Implementation of Security Scheme for QR code based Application with Enhanced (k,n) sharing Approach

Sarika Laiphrakpam[#1], Mrs. D. B. Gothawal[#2]
[1, 2]Dept. of Computer Engineering
DYPCOE, Akurdi, Pune, Maharashtra, India

***Abstract*.— QR barcodes are used extensively due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. QR code based applications are mostly used for storing small piece of data and share it with others. This type of application lacks security because any one can scan the QR code and gain information. The proposed system designed for providing security to QR code based application. The system can store users private, public data and share it with others using splited QR code techniques with the help of division algorithm that is enhanced (k,n) sharing. The authorized people only scan the shared QR code and gain private information.In this article, we design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system.**

***Keywords*—Secret Sharing, QR Two-Dimension Matrix, Sharing Approach.**

I. OVERVIEW

EXISTING SYSTEM

Compared with a one-dimensional barcode, the two dimensional (2D) QR barcode can store a larger datapay load and possesses the capability of correcting errors. The barcode data easily can be decoded and retrieved via an automatic barcode system. However, the lack of security of the barcode with private data creates problems for its real-world application.

DISADVANTAGEOFEXISTING SYSTEM

- The sharing scheme also is incapable of preventing cheaters in its real-world application.
- The barcode data easily can be decoded and retrieved via an automatic barcode system.
- Challenge on security.
- Lack of accuracy. It is very burden to Users.
- Lot of paper works.

II. INTRODUCTION

As the development and progress of science and technology, the performance improvement in computer brings many conveniences in life, and many things such as shopping online, bank transfer, ticket ordering, can be resolved in the room easily without going out. However, these tasks have a common goal need to achieve, authentication.

QR code (quick response code):-

It is a type of two dimensional barcode developed by Denso-Wave company in 1994 [1]. QR code is a piece of long multilingual text, a linked URL, an automated SMS message, a business card or just about any information can be submerged into the two-dimensional barcode. The QR code system became popular in the automotive industry due to its high-speed scanning, reliability, greater storage capacity compared to standard UPC barcodes and fast readability. A secret QR sharing approach is to protect the private QR data with a secure and reliable distributed system.

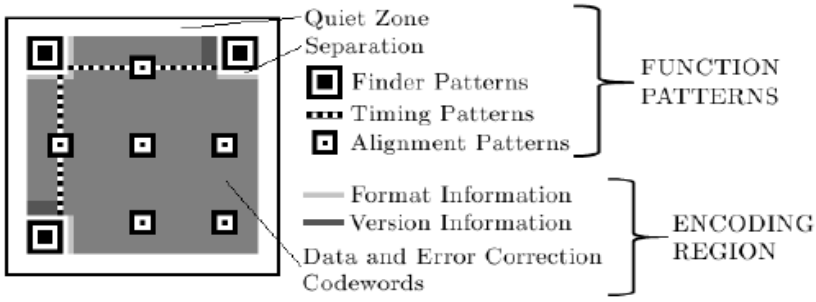


Figure:-QR code structure [3][12]

Characteristics of QR code:-

- **High data capacity:** QR code can store 7,089 numerical values and 4,296 alphanumeric Values, and 1,817 kanji characters.
- **High speed scanning:** A mobile phone with camera function can get the content from a barcode as easy as possible.
- **Small printout size:** QR Codes carry data on both horizontally and vertically, thus QR codes are better than 1D barcodes in data capacity.
- **Advance error correcting:** Even if 50% areas of barcode are damaged, QR codes still can be recognized correctly.
- **Freedom direction scanning:** The scanning direction of QR code is freedom.

A. Novel Sharing Technique Using QR Code:-

In these mobile devices uses barcode tag to read the content directly. There is a risk of security problem in barcode. For this purpose QR code is designed for secret sharing mechanism. Due to this data privacy during data transmission is enhanced. The secret data is further divided into some shadows and they result into embedded barcode tags. They must be equal or greater than the threshold. The main advantage of this technique improves data security for data transmission. Barcode provides a convenient way for people labeling a tag n product.
Barcode is basically of two types: -
1- Dimensional: -1-dimensional puts emphasis on product identification.
2- Dimensional: -.2-dimensional puts emphasis on description.
The main disadvantage of barcode is limited storage in 1-d & 2-D.

