Secured Document Generation and Authentication mechanism using VSS and QR code

Deepen Saha[1], Shubham Sonar[2], Praful Telore[3], Lalit Jadhav[4]

Students, Dept. of Information Technology, MET'S BKC IOE Nasik, Maharashtra, India[1, 2, 3, 4]

---***---

Abstract –

In this paper, a secured document generation and authentication system is proposed using Visual Secret Sharing (VSS) scheme and Quick response (QR) code. Using this system, Identity document generation and authentication made easy and hassle free with powerful encryption mechanism of VSS and ease of QR codes. In this proposed system, a binary image is split into 2 different parts using VSS and encoded into 2 different QR codes called share 1 and share 2. The first code (share 1) is printed on identity document whereas second code (Share 2) is kept in the database. Whenever IdDocument authentication is required, using QR code scanner (camera phone) scans share 1 from the document whereas share 2 is extracted from database and combining result of both shares authenticates particular user.

***Key Words*: IdDocument, VSS, QR code, Aadhar**

1. INTRODUCTION

Nowadays technological development of world is growing faster day by day. It helps the easier way to solve complex problems but over its advantages, it comes with disadvantages too.

Technology can allow doing illegal activities easier thus use of technology cannot be controlled, it can be used in many areas by people who intend to do illegal activities.

Currently there are few methods to recognize someone's identity and originality, like IdDocument like passports Aadhar card, voter's cards are best methods to verify that what he is saying or claiming is true.

1.1 Literature Survey:

But as discussed above, using many methods with help of technology, documents are also being forged i.e. Duplicate or fake documents are generated which are not easily detectable.

To solve this problem in technological and efficient way, several mechanisms have been developed [1]. Authentication using password mechanisms exist but it can be easily cracked using dictionary attacks and brute forcing [2] & [3]. For e.g. Aadhar card.

Aadhar card is scheme of The Unique Identification Authority of India (UIDAI) is an attached office of the Planning Commission of India, established to issue a Unique Identification Number ("Aadhar") to residents of India who desire to have it .In Aadhar card generation process requires biometric and demographic data of issuer and store them into centralized database and issue a 12 digit unique number. But in recent cases, aadhar cards are also being forged and fake aadhar cards was also made.

Case-1) Fake Aadhar Card made in Kanpur:
In the June month of the year 2014, a raid was organized by the police who caught four people in Akbarpur area of Kanpur district while in the March month of the same year; many Aadhar card project officers were caught on a hidden camera in a Cobra-post sting operation.

Case-2) For the citizens of other countries such as Bangladesh and Nepal. Couple of officers was caught when they offered to forge the documents to the citizens of Nepal and Bangladesh who were not having the proof of Indian Residence to make the Aadhar card.in addition to this, fake proofs of identity and residence were provided at a cost of Rs.250 to Rs. 5000.and the Aadhar card was issued to them without any biometric records. This means that the crucial part of scanning the finger print and retina of the person were not done.

Case-3) Documents submitted at Delhi high court revealed that the Delhi's Regional Passport Office (RPO) issued five passports in 2015 on non-existence addresses in Delhi. In fact these passport applicants were not even Indian nationals.

These are just a few cases but in real, there were many bigger rackets that include such an act of faking the Aadhar card in the country to those who are not the residents.

2. PROPOSED SYSTEM

In the Secured Document Generation and Authentication mechanism, we are using VSS and QR code combined for providing better secrecy and faster encryption decryption process. The various components and functionalities of the proposed system are explained below.

2.1 Visual secret sharing (VSS) scheme

VSS is powerful cryptographic method proposed by Naor and Shamir [3]. Visual Secret Sharing is a visual encryption algorithm that encrypts and splits an image that has visually intelligible data into two or more images that are visually unintelligible called shares. In order to retrieve the original image, each and every generated share is brought together and decrypted.

Following is the way the images can be visually encrypted into two shares. Logically we can represent 1 as 1 + 0 in logical Mathematics. In a similar way we can represent 1 and 0 in following possible forms.

$$1 = 1 + 0$$
$$1 = 0 + 1$$
$$1 = 1 + 1$$
$$0 = 0 + 0$$

Considering 1 to be a black pixel and 0 to be a white pixel in an image on left hand side of the above representations. Then the representation on the right hand side represents the two generated shares that can be passed through 'OR' operation in order to generate the actual image.

Even more mathematical manipulations can be used to generate more than two shares and exploit the various possibilities of different color pixels.

