Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 5s (2025)

Optimizing Passport Verification Processes with Secure QR Code Technology

Vikas H[1], Meghavarshini S K[2], Divakara M[3], Manjunath M[4], Girish B Shivalingappanavar[5], Preethi G[6]

[1] vikasvicky.hr@gmail.com, Department of Electronics and Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru

[2] meghakgowda988@gmail.com, Department of Electronics and Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru

[3] divakarame@gmail.com, Department of Electronics and Communication Engineering Sri Venkateshwara College of Engineering, Bengaluru,

[4] manjunathmhr1@gmail.com, Department of Electronics and Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru

[5] girishs_9@rediffmail.com, Department of Electronics and Communication Engineering, Dr. Sri Sri Sri Shivakumar Mahaswamiji College of Engineering, Bengaluru Rural

[6]preethigaviyappa29@gmail.com, Department of Electronics and Communication Engineering, Mysore College of Engineering and Management Engineering, Mysuru

Article History:

Received: *06-10-2024*

Revised: *27-11-2024*

Accepted: *04-12-2024*

Abstract:

The main concern of today can be the quality and the security of the data. One of the new methods of the security system to resolve this can be the utilization of the QR codes, which can reduce the larger misinterpretation of the data and enhance the security, considering this research article promotes a method to encrypt the data to a QR code, which can avoid the manipulation of the data. The preferred QR code is encrypted using a secret key and will not be shared to the unauthorized personals, the usual and finest method of encryption is incorporated, which is TTJSA algorithm. The quick response system is used to encrypt the data, in to the embedded system to a form of unique style of information in the documents, the original data can be encrypted and can be verified as competing to the original data. As the system is unique and flexible to certain extent, the same can be used for the many other applications as well, this can always avoid the theft of the data from the hackers as the encryption and the decryption used are highly secure.

Keywords: Barcode, Cryptography, Decryption, Encryption, Quick Response code, Secret key.

1. Introduction

The structure of QR codes is 2-dimensional (2D) in nature, the popularity of the QR codes is consistently increasing, due to the capability of the holding large amount of data when compared to the bar codes. The similar technology can also be incorporated in certain application of the banking systems, transportable system and security system. Denso Corporation was the inventor of the QR code, and it belongs to the family of the barcode that are normally read and decoded by the cameras of the smart phones, Laptops and other smart devices, the structure of each QR code is unique and is

made of the white square filled with some peculiar patterns made of black squares [1]. The usual usage of the QR code corresponds to the Website links, social media links, data, video and images as well.

The quality information should be protected to a larger extent in current generation of digital world, the security is a key concern for every aspect of the technology, this purpose can be solved using the digital documentation methodology, which should be an authentic and secure source of encoding [2]. In this research article, a new methodology is proposed to encode the passport data into a QR code, enabling a secure encryption method, this can majorly avoid the tampering of the actual data in the passport. The TTJSA is a unique and foolproof algorithm that enables the solution for the proposed problem, this algorithm cannot be cracked unless the key is disclosed to the hacker [3]. The Original data is printed in the form of QR code and is encoded using the TTJSA algorithm with a secure key, on the other hand the decoding is performed with the key and decoding the QR code. This is the key concept behind the non-tampering of the data on the passport [4].

A. Behavioral QR codes:

The password system has safeguarded our confidential information in online applications for years. Each attempt to access an application account must pass certain authentication procedures that verify user ID and password. As more and more daily life services become available online, users have to manage more accounts and passwords [5]. Users are moreover restricted by strict password rules when setting up an account, such as lower- and upper-case letters with at least number one and a character. This is because passwords that are easy to remember are also insecure against dictionary attack or brute force guessing. Thirdly, a study conducted by Bonneau and Preibusch states that repeatedly using the same passwords renders highly-protected sites by cracking other badly managed password servers. Some application servers even request users to change those complicated passwords periodically, making them even harder to remember [6].

