DESIGN AND IMPLEMENTATION OF SECURE QR CODE APPLICATION

D Rajendra Dev [1], K Gowri Rajeswari [2], D Bindu [3], J Vijayasri [4] , G Poornima [5,] G Jahnavi [6]
Department of Computer Science and Engineering Vignan's Institute of Engineering for Women,
Visakhapatnam, Andhra Pradesh, India.

ABSTRACT
The QR code cryptography with a password and sends it to the required hiding the information QR code. Securing and hiding personal confidential information has become a challenge in these modern days. Due to the lack of security and confidentiality, there are chances that forgery of the confidential information or unauthorized access of a system can cause a big margin loss to a person or a system. At present, confidentiality is maintained in old ways and for that reason, there are possibilities that the confidential information might get forged or hacked. Personal confidential information can be securely shared with the expected person and the person can verify the information by checking its authenticity. Similarly, confidential information can also be kept securely hidden and used to meet a specific purpose like getting access privilege of a secured system and the system can validate the confidential information by checking whether the person is authorized or the information is valid. QR codes are being used increasingly to share data for different purposes. In information communication, QR code is important because of its high data capacity. However, most existing QR code systems use insecure data format and encryption is rarely used. A user can use secure QR code technology to keep information secured and hidden. cryptography, encrypt, confidential, secure, QR code.

Keywords:
 cryptography, encrypt, confidential, secure, QR code.

1.INTRODUCTION
The rapid development of networks such as the internet, intranet, wireless communication, etc., requires securing QR codes are being used to conceal personal confidential information. increasingly to share data for different purposes, such as authentication, verification, etc. The The high data capacity of QR codes contributes to their popularity. It is possible to use a secure QR code technology to keep his sensitive information perfectly secured at all times, without Information gets leaked to the outside world.
Visual cryptography is a secret sharing scheme that takes a secret image as input (i.e. printed, handwritten) and encrypts it into a set of other images called shares in such a way that the original A secret is revealed if the shares are printed on transparent materials and superimposed or staked over another. The simplest kind of visual cryptography, also known image as input and treats each pixel separately. The suggested structure has a web application thatuses visual cryptography to secure data. The program provides a necessary and simple connection.A two-layered grid scanner tag called a QR code can encode and store a lot of speed as well as accommodation, QR code shave been utilized widely in numerous fundamental applications like wellbeing, schooling, and finance Various secured QR-based payment methods framework is proposed in writing.

2. LITERATURE SURVEY
In this paper we studied, a technique for implementation of QR code application based on cryptography. Visual cryptography is a new secret-sharing technology. It improves the secret share to restore the complexity of the secret, relying on human visual decryption. Compared With traditional cryptography, it has the advantages of concealment, security, and the simplicity of secret recovery The method of visual cryptography provided high security.

requirements of the users and protects them against various security attacks. It is easy to generate value in business applications. In this paper, we propose a secure QR code. scheme to protect the user's information from being stolen using visual encryption technology. The scheme can be applied in the fields of document management and customs security. system, medical medicine, and other fields. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans without the aid of computers. In 1994, M. Naor and A. Shamir first introduced visual cryptography and provided their constructions of visual-cryptographic solutions for the general knowledge out of a secret sharing their problems at their paper A visual cryptography scheme is a method to encode a secret. noise-like shadow image called share images, and the share images need some processing to r image into a construct the secret image The detailed principle of visual encryption is that the secret image is divided into several share images by cryptographic operations and distributed to different participants. The pixels of each share image appear to be randomly distributed. Decryption is possible by stacking an adequate number of shares. The secret image revealed and can be decoded by the human visual system (HVS) on the condition of the absence of any complicated computation or replacement algorithms. Moreover, no Knowledge of sophisticated cryptographic techniques is needed for the encryption and decryption processes. QR codes are for the most part used to convey or store messages because of higher or huge capacity limits when compared to other typical regular "standardized identifications."

3. PROPOSED SYSTEM

The proposed system maintains key generation as well as QR code generation. Also, the system verifies an encrypted QR code using the AES Digital Signature mechanism to check whether the personal confidential information in the encrypted QR code is signed by the authentic source.