2.2 Quick Response (QR) code

QR code system was invented in 1994 by Denso Wave. QR codes are two-dimensional bar codes that contain any alphanumeric text such as plain text, phone numbers, email addresses and often feature URLs that direct users to sites where they can learn about an object or place (redirecting) [4].Basically QR codes became popular in Japan automotive industry but because of its fast readability and efficient storage capacity it requires less time to expand its usage in worldwide. One of the Main purpose of using QR codes is for consumer advertising. Fig-1 shows the structure of QR code. Table 1 shows the storage capacity of QR code for different encoding format.

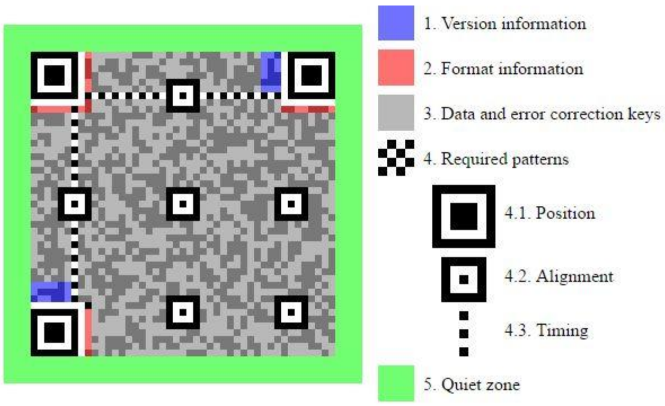

Fig -1: Structure of QR code

Maximum character storage capacity (40-L)			
Input mode	Max.charecters	Bits/character	Possible char.,default encoding
Numeric only	7089	3⅓	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Alphanumeric	4296	5½	0–9, A–Z (upper-case only), space, $, %, *, +, -, ., /, :
Binary/byte	2953	8	ISO 8859-1
Kanji/kana	1817	13	Shift JIS X 0208

Table -1: Max. Character Storage capacity of QR code

2.3 Workflow of System

In the proposed system, total task of generation and verification is divided in 3 main modules i.e. Request, Generation and verification.

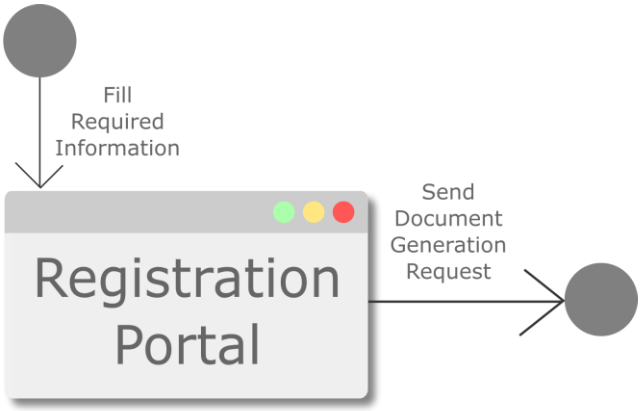

Fig -2: Registration Process

2.3.1 Request

Fig-2 explains about the request module. In this module, the issuer who request to issue the ID Document initially fills up all necessary details such as personal information and submits documents that required to issue particular ID Document.

After this, the individual must select which type of document he wants to issue like passport, aadhar, ATM card etc. Then after submission of the request the individual will get notification about same.

The issuer must have hard copy of required documents which is uploaded to user portal. The status of the document can be checked using the appropriate page provided.

2.3.2 Document Generation

Very crucial part of the system is Document generation and admin dashboard module in which issuer's data and information i.e. basic information and documents uploaded by individual are verified manually by admin.
User's/issuer's requests are handled by admin. The document request goes through a predefined hierarchy which leads to thorough verification of the document request as shown in Fig-3 below.