B. Security Analysis and Performance:-

This section describes mainly about the security performance of the proposed scheme. This concept is based totally on secret sharing scheme. The secret data is divided mainly into shares of shadows by the technique called secret sharing. The generated shadows are embedded into each QR code tag. If someone wants to direct the content from QR codes that is impossible if the numbers of received shadows is not achieved in the predefined threshold.

As a secret image sharing category, the concept of a visual secret sharing scheme [13] (also called a visual cryptography scheme, i.e., VCS) was first proposed by Naor and Shamir. In a (k, n)-VCS, a secret image is distributed into n shares. Any k shares can obtain the secret by human vision when they are superimposed. However, possession of fewer than k shares meant no information about the secret image could be revealed. Later [19] introduced a special type of VCS, termed the XOR-based VCS (XVCS), in which the recovery process was based on an XOR Boolean operation. With advances in computing devices, this method of recovering information is feasible and reasonable.

III. LITERATURE REVIEW

TECHNIQUES USED FOR SECURITY SCHEME FOR QR CODE

Shweta Sharma et al.[8] investigates different from the conventional QR application, the proposed system can give secure communication and have better efficiency and accuracy nthan others. Here a QR code based cryptography technique which uses 3 layers of security in information sharing isused for better efficiency and accuracy. This QR code-based system is used for secret information sharing. For sharing the data in secure manner author needs QR code of message that is privately encrypted and Encoding of the QR code is done using MATLAB.

Upendra Joshi et al. [6] investigate a new method (n, n)- NVSS . This proposed (n, n) - NVSS scheme will share digital secret image over n - 1 arbitrary natural picture (called natural shares) and one noise - like share. The original pictures will be in the form of photos or hand - painted photos in digital kind or in printed kind. The shares that appear like screeching share may be created to support these natural shares and also the secret image. The unaffected natural shares square measure varied and harmless, thus considerably reducing the transmission risk drawback.

Paper [16] gives a survey of different techniques used for distributed secret sharing approach. Different techniques for encryption and decryption are mentioned, such as encryption of small secret message using TTJSA method which is a combination of 3 distinct cryptography techniques that is(i) Generalized modified vernam cipher method with feedback(ii) NJJSAA technique which is essentially bit level encryption method to encrypt or to decrypt any file. (iii) MSA algorithm which is actually a modified generalized Play fair method which provides several encryptions and several decryptions.

Xiaohe Cao et al.[1] proposed a secure QR code schema based on visual cryptography[14]. Here the QR code is divided into two share images that can be transmitted separately. The pseudo-random matrix generation is used to share two images, that is, the pixels in the two share images are determined by the corresponding values in the pseudo-random matrix. The two share images can be loaded just to restore the information. The system can provide better security for the QR code.

Visual cryptography [1][14][15]scheme is a method to encode a secret image into n noise. In visual encryption, the secret image is divided into several share images by cryptographic operations and distributed to different participants. Decryption is possible by loading a sufficient number of shares. The secret image will be revealed and can be decoded by the human visual system (HVS) [1][15] on the condition of the absence of any complicated computation or replacement algorithms. By taking the implest two-out-of-two visual threshold scheme where each pixel of the image is encoded into a pair of sub-pixels in each of the two shares. If the pixel is white, one of the two columns tabulated under the white pixel shown in figure 2. If the pixel is black, one of the two columns tabulated under the black pixel is selected [1]. In every scenario, the choice is performed by randomly tossing a fair coin, such that each column has equal probability to be chosen. Then, the first two pairs of sub-pixels in the chosen column are allocated to share A and share B, in order.