If the QR code exists against the given identification number, the user will clearly see the successfully verified details of the QR code bearing the personal confidential information.

The client side of the application consists of the web application along with the mobile responsive feature. The web application contains a QR code verification process in terms of personal confidential information verification (authentication) as shown in the QR code.

Users interact with the application by registration process which is followed by authorizing the credentials each time a user wish to enter into the system. It is assumed that the user has the QR code along with the unique identification number printed on a legal document like as certificate, check, NID, ATM card, PIN, PNR, ticket, coupon etc. While being connected with the server, the client-side application's verification module takes the QR code identification number from the user and verify that the QR code printed on the legal document is genuine/authentic.

3.1 PROPOSED SYSTEM ARCHITECTURE

The Software Requirement Specification is produced at the culmination of the analysis task. The introduction of the Software Requirement Specification states the goals and objectives of the software, describing it in the computer-based system. A requirement is a statement about what the proposed system will do and that all stakeholders agree in-order for the customer's problem to be adequately solved. Requirements can be specified into three major types. They are: User Requirements and Software Requirements.

A. Visual Studio Code Editor:

Visual Studio Code is a free code coding editor that helps you start coding quickly use it to code in any programming languages, without switching editors, visual Studio code has support for many languages, including Python, Java, C++ and JavaScript.

B. Sqlite3 Database:

A standalone command-line shell program called sqlite3 is provided in SQLite's distributed. It can be used to create a database, define tables, insert and change rows, run queries and manage SQLite database file. It also serves as an example for writing applications that use the SQLite library.

C. Framework :- Tkinter or Flask Framework

Tkinter :- Tkinter is the de facto way in Python to create Graphical User interface (GUIs) and is included in all standard Python Distributions. In fact, it's the only framework built into the Python standard   library. This python framework provides an interface to the TK toolkit and works as a thin object-oriented layer on top of TK. The TK toolkit is a cross-platform collection of 'graphical control elements', aka widges, for building application interfaces.

D. Hardware Requirements:

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware, A hardware requirements list is often accompanied by a hardware compatibility list (HCL), especially in case of operating systems. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular operating system or application.

