$ !=0 )
        {
        Tex (a) = a & ' ';
        Tex (b) = b & '  ';
        T[m] ← T[m] + Tex(a) + Tex(b);
        a = a+1;
        }
    End For b
End For a
return  T[m];
```

The success of the method is mostly dependent on those values in the image that are equal to 1 or ‘255’. After this particular criterion has been satisfied, the relevant index will hopefully be saved. Following this step, before the storing operation is finished, the relevant index of the right value will be updated in order to conceal the correct index. This step comes after the previous step and comes before the final step. After a while, the embedded layer that is being created in this stage will be able to be removed without much difficulty and identified correctly. The removal of +1 from the row’s associated index is the method that may be used to identify the addition of an embedded layer. After finding the processed location or index that is specified by the pair (a, b), there must be an embedded layer, and it may be processed in two phases, as follows:

- The integer value of a should have -1 subtracted from it, and
- Take out the extra spaces that were inserted after a and b.

The first procedure is offered in order to alter the values of the original documents and to raise the level of protection afforded to the original material. The second process is recommended to signal two key considerations: 1) to identify which position is being changed, and 2) to modify the number of rows to disguise the initial location. Both of these indications are vital for the purpose of the first point. While the values of locations are being stored in a one-dimensional array, a certain number of modifications, denoted by the variable m, may be made to the data.

3.3. Layer 2: Conversion with encryption procedure

This stage is dedicated to converting the values that are contained in the look up table into a straightforward one-dimensional array (1DA) by making use of a straightforward formalization procedure.

The following is a rundown of the stages involved in the formalization process:

- Initialize input;
- Extract original values, i.e., numbers;
- Extract original values, i.e., spaces. < >;
- Replace strings containing spaces with one special character for a single space and two special characters for a double space, correspondingly;
- Change the decimal value 1DA, which is shown by 1DAd, into the binary value 1DA, which is indicated by 1DAb.

To carry out the formalization process that is applied to the 1D array, there are two primary operations that must be performed. The first step of the process involves replacing the spaces in the 1DA with special characters that are not equivalent to any of the other values in the database. As may be seen in Figure 3, a graphical algebraic depiction of the 1DAb is given for the user's convenience.

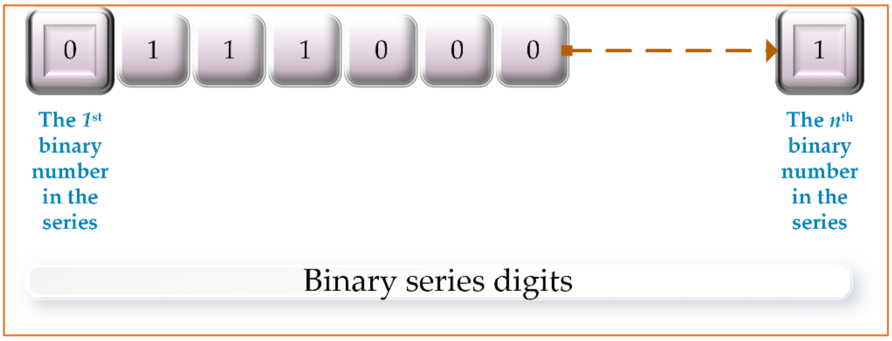
0
1
1
1
0
0
0
1
The 1st binary number in the series
The nth binary number in the series
Binary series digits

Figure 3. Illustration of 1DA as a binary-number sequence

3.4. Layer 3: QR coding encapsulation

3.4.1. Scheme

The 1DAb will be processed and encrypted utilizing a distinct architecture-based design of encryption throughout this stage. During this stage of the procedure, a logical pulse will be generated by a digital pulse generator in order to construct the secret key. In addition to the 1DAb being encoded in binary, the generation of the secret key utilizes binary generation software as well.

3.4.2. Encryption procedure

The steps of the encryption procedure component can be summarized as follows:

- Each two adjacent digits are used as an input for the logic gate XOR, as formulated in Equation (3):

$$y = a\ XOR\ b \tag{3}$$

- By referring to the Equation (3), the logical operation will have only one case either 0 or 1.