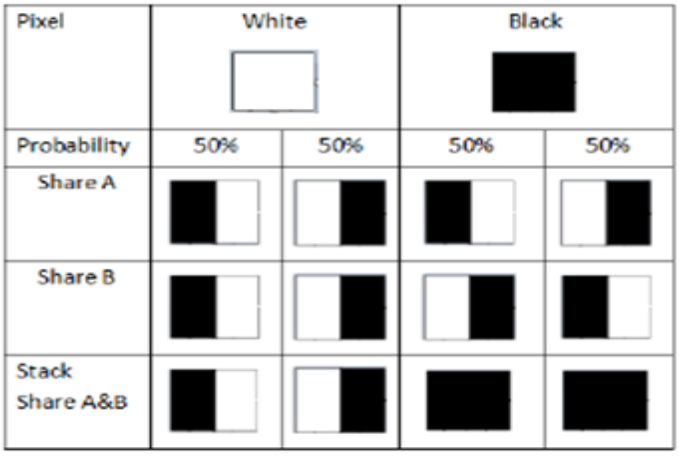


Figure:- The idea of original (2, 2) RG-based VSS [1,2]

IV. PROPOSED SYSTEM ARCHITECTURE.

The system provides more security level as it orders second level of authentication and helps to reduced storage usage by compressing or removing redundant frames without loss of actual content.

A. System Architecture

Now a days QR code is widely used for accessing the information due to its large data capacity, reliability, and high-speed scanning .But with wide application of QR code, the security problem of QR code is again an important issue .The framework is developed to store and share public, private data with each other using splitted QR code techniques. So that authorized person can scan it and get data from QR code.

1. QR Code for Authentication:

We can use QR code for authentication purpose. When user want to login the website then user have to fill some information like username and password and enter into original authorized page, this kind of technique is old so we can use QR scanning techniques for authentication purpose.

In propose system user uses the android app to scan the QR code from the web app. Authentication will be successful and use will be able to share and request for the data.

2. (k, n) method for sharing data:

Based on the enhanced (n, n) method, we are improving (n, n) method in (k, n) method. We provide enhanced security on data using these techniques. Its technique to divide data into two splited part and generate two QR's(one for server side and second for client side).

3. Request for data

When client request for data, one part of QR code is sent on client side but client cannot access original data because it is not the complete data (only one splited part of QR received) and as will as encrypted also. So client have to request for remaining part's(remaining QR).

4. Merge QR code + send Decrypted data

After server receives client request for remaining part of QR, server performs second level of authentication, once the client is verified as a trusted member both QR are merged together and decrypted on server side and original data send to client.