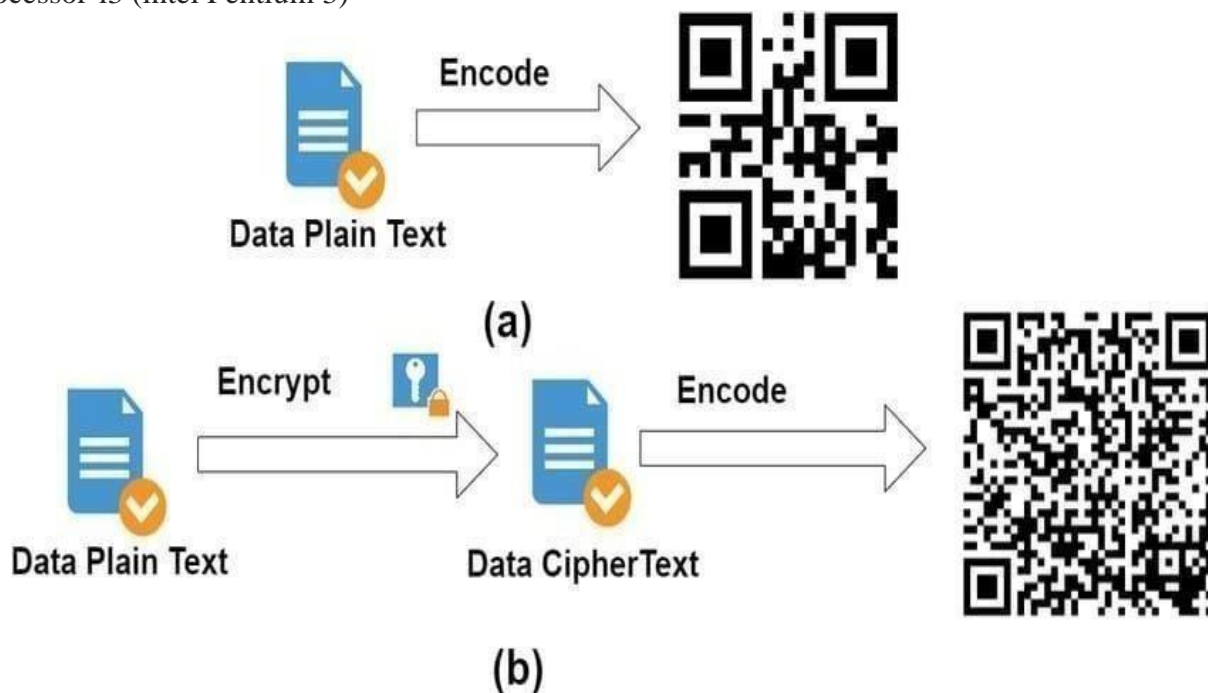Memory 512 MB RAM

Processor-i3 (intel Pentium 3)

Fig 1.0 The model of encoding the data in QR code

3.2 Methodology

Basically prototyping methodology usually is used when there will be changes during the process or progress of the project because of some new added ideas on the system. Analysis, Design and Implementation phase will perform at the same time in order to producing a system prototype.

This cycle will repeated based on comments and feedbacks until the requirement of the prototype finally meet. The final and last prototype

Project Analysis

Requirement Gathering

Coding / Development

Testing

Debugging

Re-coding, Testing, Debugging (if needed)

Delivery & Documentation which is after all the changes have been done will be called the system. Last but not least, this methodology like mentioned before is divided into 4 phase which are Planning, Analysis, Design and Implementation and the main advantage of this methodology is it can still deliver the system quickly to user although the requirement not fully meet.   The client side of the application consists of the web application along with the mobile responsive feature. The web application contains a QR code verification process in terms of personal confidential information verification (authentication) as shown in Figure. Users interact with the application by registration process which is followed by authorizing the credentials each time a user wish to enter into the system. It is assumed that the user has the QR code along with the unique identification number printed on a legal document like as certificate, check, NID, ATM card, PIN, PNR, ticket, coupon etc.
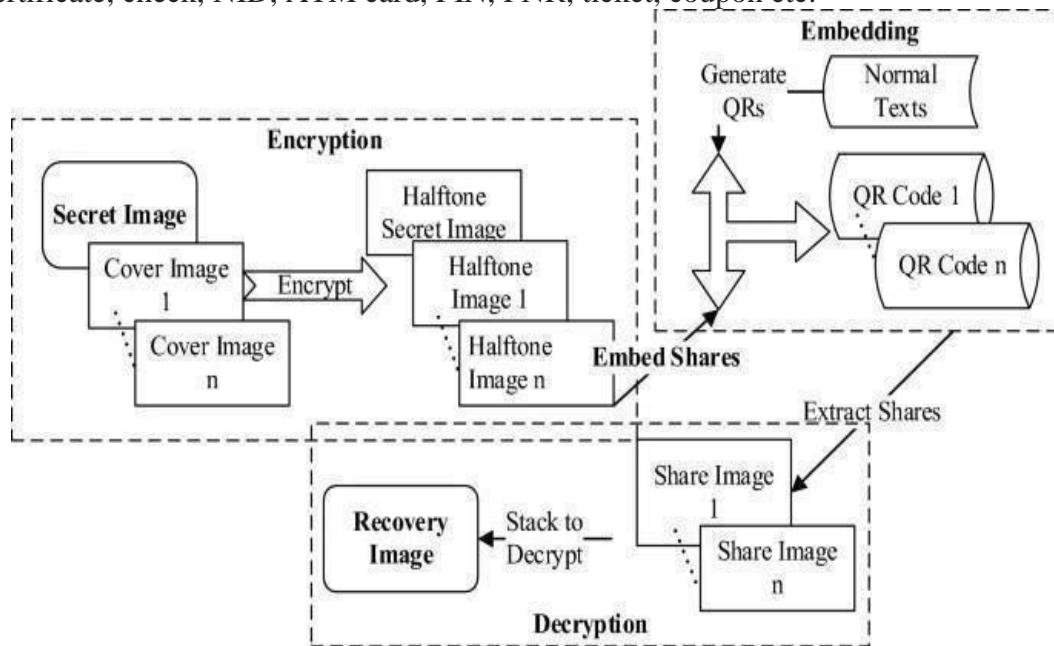

