IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Effective Feature Extraction Method in Novel Key Generation Using QR Code to secure the data

Sandha[1*], M. Ganaga Durga[2]

[1]Dept. of Computer Applications, Mannar Thirumalai Naicker College,,Madurai, India
[2] Dept. of Computer Science, Sri Meenakshi Government Arts College for Women, Madurai, India

[*]Corresponding Author: yazhini98@gmail.com, Tel.: +91-96881-17711

Available online at: www.ijcseonline.org

Accepted: 20/Nov/2018, Published: 30/Nov/2018

Abstract— In cloud environment data can be stored and shared between other resources. Any symmetric or asymmetric algorithm is used for secure data in cloud. We need to store the keys in database .The main objective of our work is to improve the protection by encrypting the information with the key generated by QR. It proposes a novel algorithm for generating key using QR image features. It is a reliable and flexible method of key generation for information security. Existing technique for key generation using feature extraction have problem such as high extraction time and high searching time .Existing method need to store more images and stored image may be damaged,. In cloud environment, searching process for authentication causes high network bandwidth, congestion and delay. This paper suggests QR code, a two dimensional code can be used for authentication. Key is extracted from the user unique QR code which is used to achieve the fast retrieval of data from the server. Lost image can be recovered using QR error correction technique. Particularly it is very useful to access mobile applications and there is no need to store more images in server. Additionally extracted key is used as prime factors p and q of the modulus n in RSA for encryption process which tries to secure from mathematical attack. This novel key is applied with asymmetric algorithm.

Keywords— Mobile Cloud computing, Feature Extraction, GLCM , Spectral Cluster Algorithm, QR Code, RSA.

I. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter .Cloud Computing has been defined as the new state of the art technique that is capable of providing a flexible IT infrastructure, such that users need not own the infrastructure supporting these services. This integrates features supporting high scalability and multi tenancy. Moreover, cloud computing minimizes the capital expenditure.

Mobile Cloud Computing is the combination of mobile computing, cloud computing and wireless networks to bring computational resources to mobile users and network operators. The goal of MCC is to enable execution of mobile applications on mobile devices, MCC provides business opportunities for cloud providers as well as mobile network operators. MCC can be defined as a rich mobile computing technology that provides elastic resources of different clouds and network technologies towards mobility, unrestricted functionality and storage. Mobile cloud computing has problem in data integrity and server authentication by sharing data with other users. To secure information across network, Cryptographic system has been widely used. Whether asymmetric system or a symmetric system, its security fully depends upon the strength of the secret key or private key. RSA, DES, and AES etc cryptographic algorithms used to secure the information. Based on their strengths, algorithm suffers due to small key length which is lead to easy hack and guess. All traditional cryptography methods used key is not based on the human relevant data. Hence, there is a possibility of accepting the opt key from the unauthorized member or attacker. Key can be guessed and cracked.

Crypto-Biometrics system resolves the issues faced by traditional cryptography system [1]. Key is extracted from the user biometric information in order to overcome the issues through discrimination, distortion and security approaches. In mobile cloud computing environment Crypto-Biometrics system need to storing possible direction of image in database lead to a storage problem. In order to overcome this problem we proposed the method, generating key from the QR using feature extraction method.

A. QR Code

Authentication is a important process in cloud computing. Data security is very big problem in public storage. In order to prevent this, a proper effective authentication system must be implemented which prevents data leakage or loss a new technique called QR code.

A Quick Response code is a 2 dimensional bar code which was developed by Densa-Wave. Basic of this technology information can be tracked. Two types of QR codes are there namely Static QR code and Dynamic QR code. It can store and digitally present much more data than other barcode. Data is aligned in vertical and horizontal direction. Information is retrieved by photograph of the code using QR code Reader with camera. QR can be read from any position. QR code scanner decodes the image through three squares present in the corner of the image.

B. QR Code Structure

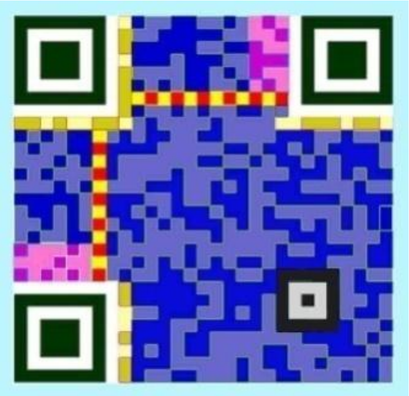

Figure. 1

The three large squares highlighted in green are the Finder pattern. These enable the decoded software and to recognize the QR Code and determine the correct orientation. The smaller brown square is an alignment marker it will be added more if the code size increased. Separators are used to separate Finder pattern from the actual data. Timing pattern contain alternate red & yellow module. Format information is 15 bit data next to separators it contains about error correction level. Pink color squares are used to encode the version data. Blue color Data part is in 8 bit size.