2. Review of literature

H. S. Ali, et. al [7] present a coordinating cryptographic symmetric key method this technique involves the bit wise rotation reversal method and Caesar cipher technique. In this method the encoding is accomplished by two algorithms, which are CCE (Caesar cipher encryption) and Bit wise rotation and reversal encryption [7]. The encoding techniques mentioned has the information is accomplished by using two algorithm and to complete the encoding of information is more secure. This methodology will be used to any text file can be tested and produce the suitable result. Because here use the two better algorithms to encoding of information in any other form using the method are Caesar cipher method encryption. Which also includes another method like MSA method then mainly used method in this process is bitwise reversal and rotation method. This process should applicable to several banking system across the globe, defense system, mobile network etc [7].

Alapetite, et. al. [8] These authors have proposed a method of sophisticated cryptographic technique utilising bit reverse and bit management. In this article, the information is encoding using two types of cryptography method they are: symmetric cryptography key and public cryptography key. In symmetric cryptography type the encryption resolution randomized key is made used for decryption process also same type of process is used. In this method the user will use the secret key these are called as a password. Then encrypting the message using these passwords again in case of decryption

process use the same method whereas used in encryption method and also use the same input have given in first process of encoding level [8].

R. Bose, et. al. [9] This paper and lights on a new technique that uses QR code in the field of cryptography this makes the method very cryptographic ground in which the cure system can store different communication data that can be featured as a large capacity storage for the conventional barcode system. This method mainly have a focus that is accumulated towards a message and also encoding the information that is provided by the secret word. The receiver obtains the data from the QR code which can be further encrypted to understand the literal form. This model can be adopted for vast management and communication systems, big business and also to encode the data which are send towards the target QR code. This method Will also work in a very fast and it is futuristic for storage capacity as well. Or the secret code will always give high security to the proposed system [9].

M. Canadi, et. al., [10] offer a new and fast approach to bit manipulation using symmetric key. The mentioned technique utilized the encryption number as a maximum of 32 and randomization maximum number is 32. Input (input data) can be in the form of matrix will have the size chose that 16x16.this input is used and where 256 types of input are obtained. This paper uses bit manipulation process which provides the block in the cipher process and MSA process for the accumulation of exploitation stream process. This process provides the manipulation of bit first along with MSA encoding next. This process can be applied continuously to increase the encryption and decoding process strength. very possibility to this method modification. One of the advantages of this process is no body can encode the message can be break. cryptographic method classical cryptographic can be divided into two types

- Cryptography is as in symmetric way input method.
- Cryptography is as in public way given input is provided [10].

J. Z. Gao, et. al. [11] The hiding of data through the efficient way requires other form characteristics. This character in now reflecting as a signature and this embedded information is existence for transmitting the data and overcome the method of steganography analysis. The analysis along with attacks of data will takes into numerous way such as disabling, pull out, demolishing secreted data. the aggressor will insert the data over the secreted data. So, for circumstance of position should two types of purposes the message disabling and their transmission the inserted data methods are differed due to information attacks [11].

Y.P. Huang, et. al., [12], Proposes the methodology of steganographic as a detecting mechanism of secreted information in a steganographic data these steganography was utilised in information communiqué along with system and secreted the information of some image are inside the data are used to send it to by the process of internet. the steganography data hiding method drastically customized. steganography method hides secret message it includes below steps. Encoding information are embedded into Quick response system are obtained the MSA algorithm. Further, lastly these randomized in general picture. then again provide the optimized information to get back the information and decode the information using decoded algorithm. This process is also a double encoded and double decoded insert method nobody will get the exact information of record. this method can next be implemented by compact the QR code through using the secreted data or record

program. So, if any of the attacker will not clever to hacking the evidence of data. In forthcoming generations this technique can be improvised in number of ways [12].

S. Lisa et. al., [13], It is a novel method that provides a collective cryptographic methods That helps in the extraction of encryption of hybrid verification system in this paper the author clearly explain how the combination of QR Code and TTJSA, akes a unique combination creating a highly secure data. Addition to this the authors also propose 3 methods that uses Vernam cipher method, NJJSA and MSA. These are the best methods to discriminate a plain text and a number of them in the ciphertext file this also helps in the encryption of QR code within the data [13].