- By focusing on the third column at Table 3.1, there are two zeros and two ones. The two zeros are ordered as first and second zero. The first zero is given a 00 value, and the second zero is given a 01 pair value. Similarly, the two ones are ordered as first and second one. The first one is given a 00 pair value and the second one is given a 01 pair value. A representation procedure of output values based on y, a, and b is formularized using a mathematical procedure as described in Equation (4).

$$\text{output}(y) = \begin{cases} 00, & y = 0 \\ 01, & otherwise \end{cases} \tag{4}$$

- If a=0 and b=0, in Equation (3), the output y will equal to 0. This y=0, is representing the first zero and is given a rank of 0. The first zero (rank 0) can be represented by 00.
- The next stage is to produce the formalized output, which consists of three digits; one of these digits is the result of the logical operation known as XOR, and the other two digits result from the addition of a representation of either the first/second zero or the number one (see Table 2, the fourth column).
- After this step, the result of the encryption method may be received.

3.4.3. Encryption technique based on QR code

The data are prepared to be created in such a manner as to generate data in this section of the process. The formalization of encrypted data is going to take place. When data has to be condensed, a QR code is the tool of choice. QR codes are able to be allotted to the appropriate nodes. In order to ensure that the safety of the contents is continuously improved. In addition to this, data may be stored and transferred via the QR code. To facilitate the verification process and make use of this QR code more easily, it may be sent to the authorized nodes through an internet channel.

The output of the phase is encrypted using the Quick Response (QR) method. Its purpose is to make the decryption procedure more difficult in the event that an effort is made to reveal the contents of the file. Another thing to keep in mind is that this stage will include a change in the form of the contents, which is intended to make protected materials more secure.

Consequently, this method has the following two extra features:

- To include an additional encryption method into the already-encrypted contents of the file.

- To alter the format of the materials as they are now presented.

4. Evaluation of MLSS

In this section, we discuss a prototype development of the proposed MLSS, followed by the presentation of the results of its evaluation.

4.1. The implementation of the system

The system is currently being implemented, and subsequent discussion will concentrate on the phase of implementation in more depth. A graphical representation of the many stages and procedures involved in the process of putting the proposed Internet of Things system into operation may be seen in Figure 4.

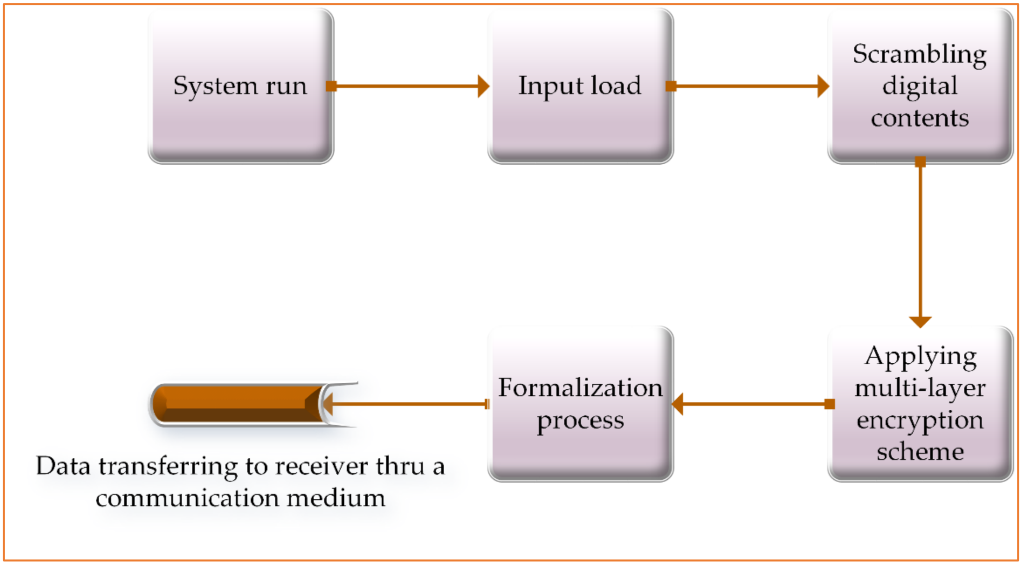
System run
Input load
Scrambling digital contents
Applying multi-layer encryption scheme
Formalization process
Data transferring to receiver thru a communication medium

Figure 4. Implementation model of the system

4.2. The evaluation of MLSS

4.2.1. MLSS's confidentiality and integrity evaluation

The evaluation of the proposed MLSS was achieved through assessing the prototype system. The objective of the system assessment was to determine whether or not the secrecy is maintained based on a variety of datasets (a group of images will be tested accordingly). Calculations were done to determine the degree of accuracy, which is expressed as a percentage.