C. Types

The 4 different types of QR codes differ in the view and features. QR code model 1 and model 2 are the first type of QR code. Up to 1167 numerals can be stored in largest version of model 1 and Up to 7089 numerals can be stored in largest version of model 2. The next type is micro QR code. It differs from regular QR model by position detection pattern and size. iQR Code is next type. The same size of IQR Code as an existing QR Code can hold 80% more information than the latter. SQR Code is used to store private information there is no difference from regular code in appearance. The next type is logo QR it incorporate high level of design features.

II. Related Work

Recently, much of growing interest has been pursued in the context of remotely stored data security David Pintor Maestre et al.[2] consider secure authentication using QR code in their defined “A Improved secure authentication method using QR codes” develop an authentication method using 2 factor authentication.. In their scheme, they utilize IMEI number of smart phone with random number of QR code for secure authentication, thus private data security is achieved. The problem here is the server must have a copy of the user's private key in order to generate the same pincode.

Thiyagarajan M, Dinesh Kumar K et al.[3] consider authentication of consumer product can be done with QR codes . They achieve the security by QR code along with the public key encryption algorithm. But the normal QR code can be easily retrieved using any smart phone. They do not consider security of QR code. Suraj kumar sahu et al. [4] describe a “Encryption in QR code using stegnograpy” where cover image and QR data is embed and encrypted. Dong-sik oh et al. [5] consider creating 3 set of QR code by converting the single information into 3 versions of QR code and stored in distributed server system.Gaurang Panchal and Debasis Samanta[6]consider SVM based ranking mechanism is used for the user verification where the storage of neither templates nor keys is required. Yao-Jen Chang [1]proposed feature generation and a stable key generation mechanism using biometric data. Tawfiq S. Barhoom [7] encrypting the data using a secret key extracted from color image which is generated by the difference in the LSB of the image pixels.

Mohammed Tajuddin [8] proposed human biometric used as key from retinal blood vessels which is not stored in the database. This mode of operations increase the network security . P Selvarani andMalarvizhi [9]Derived key from fingerprint and Iris with the help of HGAPSO,LBP algorithm and Cross over Mutation technique. Sonal Sharma [10]describe SRNN algorithm is also a public key cryptography algorithm. Here extremely large number is used as two prime factors like RSA and two short range natural numbers additionally used as pair of key due to improve the security of the cryptosystem .Many researchers have analyzed and made contribution related to feature extraction method [15, 16].

III. METHODOLOGY

The user information converted in to QR and key is generated from unique QR image using feature extraction method. Spectral cluster algorithm extract the feature from the unique QR image which is effective than the GLCM feature extraction method by time taken for feature extraction. Here affinity matrix computed from the image and after perform the singular value decomposition result will clustered.

1. FEATURE EXTRACTION

1.1 Existing feature extraction method

Gray Level Co-Occurrence Matrix (GLCM) with QR image

A gray level co-occurrence matrix (GLCM) contains information about the positions of pixels having similar gray level values.Count all pairs of pixels in which the first pixel has a value i, and its matching pair displaced from the first pixel by d has a value of j. This count is entered in the ith row and jth column of the matrix Pd[i,j]. Pd[i,j] is not symmetric, since the number of pairs of pixels having gray levels [i,j] does not necessarily equal the number of pixel pairs having gray levels [j,i].

A gray level co-occurrence matrix (GLCM) contains information about the positions of pixels having similar gray level values. A co-occurrence matrix is a two-dimensional array, P, in which both the rows and the columns represent a set of possible image values. A GLCM Pd[i,j] is defined by first specifying a displacement vector d=(dx,dy) and counting all pairs of pixels separated by d having gray levels i and j. The GLCM is defined by where nij is the number of occurrences of the pixel values (i,j) lying at distance d in the image. The co-occurrence matrix Pd has dimension n× n, where n is the number of gray levels in the image. From the co-occurrence matrix obtained, we have to extract the 12 different statistical features.