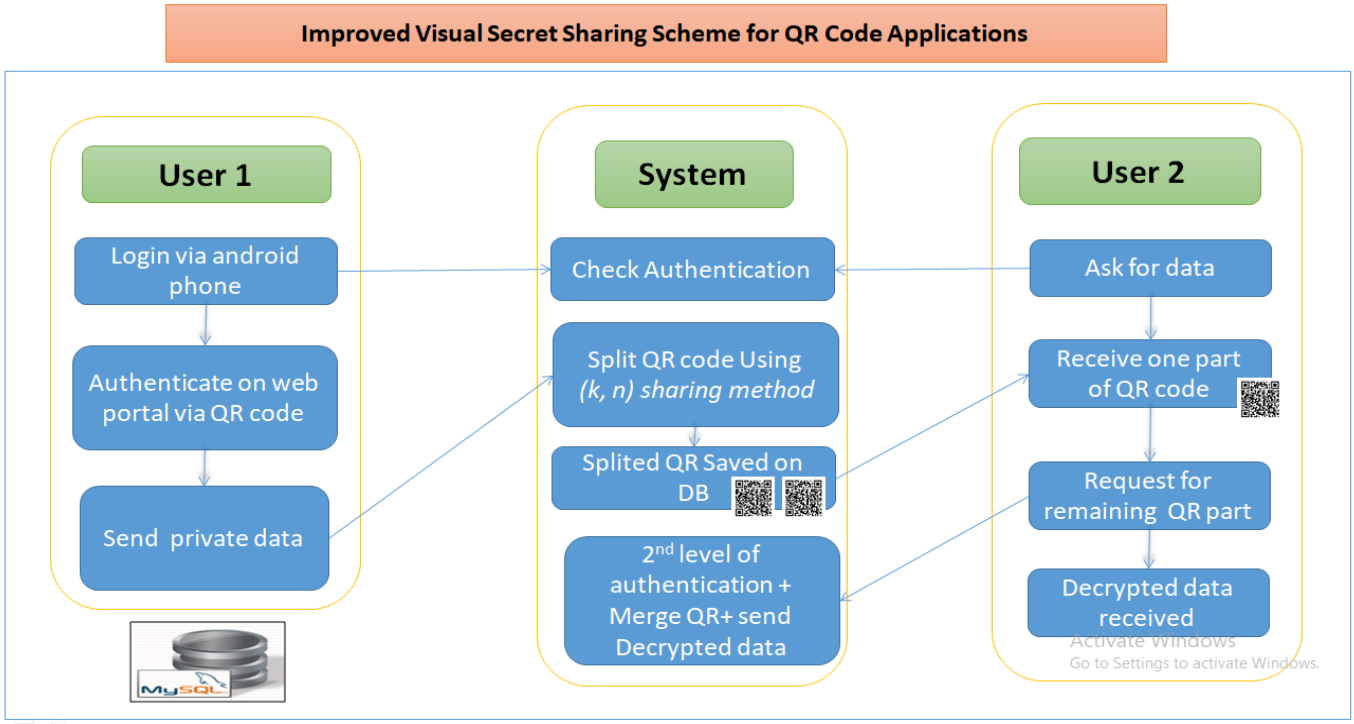
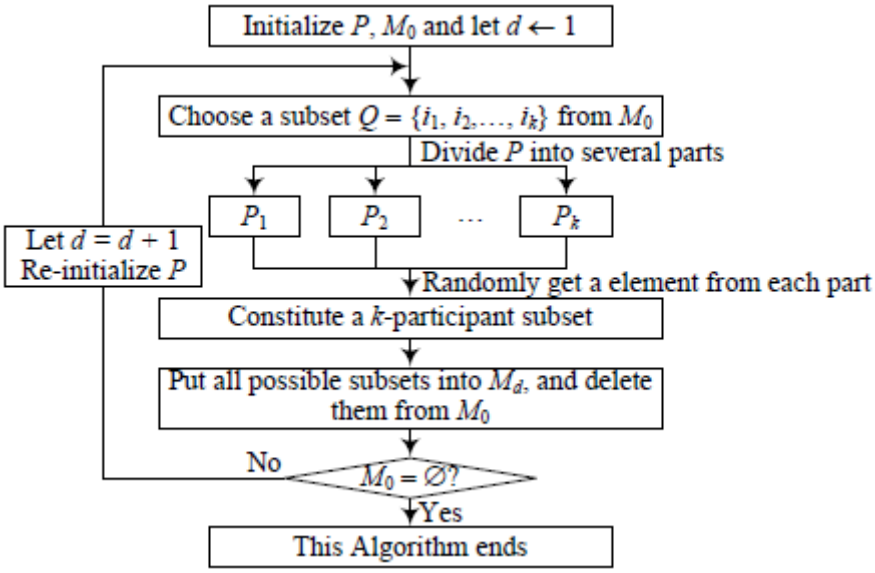


Figure: - System Architecture.

V. ALGORITHM USED:-

1. Enhanced (k, n) sharing method (Division Algorithm):

A (k, n) method can be achieved if we apply the (k, k) instance to every k-participant subset of the (k, n) access structure. However, there will be a huge amount of (k, k) instances, resulting in n! / (k! (n - k)!). The cost increases significantly as n grows. To improve the sharing efficiency, we provide two division algorithms.



Let the string of two subsets { $i_1, i_2, \ldots, i_k$ } and { $j_1, j_2, \ldots, j_k$ }. Suppose that $i_{s+1}, i_{s+2}, \ldots, i_k = j_{s+1}, j_{s+2}, \ldots, j_k$.
If $T_{it} = T_{jt}$ (1 <= t <= k), the (k, k) instances of { $i_1, i_2, \ldots, i_k$ } and { $j_1, j_2, \ldots, j_k$ }are identical. Further, the participant ip (s + 1 <= p <= k) (which is also jp) can store a common share because the shares in two instances are same. This approach reduces the number of shares. In this manner, we divide all k-participant subsets into several collections in which the subsets of each collection use a common instance.

Encryption Algorithm

2) AES Algorithm

Encryption

The following AES steps of encryption for a 128-bit block

follows:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data

(cipher text).