3. Problem statement

Form the extensive survey of the literature it is clear to have a biggest challenge in the area of the security of the data, especially when confined to the passport data. The unusual tampering of the passport data, the undigitized data on the passport are leading to several misinterpretations of the details, and the human errors on the printing and reading the data. On the other hand, all these leading to the strange security breach in several countries, this is also a major cause of the illegal activities in the countries. A technique to avoid these situations is much needed with the addition of the security. The proposed research article elaborated the usage of the QR code with the unique combination of the TTJSA algothm to improve the security and validate the data authenticity with a proper key.

Apart from this the printed records like, marks cards, certificates and many others can also be secured with the QR codes and encryption methodology, this enables both security of the data and authenticity of the data.

The Keen objective of this paper is to adopt the TTJSA algorithm in combination with QR code to develop a new and secure algorithm that can encode the printed records of data in to secure QR code. The Validation of the QR code, is the next phase of the research article, in the third phase calculation of the success rate of encryption of the data from the QR code. These are the valid objectives to drive the QR code and the TTJSA algorithm in the process of secure and authentic data encoding of the passports.

Solution Strategy

Authentication and security of the digital documents are very important in the digital world, to solve the problem one of the new methods is used, which encrypts the data with the TTJSA algorithm and is encoded to QR code. The encryption is performed using the secret encryption key, which makes the algorithm still more firm in terms of security and encoding methods. To decode the method, the QR system has to use the Algorithm and key to decode the data[14-16].

In the instances of other digital documents like marks cards, identity cards and others the complete facts are now been encrypted in the QR code, this making the system unique and opt for the digital era. This methodology will also disables the tampering and morphing of the data[17-19].

4. Proposed system:

A message encoded through the TTJSA technique and QR code system is of the encrypted data is obtained. Later it is transmitted for the receiver to obtain the QR code system is decrypted through the

TTJSA technique and secret information can be obtained. The Proposed system can be reduced as block diagram as shown in the figure 1.

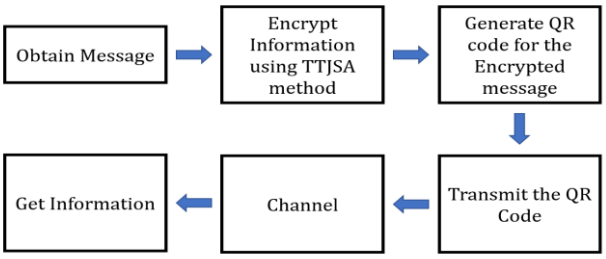

Figure.1. Flow chart of proposed method

This is one of the encryption and decryption algorithm used for hiding the data in the form of images and retrieving the same from the image into the original form. This method can be used for Aadhar card, Voter ID, License, Passport or mark sheet where the data is encrypted using a secrete key, this encrypted text information is converted into QR code which is an image generated by the QR code technique. This image is printed on the original document. The data can be retrieved by decoding the QR code using same secrete key, the contents of the QR code will be obtained in text format will be contrast to the correct information contents. Even if someone tries to temper the content of the original data, he cannot modify the since data will be obtained through Encryption of Original data, using a secrete key.

A. **Software Requirements and Specification**

The experiment has been set up on a laptop for having a processor of Intel i5, 12th generation, The minimum requirement of the memory is 16GB, Whereas the system had a SSD of 1TB. The operating system of the laptop is windows 11 with a brave browser installed. The simulation is carried out using MATLAB online version of the tool.

B. **MATLAB**

The MATLAB is an interactive environment and high level language used by engineers and scientists in the world wide. It visualizes and explore the ideas and collaborate access disciplines including image processing, signal processing, communications, control system and computational finance.

The MATLAB environment is utilised for write programs and develop algorithms and applications. It also includes these methods like differentiation and integration, Fourier analysis, eigen values

5. PROPOSED WORK DESIGN

The Proposed design can be split into 2 parts encryption and decryption algorithm, the same has been discussed in detailed in the next paragraph.