1.2. Feature Extraction based Spectral Clustering with QR

QR_{image} is taken as the input data .Perform affinity matrix which discovered co-occurrence relationships among activities performed by pixels

Σ^2 is variance m & n *are the no.* of rows and columns of the image

Perform Singular Value Decomposition of the affinity matrix, Estimate the unitary matrix,U=AA*.

A* Conjugate transpose of the affinity matrix unitary matrix which is obtained from the svd process and calculated the normalized matrix and construct the clustered matrix, Group the region of the image based threshold and obtained values of the clustered result,

$$Image = QR_{image}$$

$$A_{ij} = \frac{\exp(-\sqrt{\sum_{k=1}^{m}(Image_{ik} - Image_{jk})^2})}{2\sigma^2}$$

$$A_{ij} = \frac{A_{ij}}{\sum_{i=1}^{m}\sum_{j=1}^{n}A_{ij}}$$

$$A - is\ the\ affinity\ matrix.$$

$$\sigma^2 - variance$$

$$m\ \&\ n\ are\ the\ number\ of\ rows\ and\ columns\ of\ the\ image$$

U=AA^* // m x m unitary matrix

$$A^*Conjugate\ transpose\ of\ the\ affinity\ matrix$$

$$X = \frac{U}{\sqrt{\sum U^2}}$$

$$Cluster_{mat} = XX^T$$

$$Cluster_{fea} = \left\{i \quad if\ Cluster_{mat_{ij}} \geq 0.9\right\}$$

$$\forall\ i = 1,2,..,m.\ \ j = 1,2,\dots,n$$

1.3. Comparison between SCQR and GLCM QR

Comparison made both SCQR and GLCM QR feature extraction method based on complexity and time by giving input as our QR image .

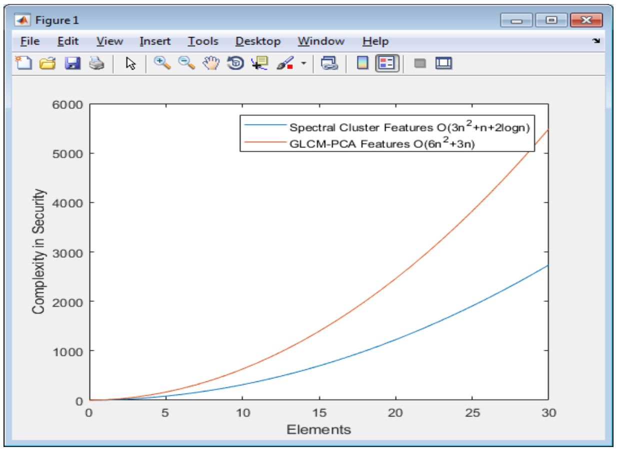

Chart -1

GLCM method have more complexity than SC –algorithm. GLCM feature extraction algorithm. contain more looping statement than Spectral cluster feature extraction algorithm . complexity of Spectral cluster algorithm is O(3n²+n+2logn) and complexity of GLCM is O(6n²+3n)

Table -1

SIZE	GLCM	SC
Byte	1.969	1.232
Word	2.076	1.874
Sentence	2.876	2.321
Paragraph	3.786	3.110
File	5.619	4.112

But time taken for feature extraction from QR By Spectral cluster algorithm is less than the A gray level co-occurrence matrix algorithm. Time is calculated based on size of data from byte to file. Extraction time measured in seconds.

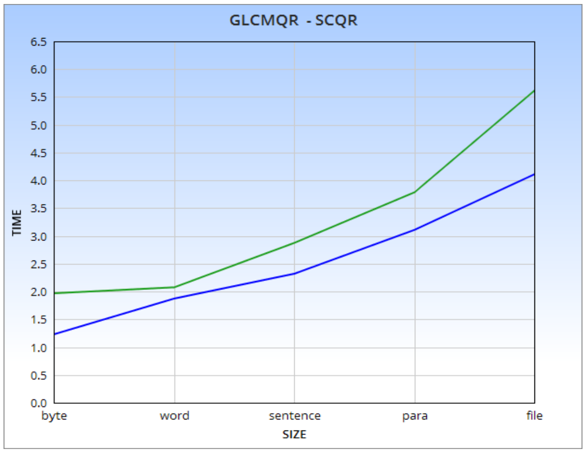

Chart -2

Blue color in the graph indicate time taken by our proposed Feature extraction method Spectral cluster algorithm. Green Color indicate the time taken for feature extraction in different size of data by GLCM algorithm.