Fig 1.1 Methodology

Encrypted

Encryption changes data or information that is normally plaintext through the usage of an algorithm so that someone must possess certain knowledge to access it. This special knowledge is normally called a key. For example, something is encrypted if someone must enter a password to access it. Encrypted QR codes are QR codes that not everyone can scan and access.

Embedding

These embedding are designed to be compatible with standard decoding applications and can be applied to any color image with full area coverage. The embedding problem is solved by the integration of halftoning method. Finally, we show experimental results of half toning of color image, embedded QR code image in color image and decode QR code image from color image.

Decryption

Decryption is the transformation of data that has been encrypted and rendered unreadable back to its unencrypted form. The garbled data is extracted by the system and converted and transformed into texts and images that are easily understandable by the reader as well as the system. Simply put, decryption is essentially the reverse of encryption, which requires coding data to make it unreadable, but the matching   decryption keys can make it readable.

4. RESULTS AND ANALYSIS

The results obtained from the proposed method have obtained an The suggested structure has a web application that uses visual cryptography to secure data. The programme provides a necessary and simple connection point for users to exchange connections using QRCode. A two-layered grid scanner tag called a QR code can encode and store a lot of data. Because of its speed as well as accommodation, QR codes have been utilized widely in numerous fundamental applications like wellbeing, schooling, and finance. Various secured QR-based payment framework is proposed in writing. AES algorithm benchmark and legalized checking module. The average execution time and memory load of benchmarks applied to 15 simulation data in each process AES encryption benchmark spent the fastest execution time from 0.0059104 seconds to the slowest in 0.001703024 seconds thus provided average value was 0.001181571 seconds (s) or 1.181571 in milliseconds (ms). The fluctuated of execution time in AES benchmark testing can be depicted in Figure 1.3.

Next, legalized module benchmark spent the fastest execution time in 0.47792602 seconds and the slowest is in 1.48998284 seconds thus provided an average value is 0.704013634 seconds or 704.013634 milliseconds. Lastly, the legalized page menu benchmark provided the fastest execution time is 0.58162999 seconds and the slowest is 1.65834403 seconds or spent in average as 0.762566141 seconds or 762.566141milliseconds.

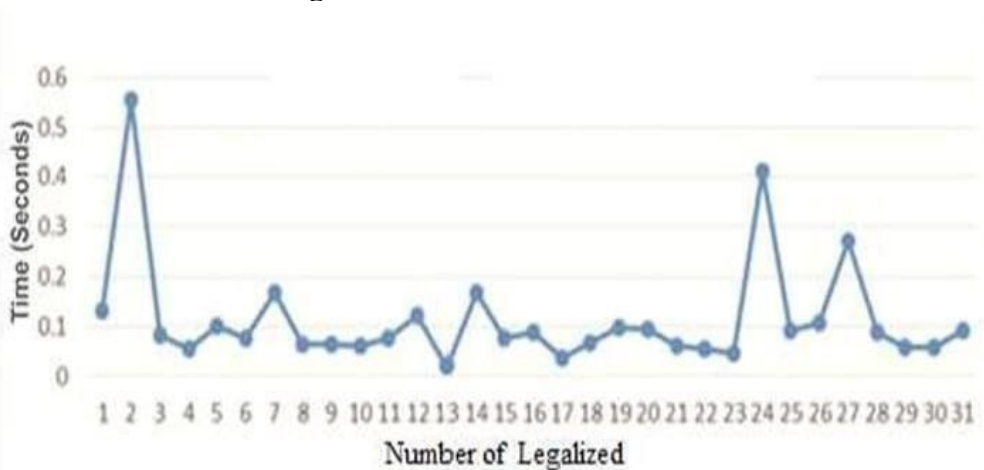| Main Process	Object	Time Execution (ms)	Memory Load (MB)
Legalization Process	AES Encryption	1.18157	0.95601
	Legalized Module	704.013	0.97829
	Legalized Page	762.566	0.77327
Legalization Checking Process	AES Decryption	1.28200	0.54662
	Checking Module	114.386	0.54868