A. Flow Chart of Encryption Algorithm:

The algorithm is developed by Nath [15], this algorithm is a amalgamation of three different cryptographic approaches that are termed as Vernam cipher encryption, MSA algorithm and NJJSAA technique. All the above-mentioned techniques will use QR code for the purpose of encryption. Figure 2, Show the algorithm and the flow chart that is used for the encoding technique, In the first step the

passport data is converted to ASCII value, then it is converted to binary value, the following phase of the algorithm is the utilization of a Vernam cipher encryption. Whereas now the data is implemented to perform XOR operation that gives a message and also a key for the same length as that of the encrypted message signal. Now the resultant message signal will be a sequence of 1s and 0s, Additional to this the ascii coding will also convert the key into the binary format, disguising the original structure of the key. The next phase of the algorithm utilizes NJJSAA Encryption techniques.

- The input file is read at a rate of 32 bytes at a time as the very first step
- This data is encrypted in two to 56 bits and it is sorted in an single dimensional array for the next step
- As the third step the bit stream is now taken as first bit and considered with digits corresponding to the methods of inputs that exchanges the 1st fragment and also the nth fragment from the tributary fragments
- The last step is to perform the interchange operation for the 3rd bit and the second bit and it continues to 256 the fragment.
- In the 5th stage the right transfer operation is performed with the help of fragments that are obtained from the data of the previous steps
- In the 6th step it is seen that the XOR operation is performed on the data. This helps the fragmentary and fragment two to pair up with the fragment four and this process continues up to 256 fragment.
- In the very next step and the last step but the right shift operation is performed for two bits right and 3 bits to the nth bit of right shift.

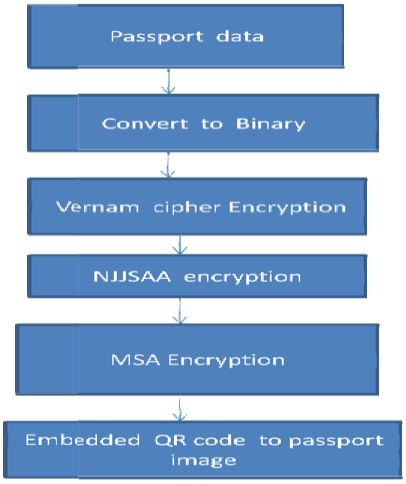

Figure 2: The algorithm flow of the process of encryption

In the next phase MSA algorithm is used, this is also a replacement process which improves the option of numerous encryption and multiple decryption techniques. It takes a character from the input file and a corresponding character from arbitrary input that helps in substituting surrounding encrypt information, In the subsequent step it is stored for into the folder. In figure 3 shows a randomized input

method that is utilised for the purpose of complete through. First call function is used for cycling and then the second function is used for upshifts of the data. The third call function is now utilized for the downshift of the data and also it performs a left chip operation after performing the right shift operation which consumed by the encryption of call function.

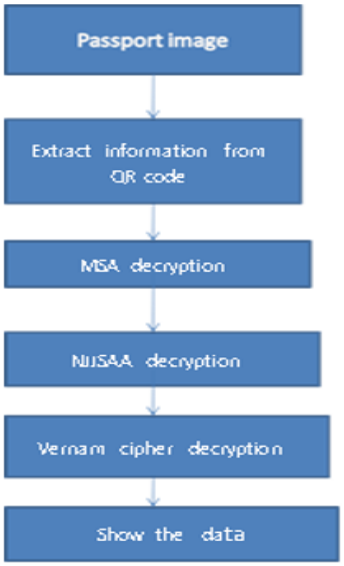

Figure 3: the Decryption algorithm of the Proposed methodology

Once the data has been encrypted, the encrypted QR code is created by the process of embedding it using a variety of protocols. The pass port image incorporates these QR codes.