2. APPLIED IN RSA CRYPTO SYSTEM

When RSA is implemented, Figuring out the prime factors p and q of the modulus n from RSA known as a mathematical attack. Obviously, knowing p ,q and totient φ(n) of the modulus n will lead attacker will decrypted easily. set up the equation (p−1)(q−1) = φ(n), that, along with the equation p × q = n, will permit the attacker to determine the values for p and q. In order to solve such a problem, the proposed method constructs a new method to change the value of n by constructing p and q from extracted feature which the users can create their own QR used for changing the value of n and to ensure more security.

RSA Key generation Algorithm

Input: Extracted Features $Cluster_{fea}$

Output: Generated Key key

Procedure:

```
$Cluster_{fea}$,
    Len=length ($Cluster_{fea}$)
    For i=1:Len
        If rem ($Cluster_{fea}(i), any_{no}$)~=0
        $Prime_{no} = Cluster_{fea}(i)$
        $uni_{prime} = unique(Prime_{no})$
        $Max_{prime} = \max(uni_{prime})$
        p=$Max_{prime}(1)$
        q=$Max_{prime}(1$
        $n = p * q$
        $\varphi(n) = (p-1)(q-1)$
        $No_2 = median(Cluster_{fea} < \varphi)$
        $No_3 = max(Cluster_{fea} < \varphi \&\& Cluster_{fea} > No_2)$
        $Public_{key} = \{1 < e < \varphi \quad \&\& \gcd(e,\varphi) = 1 \& \gcd(e, No_3) = 1\}$
        $Private_{key} = \{1 < e < \varphi \& \& mod(e * d, \varphi) = 1$
```

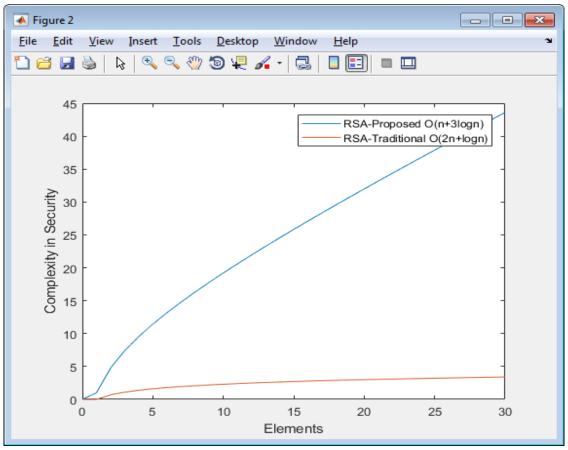

Chart-3

find the prime numbers from the clustered result, $Cluster_{fea}$, Remainder of any number is not equal to '0' then that number is the prime number Calculate non-repeated values of the primes and maximum values, Select two very large obtained prime integers as p and q. Calculate modulus for both the public and private keys, Estimate Euler Totient Function, Select an integer from the clustered result which satisfies the following condition $No_2 = \text{median}(Cluster_{fea} < \varphi)$ Select next integer which also satisfied the condition, selection of public key 'e' which satisfies the criteria.

2.1. PROCESS FLOW

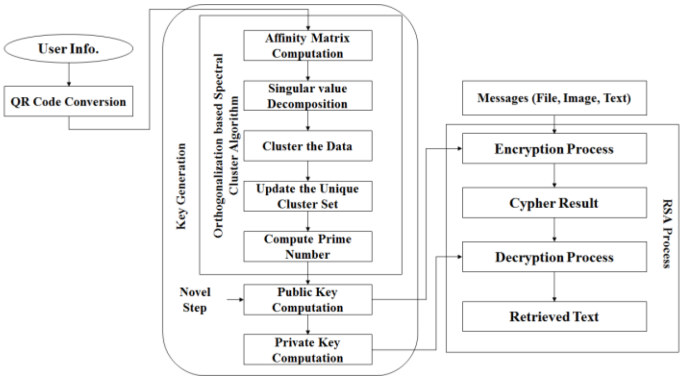

Figure- 2

In order to overcome the problem of directly store the data in database storage and time of searching bit ratio , user unique info converted as a QR. Extracted feature from the Biometric image used as key, but the problem is need to store large number of possibility image .it will be a problem if damage or corruption in image. Error correction level technique in QR can overcome this problem. GLCM algorithm used for feature extraction to create a key for encryption .but time taken for extraction is higher than spectral cluster algorithm.