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

1. Sub-Bytes

2. Shift-Rows

3. Mix-Columns

4. Xor-Round Key

b. Decryption

Decryption involves reversing all the steps taken in encryption using inverse functions:

- InvSub-Bytes
- InvShift-Rows
- InvMix-Columns

Operation in decryption is:

1. Perform initial decryption round:

- Xor-Round Key
- InvShift-Rows
- InvSub-Bytes

2. Perform nine full decryption rounds:

- Xor-Round Key
- InvMix-Columns
- InvShift-Rows
- InvSub-Bytes

3. Perform final Xor-Round Key

VI. RESULT AND ANALYSIS

The following metrics used to evaluate the classification performance of accuracy . Accuracy indicates as the sum of correct classifications over the total number of input instances.
The metrics of accuracy is defined as;

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

where TP indicates true positive and TN is true negative. FP indicates False positive and FN is the false negative.

Feature	Algorithms	Time Required (ms)
Generating QR Code	Watermarking	230
	Visual cryptography scheme	140
	Enhanced(k,n) Sharing Method	120
Split QR Code	Watermarking	180
	Visual cryptography scheme	160
	Enhanced(k,n) Sharing Method	145
Merge QR Code	Watermarking	210
	Visual cryptography scheme	170
	Enhanced(k,n) Sharing Method	138

Table 1:Algorithmcomparison with respect to time

The proposed approach makes improvement mainly on two aspects: higher security and more flexible access structures. Two
division approaches are provided, effectively improving the sharing efficiency of (k, n) method. The table 1 and the graph represents the comparative study of the three main algorithms namely watermarking

algorithm, visual cryptography scheme and enhanced (k,n)sharing algorithm which is our approach that is used in the proposed system.

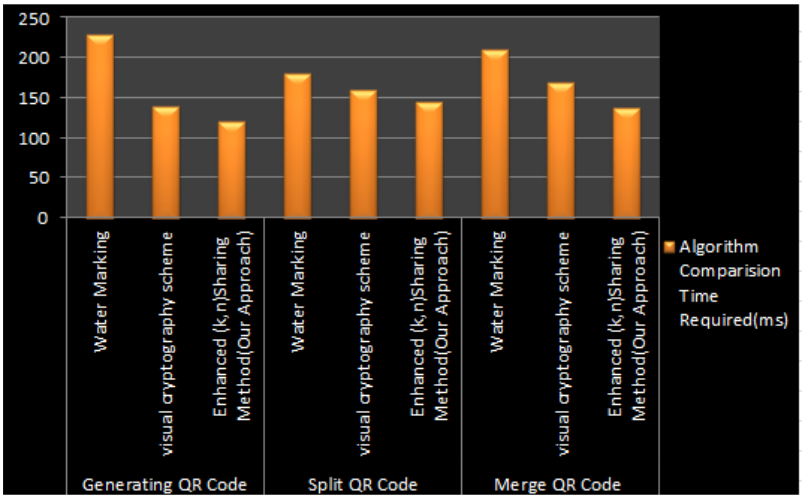


Figure. Algorithm comparison graph with respect to time

The table conclude that the watermarking algorithm takes time of 230 ms for generating QR code and the virtual cryptography schemes takes 140ms and our approach (enhanced(k,n) sharing)takes 120ms which is comparatively less than other two approaches. Similarly Split-QR code and merge QR code takes less time when using enhanced (k,n) sharing method.

Table 2:Algorithm comparison based on accuracy

Feature	Algorithms	Accuracy %
Retrieve QR Code Data	Watermarking	78
	Visual cryptography scheme	86
	Enhanced(k,n) Sharing Method	88

The table 2 elaborate the accuracy of these three algorithms to retrieve the QR code data and hence found that enhanced
(k,n) sharing method provides us with highest accuracy.