The functionality of transmitting and receiving photos has been completely implemented. It has been determined that the checking procedure was successful. Each time the image is sent to the second party, the system gives the user the option of entering a secret key or password (i.e., receiver party). In this particular assessment test, the total number of images that have been transmitted is 29, and the total number of images that have been received is also 29.

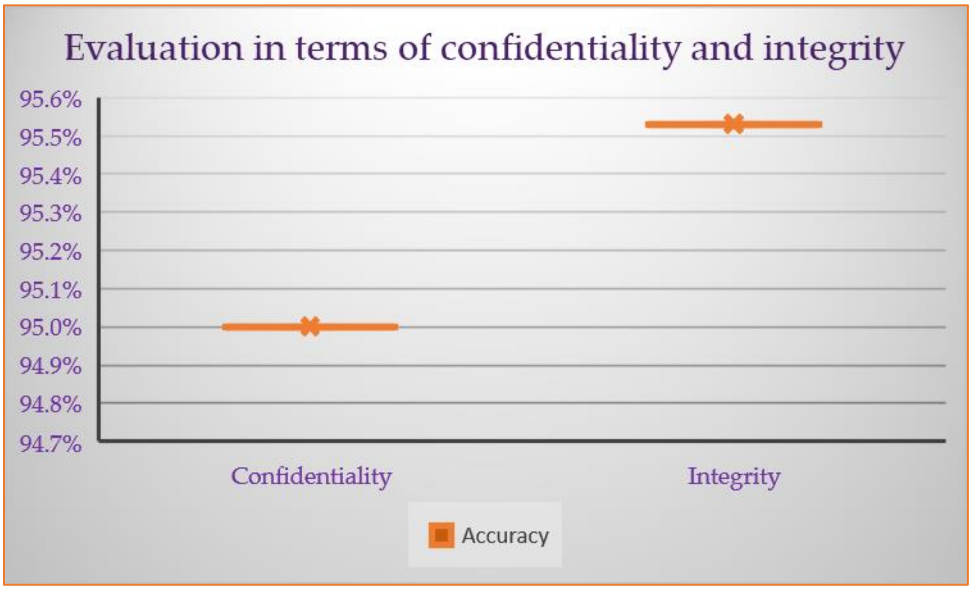

Figure 5. Confidentiality vs. integrity evaluation

As can be shown in Figure 5, the system has an accuracy of confidentiality that is more than 95% for processes using the right password and greater than 93% for procedures involving the correct secret key. That is a very high level of security, and the secrecy target with regard to the system's security has been met.

The system's reliability has been looked at from a number of different angles. In other words, a lot of different datasets and images have been used to do this experiment. There was a total of 38 images taken into consideration. The assessment for this test has been conducted by comparing two images: the original image that was taken before the image was sent, and the image that was taken after the image was delivered. A subjective assessment that is vision-based is used to compare and contrast the images in terms of the contents they include. It is a sign that the images are not integrated if they are distinct from one another owing to inconsistencies in the contents of the images. Even though the contents are integrated and identical, the two images will be distinct from one another, which is something that the subjective judgment will make obvious. Figure 6 depicts the findings that were obtained from the examination.

The experimental study indicates that the suggested system has a secrecy level of 95%, which is shown in Figure 5. In comparison, the linked dataset's integrity level is 95.53%, which is displayed in this figure. These percentages are regarded as satisfactory and possessing high levels of accuracy.

4.2.2. MLSS’s data loss evaluation

The person who is supposed to get the image will get a duplicate of the original image. On the other hand, it is possible that the size of the image that was received will be altered in some circumstances. It is necessary to measure both the size of the original image and the size of the image that was received. As a direct consequence of this, the assessment in this part will centre on this subject. When coming to this conclusion, each of the fifty-two images was taken into account. The variable to be collected is the data loss rate, which will then be calculated as RDL.