Flow Chart of Decryption Algorithm:

Further the detail further the details of the passport can be extracted by decrypting the QR Code the decoding method is exactly opposite to the encoding techniques, the algorithm uses the same input as if the beginning of encoding method. Technically a camera or a scanner Is used to scan the QR code and also it is used to encrypt the data.

4. SYSTEM DESIGN

A. QR code Features

QR code is urbanized by Denso corporation in 1994. Example of QR code representation as shown in figure 4. In QR code 40 versions are there in that for error correction four levels are used and for encoding 7089 numeric data symbol size maximum. The 30% of the code symbol words allows error correction for recovery.QR code will have advanced features [20][21].

Figure 4: QR code representation of example.

- High data encoding capacity:
- QR code system has maximum ability to encode about 7089 characters.
- High speed scanning and reading:
- QR code reader has the ability to recognize many QR code symbols and therefore is read fast.
- capable of reading Japanese and Chinese encoding:
- QR code can also read Japanese and Chinese characters just as fast as English characters.
- Can be read form any direction:
- Since it is a two-dimensional code, it can be scanned and read from any direction.

B QR **code encoding**

The QR code consists of a function pattern, encoding region as shown in figure 5. Timing patterns, finder, separator and patterns alignment comprise patterns functions encoding data is used by function patterns. These patterns are situated at three corners of representation planned to assist in location easy of its position, size and fondness [22].

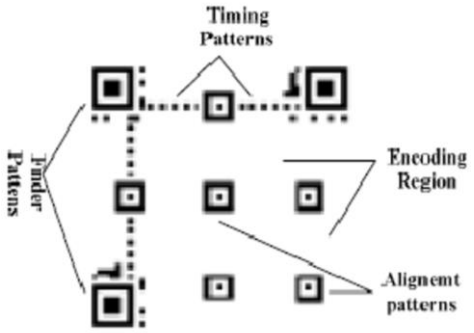

Figure 5: QR code system arrangement.

There are several steps to perform a QR code encoding, In the earlier stages the input data is determined using the most competent mode and it forms a stream of bits. The codewords are created by extracting and dividing the bit streams into several parts these code words are now separated into several blocks which includes the error correction codes to each word block. A matrix is used to represent all these code words in a single cluster, they are now masked with the pattern of mask. Further these patterns are now being the function of additional and to the QR representation the QR code representation is produced within no time.

C. SECURITY ANALYSIS:

In this method consider the data of the any student marks obtained as shown in figure 6 which is original data of the student then this obtained marks some unknown person changed the marks of the obtained by the students in one subject is as shown in figure 7 then they will do the encryption for the changed tempered data then again consider the frequency analysis for both these data that is for original data and tempered data after run the frequency analysis then it will shows the different patterns for both of date this frequency analysis as shown in fig.5.4.1 and 5.4.2.

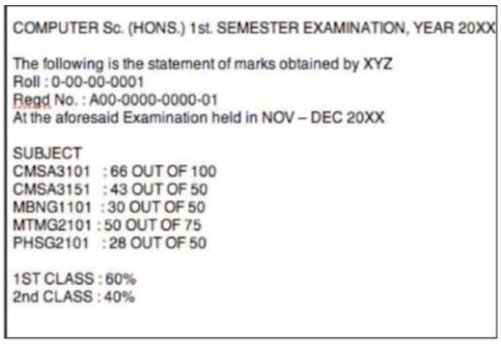

Figure 6: Original Data

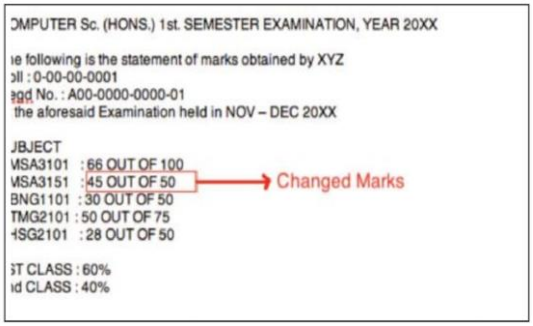

Figure 7: Tampered Data

Frequency Analysis :