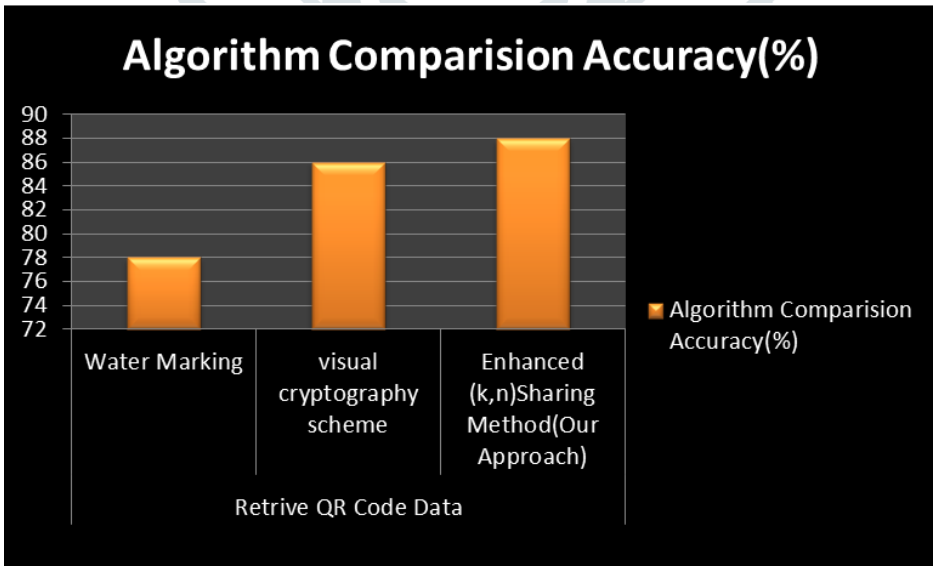


Figure. Algorithm comparison based on accuracy

The table 3 and the corresponding graph that represents the comparative study of the three main algorithms namely DES algorithm, Triple DES and AES algorithm. These three algorithms are used for encryption and decryption purpose for visual secret sharing scheme based on QR code. The table also Elaborate the efficiency of these three algorithms to retrieve the QR code data with respect6 to time (MS).

Table 3:Algorithmcomparison with respect to time(ms)

Sr. No.	Algorithm	Time (ms)
1. Encryption	DES	95
	Triple DES	88
	AES	68
2. Decryption	DES	86
	Triple DES	78
	AES	75

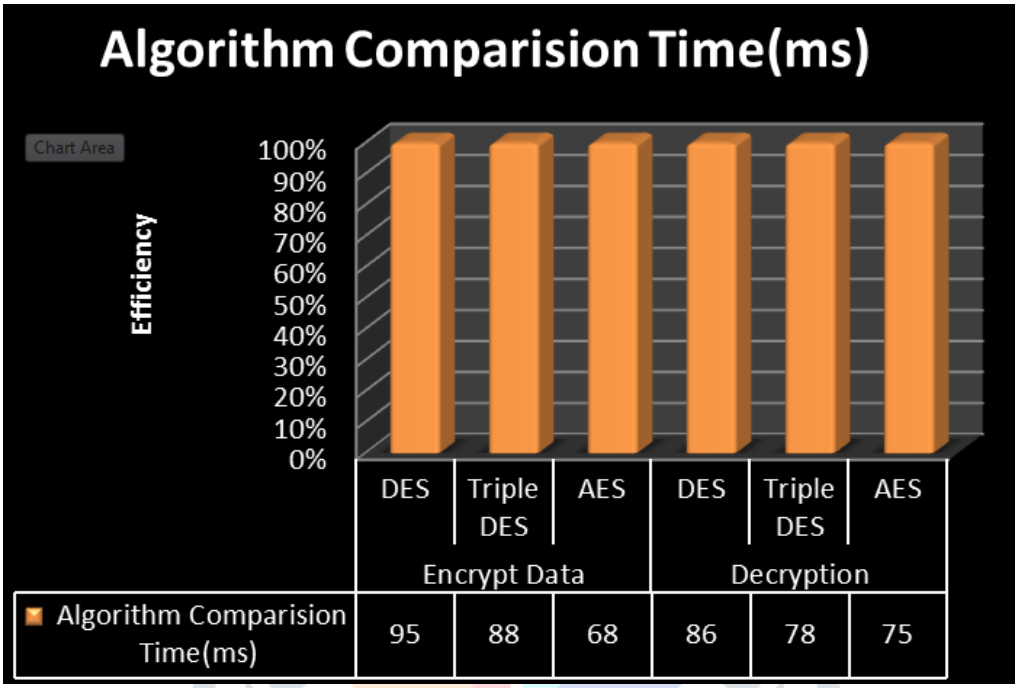


FIGURE. THE ALGORITHM COMPARISON WITH RESPECT TO TIME (MS)

CONCLUSION

As the application of the QR code techniques are increase it is required to increase the security for QR code techniques .The proposed secure QR code application provides more security level as it orders second level of authentication. When clients wants to access the information he uses the android app to scan the QR code from the web app . The none part of QR code is sent on client side and client request for remaining part of QR to the server. After verifying that client is both QR are merged together and decrypted on server side and original data send to client. Provide enhanced security on data using (k, n) method .