Fig 1.3 Performance Evaluation

Fig. 13. Execution time for checking module

Memory load for AES encryption benchmark during the legalization process provided the smallest one is in 0.9539948 MB and the biggest is in 0.956019093 MB thus proposed the average value is 0.95601 MB. Legalized Module benchmark spent memory load from 0.9762878 MB as the smallest and 0.9804382 MB as the biggest one thus average value around0.978295873 MB. Meanwhile, legalized page menu benchmark spent memory load in 0.7643204MB up to 0.7919862 MB thus average value around 0.773273 MB. The graphical performance of memory   load in the legalization process.
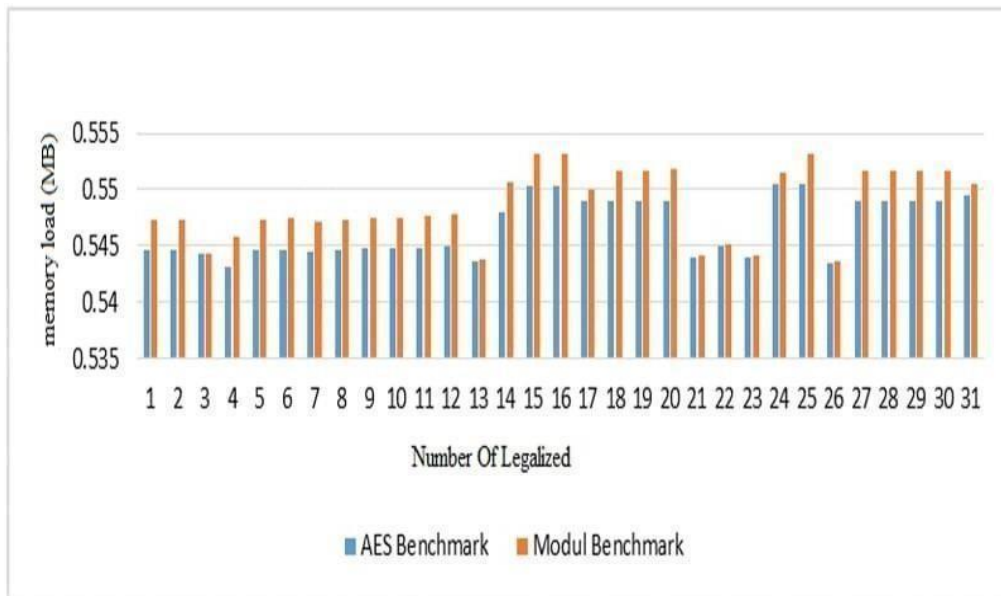

Fig. 14. Memory Load for Bechmark Testing in Legalization Checking Process

For legalization checking process, 31 data testing were simulated. AES decryption benchmark provided the fastest execution time in 0.01621246338 milliseconds and the lowest in 4.427195 milliseconds thus the average values in 1.282007 milliseconds.

Memory load for AES decryption benchmark during the legalization process provided the smallest one is in 0.5431519 MB and the biggest is in 0.5504684 MB thus proposed the average value is 0.546623229 MB. Meanwhile, checking module spent memory load in 0.5436478 for the smallest and 0.553215 MB for the highest thus provided the average value is 0.548683165 MB. The description of this performance is explained in Figure 14.