The size of the image before it is delivered presumably differs from the size of the image after it has been transferred by a certain amount; this difference is referred to as the rate of data loss (RDL). Figure 6 depicts the outcomes that may be expected from carrying out the steps outlined for this evaluation by applying a subtraction between contents of input and output.

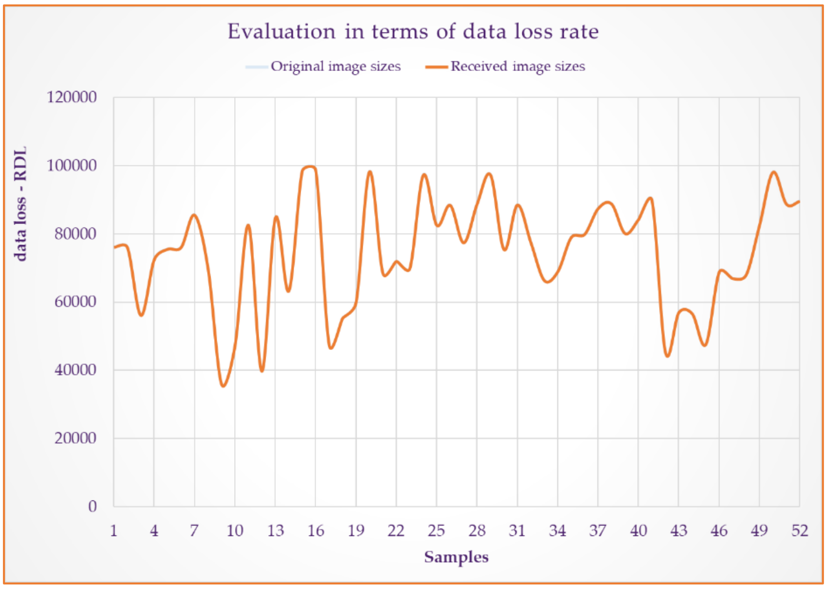

Figure 6. Data loss evaluation

4.2.3. MLSS's transferring rate accuracy (ATR) evaluation

At some point, the image from the source will be copied over to the destination. On the other hand, there is a chance that the size of the image that was received will be altered in some way. As a result, it is essential to take dimensions of both the original image and the one that has been received. As a result, we will be concentrating our analysis in this part only on this topic. For the purpose of carrying out this analysis, a total of 52 images were taken into consideration. The variable that is going to be acquired and computed is going to be the transferring rate.

As a consequence of this, the mathematical formula that is used in the computation of the ATR may be easily represented as in Equation (5):

$$A_{TR} = \frac{size_{img_2}}{size_{img_1}} (\%) \tag{5}$$

where

- A_{TR} denotes the correctness of the transferring rate and it is calculated in percentage [%] form.
- $size_{img_1}$ represents the total dimensions of the image before it is sent to the recipient.
- $size_{img_2}$ represents the size of the image after it has been received by the intended receiver.

The formula that is shown in Equation (5) will be used on all of the samples, and the results that are produced will be presented in the form of a curve in order to emphasize the overall averages of accuracy for the transferring rates for all of the samples. Figure 7 illustrates this point further.