References

[1] Xiaohe Cao, Liuping Feng*, Peng Cao and Jianhua Hu "Secure QR Code Scheme Based on Visual Cryptography ",2nd International Conference on Artificial Intelligence and In- dustrial Engineering (AIIE2016

[2] M. Gayathri1*, A. John Blesswin1 and G. Selva Mary2"An Effcient QR-code Au- thentication Protocol using Visual Cryptography for Securing Ubiquitous Multime- diaCommunications",Indian Journal of Science and Technology, Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/102071, October 2016.

[3] Yang-Wai Chow ,ID Willy SusiloD , Joseph Tonien , Elena Vlahu-GjorgievskaandGuomin Yang, "Cooperative Secret Sharing Using QR Codes andSymmetric Keys Symmetry", 2018.

[4] William Puech,ChristopheDestruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard," Two level QR code for private message sharing and document authentication", 2015 IEEE .

[5] SongWan, Yuliang Lu, Xuehu Yan and Lintao Liu "Visual Secret Sharing Scheme With (k, n) Threshold Based on QR Codes",2016 12th International Conference on Mobile Ad-Hoc and Sensor Network.

[6] UpendraJoshi"Enhancing Security by Using Multiple Images and QR Code",2016 IJEDR. 7

[7] Pei-Yu Lin,"Distributed Secret Sharing Approach withCheater Prevention based on QR Code",2015 IEEE.

[8] Shweta Sharma, VikasSejwar,"Impementation of QR code based Secure system for Information Sharing Using MATLAB",2016 8th International Conference on Computational Intelligence and Communication Networks.

[9] NarendraPanwar,Dr. Manmohan Singh Rauthan,Dr. AmitAgarwal,"Privacy of Patient Information",2016 International Conference on Micro-Electronics and Telecommunication Engineering.

[10] Yang-Wai Chow, GuominYang,WillySusilo,"Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing", Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I .

[11] SumitTiwari "An Introduction To QR Code Technology",2016 International Conference on Information Technology.

[12] Jun-Chou Chuang, Yu-Chen Hu,Hsien-JuKo,"A Novel Secret Sharing Technique Using QR Code",May 2014.

[13] Yuqiao Cheng, Zhengxin Fu, Bin Yu"Improved Improved Improved Visual VisualVisualVisual Secret Sharing Secret Sharing Secret Sharing Scheme SchemeScheme for QR Code Application ApplicationApplications",IEEE Transactions on Information Forensics and Security 2018.

[14] M. Naor and A. Shamir, "Visual Cryptography", Adv.Cryptogr., pp. 1-12, 1995.

[15] Chandrasekhara&Jagadisha"SECURE BANKING APPLI CATION USING VISUAL CRYPTOGRAPHY AGAINST FAKE WEBSITE AUTHENTICITY THEFT",(IJACECT - 2013.

[16] Prof. D. H. Patil1, Rutuja Mhaskar1, Aishwarya Shirgurkar1, Priya Surywanshi1, Aniket Panmalkar1," A Survey Paper on Distributed Secret Sharing Approach on QR Code",IJARCCE ,November 2016.

[17] H. C. Huang, F. C. Chang, and W. C. Fang, “Reversible data hiding with histogram-based difference expansion for QR code applications,” IEEE Trans. Consum. Electron., vol. 57, no. 2, pp. 779–787, May 2011.

[18] Longdan Tan, Kesheng Liu, Xuehu Yan, Lintao Liu, Tianqi Lu, Jinrui Chen, Feng Liu, and Yuliang Lu “Robust Visual Secret Sharing Scheme Applying to QR Code”,National University of Defense Technology, Anhui, 230037, China,11 December 2018.

[19] P. Tuyls, H. D. Hollmann, J. H. Lint, et al., “Xor-based visual cryptographyschemes, Designs, Codes and Cryptography, vol. 37, no. 1, pp.169186, 2005