5. CONCLUSION & FUTURE SCOPE

In this undertaking, we proposed a solid QR Code sharing application and expanded the security of connections with picture cryptography. Dissect the techniques for creating and examining Quick Response (QR) codes. Speedy Response codes are 2-D matrix codes that are utilized to encode and translate data. QR codes can encase data, for example, in text or URL joins. The various sorts of QR codes and their essential construction are talked about. The down to earth investigation was performed to inspect how really QR Codes function. Fast Response Code is an exceptional element of any gadget that gives machine vision capability to the gadget that is safeguarded by human vision. It has a number of benefits that make it more usable and are additionally discussed. The finish of the examination is a QR code, which is the modernization of item or individual recognizable proof openly by concealing data to others and to interface various characters at a solitary area.

Under the future scope,

We may further enhance this application to formulate encrypted QR codes with multi-level encryption techniques.

The QR codes could be integrated with different biometrics and ERP applications for the exchange of data between B2B and B2C in a secured environment with the use of hardware.

We may utilize QR codes for their storage on cloud as encrypted images which have data stored in them that is further encrypted using several encryption techniques.

Flexibility to add customization

Ability to track scans

Affordability

Ability to store a large amount of data and multimedia

Ease of Accessibility

REFERENCES

[1]   Taolin Ma, Huixu Zhang, Jun Qian, Xinglong Hu, and Yufei Tian: The design and implementation of an innovative mobile payment system based on QR Code. 2015 International Conference on Network and Information Systems for Computers, 435–440, 2015.

[2]   Jerry Zeyu Gao, Lekshmi Prakash, and Rajini Jagatesan Understanding 2D barcode technology and applications in m-commerce design and implementation of a 2Dbarcode processing solution, 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), pages 49–56, 2007.

[3]   Kamal, Sawsan, and Ameen; Basheer (2016) "A New Method for Ciphering a Message Using QR Code". https://doi.org/10.1155/2018/4036815 (2018).

[4]   Cheng, Y., Fu, Z., Yu, B., and Shen, G. A new two-level QR code with a visual cryptography scheme, Multimed. Tools Appl. 77(16), 20629–20649, https://doi.org/10.1007/s11042-017-5465-4 (2018).

[5]   Dey, S., Nath, A., and Agarwal, S., "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System" , International Conference on Communication Systems and Network Technologies, DOI 10.1109/CSNT.2013.112, 2013.

[6]   Bhavar , S., Jadhav, J., Kulkarni, N., and Patil, K., "Authenticate Message Hiding in QR Code Using AES Algorithm", International Engineering Research Journal (IERJ), Volume2 Issue 1, Pages 367–369, ISSN 2395-1621.

[7]   DR.C.K.Gomathy , V.Geetha , S.Madhumitha , S.Sangeetha , R.Vishnupriya Article: A Secure With Efficient Data Transaction In Cloud Service, Published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5 Issue 4, March 2016, ISSN: 2278 – 1323.

[8] Cai, H.L.; Yan, B.; Chen, N.; Pan, J.S.; Yang, H.M. Beautified QR code with high storage capacity using sequential module modulation. Multimed. Tools Appl. 2019, 78, 22575–22599.

[9] Akta, C. The Evolution and Emergence of QR Codes, 1st ed.; Cambridge Scholars Publishing: Cambridge, UK, 2017.

[10] Dudheria, R. Evaluating Features and Effectiveness of Secure QR Code Scanners. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China, 12–14 October 2017; pp. 40–49.

[11]   KasperSky Lab. QR Code Reader and Scanner: App for Android. 2018. Available online: https://free.kaspersky.com/?cid=acq-gplay-lnk#mobile (accessed on 16 April 2020).

[12] G Data Software AG. G DATA QR Code Scanner. 2018. Available online: https://www.gdata.de/ (accessed on 16 April 2020).

[13] NortonMobile. Norton Snap QR Code Reader. 2016. Available online: https://support.norton.com/sp/en/us/home/current/solutions/v64691018_EndUserProfile_en_

us?client=norton&site=nrtn_en_US (accessed on 16 April 2020).

[14]   Trend Micro. QR Scanner-Free, Safe QR Code Reader, Zero Ads. 2018. Available online: https://www.trendmicro.com/en_us/business.html (accessed on 16 April 2020).

[15]   Avira. Free QR Scanner. 2018. Available online: https://www.avira.com/ (accessed on 16 April 2020).