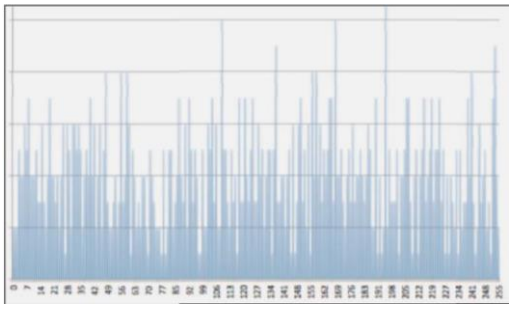

Figure 8: original file encrypted frequency analysis.

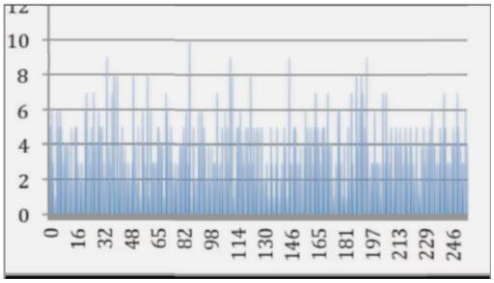

Fig 9: Tempered data of encrypted frequency analysis.

The figure 8 shows frequency analysis of encrypted original file .and the figure 9 shows frequency analysis it shows analysis of encrypted tempered data. So that from the evident for the tempered data and original data encryption of tampered data will have different pattern from the encryption of original data again encoding the information of frequency analysis will be contrast than shows that which one will be unique otherwise not.

6. IMPLEMENTATION AND RESULTS

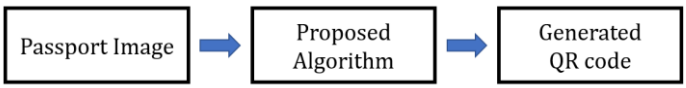

Figure 10: Design Flow

A. Implementation:

MATLAB is an incorporated scientific computing surroundings that combine numeric calculation highly developed graphics and visualization as well as high level programming language. The Implementation of the proposed methodology is depicted in the figure 10.

B. Results Snapshots

The current folder path, work space, command window, command history, and editor window are the components of the MATLAB window. It is possible to choose the desired path—that is, the folder and folder name that will show on the current folder path—by using the current folder.The variables in the current code will be listed in the work space. The work that is being done in the current event will be recorded by the command history, the command window will display the results of the work that has

been done in the code, and there will be commands like Clc to clear the command window and clear to clear the work space. Additionally, a figure window will be obtained when you type an argument like figure in the command window.

The code used to implement the project is found in the MATLAB code window. code will generated using MATLAB function and Guide window that is graphical user interface development and environment .this code is the important part for the development of project.

Figure 11: Passport image

The figure 11 shows the image of the Passport after run the program the blank window will appear then select one passport image will appear on the blank window. The Passport image will contains the details of text like Name ,Date of birth ,Passport number, Nationality ,City ,Issue date, Expiry date, Gender .these are the inputs of project. These particulars are filled in corresponding empty box.

Figure 12: Generate QR code

A sample QR code is shown in the figure 12. Once the passport image and the details of the passport user is filled into the passport command using the TTJSA encryption algorithm method, The Varnaam cipher encryption and NJJSA encryption and MSA encryption are used to encrypt the data into an encoded pattern. The generated QR code consists of different protocol these are used to embed the details of the passport owner and the details of the passport into a QR code. Figure 13 shows a sample of data that has been stored on the QR code.

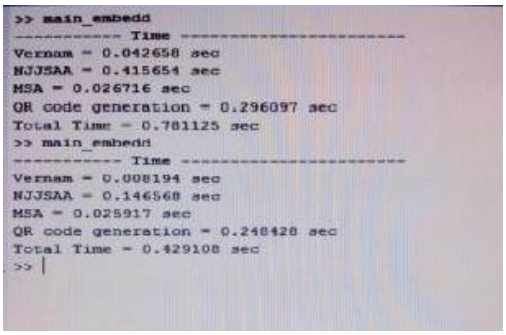

Figure 13: Command window display time

Encrypting the information using various method it takes some time during encryption process. after the development of QR code display the how much time taken in each method that will displayed in the command window is as shown in figure 14.