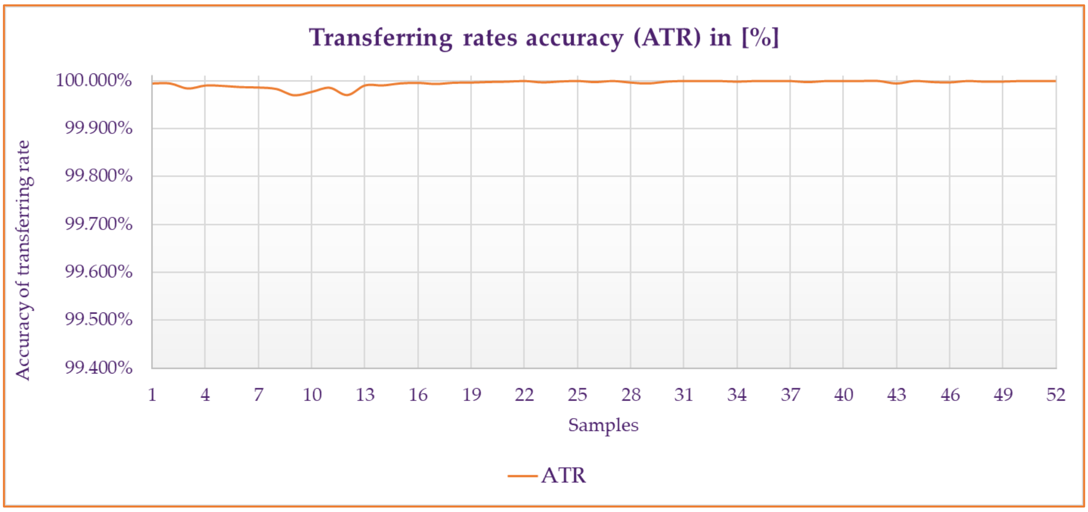

Figure 7. Transferring rates accuracy evaluation procedure

Accuracy for full samples has been shown in Figure 7, it has been proven to be above or equal to 99% of the time on average. This percentage demonstrates that MLSS has a high degree of accuracy with relation to the transmission of digital contents.

5. Conclusion

This paper proposes an MLSS applying a set of protection and security schemes to digital contents. Digital contents as an input will be initialized and pre-processed. Then, post-processing will be done. the necessary information will be extracted. Then, MLSS scrambles processed data previously. Contents will be changed to make data more ambiguous. Using a QR code technique-based encryption scheme, the encrypted data will then be safely wrapped up. After that, the digital contents will be ready to be transferred to the other party via an IoT medium. At the destination part, a verification procedure will be used. MLSS has been tested, and its effectiveness has been examined. MLSS has demonstrated that it is safe and has a very low range of data loss.

References

Ain, N., Vaia, G., DeLone, W. H., & Waheed, M. (2019). Two decades of research on business intelligence system adoption, utilization and success–A systematic literature review. *Decision Support Systems, 125*, 113113.

Alterazi, H. A., Kshirsagar, P. R., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G., & Lin, J. C.-W. (2022). Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. *Sensors, 22*(16), 6117.

Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities* (pp. 123-149): Springer.

Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. *Computer Science Review, 39*, 100332.

Bohli, J.-M., Langendörfer, P., & Skarmeta, A. F. (2022). Security and privacy challenge in data aggregation for the iot in smart cities. In *Internet of Things* (pp. 225-244): River Publishers.

Dhar, S., Khare, A., & Singh, R. (2022). Advanced security model for multimedia data sharing in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, e4621.

Golec, M., Gill, S. S., Bahsoon, R., & Rana, O. (2020). BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. *IEEE Consumer Electronics Magazine*.

Gupta, B., Chaudhary, P., Chang, X., & Nedjah, N. (2022). Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Computers & Electrical Engineering, 98*, 107726.

Gupta, D. N., & Kumar, R. (2021). Networking in IoT: Technologies Usage, Security Threats, and Possible Countermeasures. *International Journal of Sensors Wireless Communications and Control, 11*(6), 619-626.

Hang, L., & Kim, D.-H. (2020). Reliable task management based on a smart contract for runtime verification of sensing and actuating tasks in IoT environments. *Sensors, 20*(4), 1207.

Haque, A. K. M. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems, 39*(5), e12753. doi:https://doi.org/10.1111/exsy.12753

Hasan, R., & Hasan, R. (2022). Pedestrian safety using the Internet of Things and sensors: Issues, challenges, and open problems. *Future Generation Computer Systems*.

He, D., Yu, X., Li, T., Chan, S., & Guizani, M. (2022). Firmware Vulnerabilities Homology Detection Based on Clonal Selection Algorithm for IoT Devices. *IEEE Internet of Things Journal*.

Hofer-Schmitz, K., & Stojanović, B. (2020). Towards formal verification of IoT protocols: A Review. *Computer Networks, 174*, 107233.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56-59.