Fix the p and q value from the output of spectral cluster algorithm to avoid the leakage of p and q. RSA encryption takes place and encrypted data stored in to cloud and decrypted.

IV. Conclusion and Future Scope

We thus conclude this proposed system saying that it will be a best data security model can be implemented in cloud environment to avoid the cloud storage problem. Future enhancement of this work is to find the new algorithm using our proposed key.

References

[1] Yao-Jen Chang,Wende Zhang, and Tsuhan Chen "Biometrics-based cryptographic key generation" .In the Proceedings of the 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763)

[2] David PintorMaestre "QRP: An improved secure authentication method using QR codes" UniversitatOberta de Catalunya 08018, Barcelona, Spaindpintor@uoc. edu June 8, 2012.

[3] Thiyagarajan M, Dinesh Kumar K"Qr code authentication for product using cloud computing"Journal Of Global Research InComputer Science,Volume 3, No. 2, February 2012

[4] Suraj Kumar Sahu: " Encryption in QR Code Using Stegnography"International Journal of Engineering Research and Applications,Vol. 3, Issue 4, Jul-Aug 2013, pp.1738-1741

[5] Dong sik-oh, Bong han-kim and Jae- Kwang Lee : "A Study on Authentication System using QR code for Mobile cloud computing Environment".Springer,Hennam University Daejeon,Korea "Future Information Technology" pp500-507

[6] GaurangPanchal a , DebasisSamanta a , "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security" Elsevier "Computer and electrical engineering "Volume 69, July 2018, Pages 461-4782018

[7] Tawfiq S. Barhoom,Zakaria M. Abusilmiyeh"A Novel Cryptography Method Based on Image for KeyGeneration" Palestinian International Conference on Information and Communication Technology 2013 pages 71-76

[8] Mohammed Tajuddin C. Nandini "Cryptographic Key Generation using Retina Biometric Parameter" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013

[9] P Selvarani , N Malarvizhi"Secure data in cloud with multimodal key generation" International Journal of Engineering &Technology, Volume 7 (1.7) 2018 Special Issue 7

[10] SonalSharma"Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" ijarcsse Volume 2, Issue 8, August 2012 ISSN: 2277 128X

[11] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, SebastianSchrittwieser, MayankSinha, EdgarWeippl: "QR-Code Security". SBA Research, 2010

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song. "Remote data checking using provable data possession".ACM Trans. Info.& System Security , May 2011.

[13] C. Wang, Q. Wang, K. Ren and W. Lou, &ldquo,"Privacy-Preserving Public Auditing for Storage Security in Cloud Computing"rdquo, Proc. IEEE INFOCOM ',10, Mar. 2010.

[14] Sandha, M.GanagaDurga, " Study on Data Security Mechanism in Cloud Computing" 2014 ,IEEE digital Library

[15] E. Mary Shyla , M.Punithavalli "Hybrid Facial Color Component Feature Identification Using Bayesian Classifier" International Journal of Scientific Research in Computer Science and Engineering Vol-1, Issue-3 E-ISSN: 2320-7639

[16] A. Shakin Banu^1 , P.Vasuki ^{2} , S. Mohamed Mansoor Roomi^3 , A. Yusuf Khan^{4,}" SAR Image Classification by Wavelet Transform and Euclidean Distance with Shanon Index Measurement" International Journal of Scientific Research in Network Security and Communication (ISSN: 2321-3256) Vol.6 , Issue.3 , pp.13-17, Jun-2018

Authors Profile

Mrs Sandha completed Master of Computer Applications from Anna University in the year 2009. She is currently pursuing her Ph.D. and is currently working as Assistant Professor in the Department of Computer Applications , Maanar Thirumalai Naicker College since 2018. She has published 3 research papers in reputed international journals including Scopus & UGC and conferences including IEEE and they are available online. Her main research work focused Cloud Security and Privacy, Information Security. She has 5 years of teaching experience.

Mrs Dr.M.Ganaga Durga pursued Bachelor degree from Thassim Beevi Abdul Kader College for Women and Master degree from Gobi Arts and Science College, Tamilnadu, India. She completed her Ph.D. from Mother Teresa Women's University and is currently working as Assistant Professor in Sri Meenakshi Government Arts College for Women, Tamilnadu. She has published more than 23 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and are available online. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy. She has 23 years of teaching experience and 8 years of Research Experience.