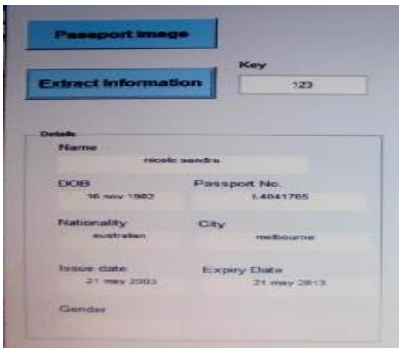

Figure 14: Extract the information

The figure 15 shows the extract information. The TTJSA algorithm is used to extract the Passport image, from QR code. The decoding method be opposite method exactly and then obtain the original data, further, use the input method same as in encoding method.

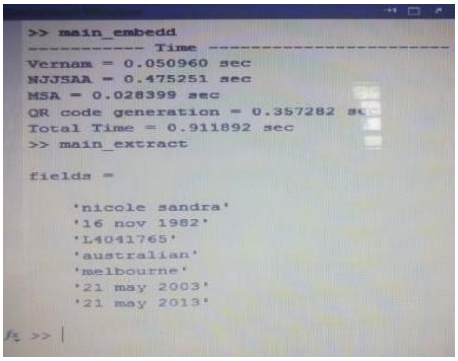

Figure 15: Encrypted text fields

After extract information from QR code by decryption process and get back to the encrypted original message. These messages will display in the command window as shown in figure 15.

7. ADVANTAGES AND APPLICATIONS.

The novel method of using Quick Response (QR) codes for secure passport validation offers transformative benefits in the domain of identity verification and international travel security. By leveraging the robustness of QR codes integrated with encryption techniques, this approach ensures

enhanced security, efficient processing, and reduced chances of forgery. Its applications span across multiple sectors, revolutionizing traditional methods of identification and authentication. Below, we delve into the key advantages and potential applications of this innovative system, the advantages and applications are as follows:

A. ADVANTAGES

All two dimensional symbols are integrated into the QR code. The vintage points of the QR code technique is that they have a larger data capacity with the high density of data. These quotes can be read from 360 degree angles and the response of the codes are literal quick. The capability of these QR codes in terms of error correction capability is very high. The special characters and alpha numerical characters can also be used in the QR code.

B. APPLICATIONS

- The above system can be used to verify data for other applications like mark sheet, driving license ,voter ID , Aadhar card etc.
- This method can also be applicable to other applications like banking system, finance system, defense system, educational system, mobile network etc.

8. Conclusion and Future Enhancement

Development of QR code will offer data encryption using various algorithms and QR code encoding. The TTJSA algorithm is used to decode the encrypted data from the Quick Response System on today's quicker smartphones running Android or a mobile operating system. Here, the data or any kind of information was encrypted and decrypted using three different kinds of algorithms. After analyzing all three methods with various picture or data formats, it can be concluded that the Vernam approach is the most appropriate for encrypting images or data. In contrast, the NJJSAA method is not seen to be very effective for encrypting any data because it has a higher PSNR value and a lower MSE value.

Other algorithms that can provide lower PSNR and MSE values can be used to further improve this work. This work's future scope includes the ability to generate QR codes using the Android OS, which can be simpler to create and use, without the need for any algorithms. The Android may have an integrated application that allows it to be scanned and saved for later use, which could also help reduce CPU time.