Karras, C., Karras, A., & Sioutas, S. (2022). Pattern recognition and event detection on iot data-streams. *arXiv preprint arXiv:2203.01114*.

Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing, 23*(3), 2067-2087.

Khan, M., Khalid, R., Anjum, S., Khan, N., Cho, S., & Park, C. (2022). Tag and IoT based safety hook monitoring for prevention of falls from height. *Automation in Construction, 136*, 104153.

Lai, S. T., Leu, F. Y., & Chu, W. C. C. (2014, 2-4 July 2014). *A Multi-layer Secure Prevention Scheme for Improving e-Commerce Security.* Paper presented at the 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.

Li, Y., Zuo, Y., Song, H., & Lv, Z. (2021). Deep learning in security of internet of things. *IEEE Internet of Things Journal*.

Mohiyuddin, A., Javed, A. R., Chakraborty, C., Rizwan, M., Shabbir, M., & Nebhen, J. (2022). Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. *International Journal of Fuzzy Systems, 24*(2), 1203-1215.

Nashwan, S. (2021). An End-to-End authentication scheme for healthcare IoT systems using WMSN. *Comput. Mater. Contin, 68*, 607-642.

Ni, C., Cang, L. S., Gope, P., & Min, G. (2022). Data anonymization evaluation for big data and IoT environment. *Information Sciences, 605*, 381-392.

Nizzi, F., Pecorella, T., Esposito, F., Pierucci, L., & Fantacci, R. (2019). IoT Security via Address Shuffling: The Easy Way. *IEEE Internet of Things Journal, 6*(2), 3764-3774. doi:10.1109/JIOT.2019.2892003

Nourani, M., Kabir, S., Mohseni, S., & Ragan, E. D. (2019). *The effects of meaningful and meaningless explanations on trust and perceived system accuracy in intelligent systems.* Paper presented at the Proceedings of the AAAI Conference on Human Computation and Crowdsourcing.

Pavlović, N., Šarac, M., Adamović, S., Saračević, M., Ahmad, K., Maček, N., & Sharma, D. K. (2022). An approach to adding simple interface as security gateway architecture for IoT device. *Multimedia Tools and Applications, 81*(26), 36931-36946.

Puthal, D., Wilson, S., Nanda, A., Liu, M., Swain, S., Sahoo, B. P., . . . Prasad, M. (2022). Decision tree based user-centric security solution for critical IoT infrastructure. *Computers and Electrical Engineering, 99*, 107754.

Raghuvanshi, A., Singh, U. K., & Joshi, C. (2022). A review of various security and privacy innovations for IoT applications in healthcare. *Advanced Healthcare Systems: Empowering Physicians with IoT- Enabled Technologies*, 43-58.

Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J., & You, I. (2019). A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. *IEEE Access, 7*, 142531-142550. doi:10.1109/ACCESS.2019.2943929

Shurman, M. M., Khrais, R. M., & Yateem, A. A. (2019). *IoT denial-of-service attack detection and prevention using hybrid IDS.* Paper presented at the 2019 International Arab Conference on Information Technology (ACIT).

Sollins, K. R. (2019). IoT Big Data Security and Privacy Versus Innovation. *IEEE Internet of Things Journal, 6*(2), 1628-1635. doi:10.1109/JIOT.2019.2898113

Tavakoli, M., Carriere, J., & Torabi, A. (2020). Robotics, smart wearable technologies, and autonomous intelligent systems for healthcare during the COVID- 19 pandemic: An analysis of the state of the art and future vision. *Advanced Intelligent Systems, 2*(7), 2000071.

Tukur, Y. M., Thakker, D., & Awan, I. (2019, 26-28 Aug. 2019). *Multi-layer Approach to Internet of Things (IoT) Security*. Paper presented at the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud).

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.

Yahyaoui, A., Abdellatif, T., Yangui, S., & Attia, R. (2021). READ-IoT: Reliable event and anomaly detection framework for the Internet of Things. *IEEE Access, 9*, 24168-24186.

Yao, X., Farha, F., Li, R., Psychoula, I., Chen, L., & Ning, H. (2021). Security and privacy issues of physical objects in the IoT: Challenges and opportunities. *Digital Communications and Networks, 7*(3), 373-384.