References

[1] Reed and G. Solomon. Polynomial codes over certain finite fields. Journal of the Society for Industrial and Applied Mathematics, 8(2):300–304, 1960.
[2] "QR Code, Wikipedia", http://en.wikipedia.org/wiki/QR_code [Retrieved 2012-02-09]
[3] "ZXING- QR Code Library ", http://code.google.com/p/zxing/ [Retrieved 2012-02- 09] [15] "2D Code", http://www.denso- wave.com/QRcode/index-e.html [Retrieved 2012-02- 09]
[4] "Malicious QR Code", http://www.abc.net.au/technology/articles/2011/06/08/ 3238443.htm [Retrieved 2012-02-09]
[5] "QR Code", http: // www.tec - it. Com /en /support /knowbase /symbologies /QRcode /Defa ult.aspx [Retrieved 2012-02-09]
[6] "Reed-Solomon and Bose – Chaudhuri - Hocquenghem Code " , http: // www. berndfriedrichs.de/downloads_ecc/ ecc2010_ch08.pdf [Retrieved 2012-02-09

[7] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, et al., "QR code security," in Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, 2010, pp. 430-435.
[8] H. S. Al-Khalifa. Utilizing QR code and mobile phones for blinds and visually impaired people. In ICCHP, pages 1065–1069, 2008.
[9] Alapetite. Dynamic 2d-barcodes for multi-device web session migration including mobile phones. Personal and Ubiquitous Computing, 14(1):45–52, 2010.
[10] R. Bose and D. Ray-Chaudhuri. On a class of error correcting binary group codes*. Information and control, 3(1):68–79, 1960.
[11] M. Canadi, W. Ho pken, and M. Fuchs. Application of QR codes in online travel distribution. In ENTER, pages 137–148, 2010.
[12] J. Z. Gao, H. Veeraragavathatham, S. Savanur, and J. Xia. A 2d-barcode based mobile advertising solution. In SEKE, pages 466–472, 2009.
[13] Y.-P. Huang, Y.-T. Chang, and F. E. Sandnes. Ubiquitous information transfer across different platforms by QR codes. J. Mobile Multimedia, 6(1):3–14, 2010.
[14] S. Lisa and G. Piersantelli. Use of 2d barcode to access multimedia content and the web from a mobile handset. In GLOBECOM, pages 5594–5596, 2008.
[15] S. Dey, S. Agarwal, and A. Nath, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," in Communication Systems and Network Technologies (CSNT), 2013 International Conference on, 2013, pp. 512-517.
[16] S. Dey, "SD-EQR: A New Technique To Use QR CodesTM in Cryptography," arXiv preprint arXiv:1205.4829, 2012.
[17] Dr. Shubha Joshi, Dr. Mitul Dutta, Dr. Karuna Gajanan Pawashe, Dr. Amit Bajirao Jadhav, Dr Harish S., Satyam Singh, “International Journal of Medical Toxicology and Legal Medicine”, International Journal of Medical Toxicology & Legal Medicine, Volume 28, No. 1, 2025, e-ISSN: 0974-4614, p-ISSN: 0972-0448, page 156-166
[18] Dr. Nikhilchandra Mahajan, Dr. Jayita Moulik, Dr. Abhinov Thamminaina, Dr. Mario Antony, Dr. Anil Kumar C., Dr. Bommuluri Bhavana Rao, “The Use of Toxicology in Workplace Drug Testing: Legal and Ethical Issues”, International Journal of Medical Toxicology & Legal Medicine, Volume 28, No. 1, 2025, e-ISSN: 0974-4614, p-ISSN: 0972-0448, page 167-176.
[19] Dr. Vinod H. Patil, A. Deepak, Dr. Himanshu Sharma, Lavanaya Vaishnavi D. A., Upendra Singh Aswal, K. K. Bajaj, Dr. Anurag Shrivastava, “Development of Functional Test Cases Using FSM and UML Activity Diagrams for MDT”, International Journal of Intelligent Systems And Applications In Engineering, ISSN:2147-67992, IJISAE, 2024, 12(14s), 12–21.
[20] ISO 16022:2006. Data Matrix bar code symbology specification. ISO, Geneva, Switzerland.
[21] ISO 18004:2006. QR Code bar code symbology specification. ISO, Geneva, Switzerland.
[22] ISO 24778:2008. Aztec Code bar code symbology specification. ISO, Geneva, Switzerland.