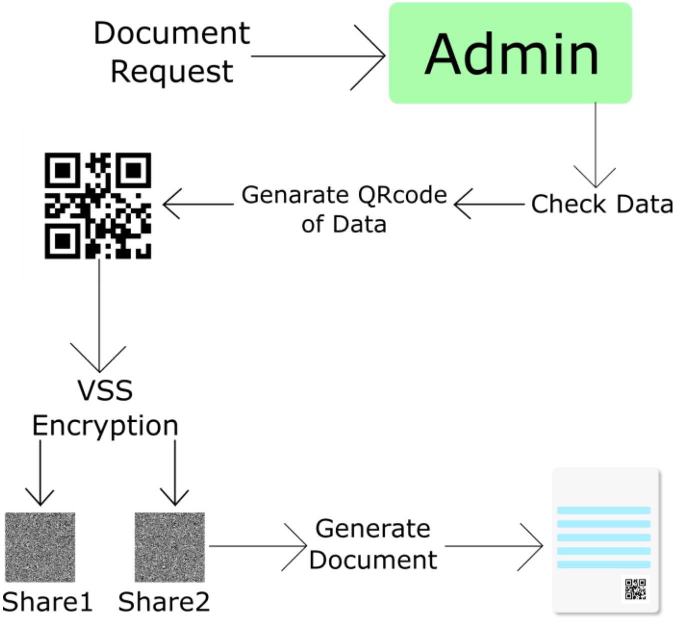

Fig -3: Document Generation Process

After verification through hierarchy of process, admin finally signs the document request with its key, so that it can be processed further. The document request heads towards the document generation mechanism which uses VSS and QR code. In VSS encryption process, unique QR code is generated for respected request and that QR code is split in to two shares with random noise or can be called as unintelligible data. Share 1 and 2 are stored on different secure file servers and an encrypted QR code is generated with specific location of two shares. The QR code provided on the document can only be scanned with special scanners designed for verification process.

2.3.3 Document Verification

In the verification process, verifier is the authority, who is responsible for verification of document example of such is, security check at airport for passport verification. Verifier will scan the QR code which comes with ID Document provided by issuer. In scanning process, verifier must login on the scanner application, which when used for scanning uses the Encrypted QR code data with server to authorize and then authenticate the data.

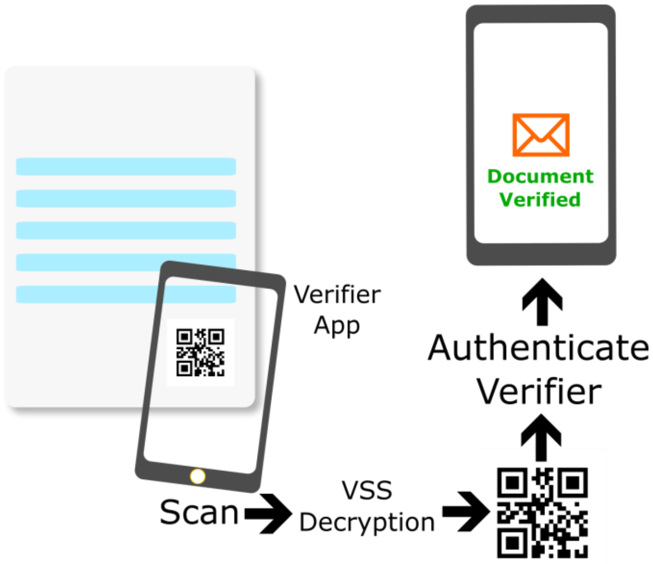

Fig -4: Document Verification Process

In addition to this, Verifier must be logged in into the system to access the Encrypted data in QR code. After above mentioned steps fulfilled then only verifier will have access to the server and the decryption mechanism would be initiated. After decryption verifier will able to see the essential details of individual. The system works on two step verification. First one is done on the server side with no verifier interruption and second one is done manually to verify the details. The diagrammatic representation of the module is shown in Fig-4 above.

3. SYSTEM ANALYSIS

The proposed system is distributed in nature and follows hierarchical approach. Due to its distributed nature and hierarchical approach the generation of documents is efficient and reduces the work load on individual in the document generation office. The proposed system also helps to overcome the bribe system and avoids falsification of documents to a great extent. Further, the documents can be generated in timely manner and long queues can be avoided with less usage of paper.

4. CONCLUSION

Thus, we can conclude that if we consider areas affected by forging documents it may cause problems in future. Hence, the proposed system is a new methodology to generate highly secure ID Documents. The proposed system can be used to identify and validate documents to avoid forgery of documents and increase the efficiency of the document generation process. It can be used in many sectors such as scholarships, job recruitment etc. Hence this mechanism can only be used for verifying the authenticity of the identity document; further this mechanism could be improved for verifying different documents and for extending the scope of the system to different sectors.

ACKNOWLEDGEMENT

We thank Ranjana Dahake, Professor from Mumbai Educational Trust Bhujbal Knowledge City IOE, IT Department who provided insight and expertise that greatly assisted the research.

We thank our staff from IT department for comments that greatly improved the manuscript. We would also like to thank our classmates and seniors for their valuable inputs.

REFERENCES

[1] Espejel-Trujillo A., Castillo-Camacho I., Nakano-Miyatake M., “Identity document authentication based on vss and QR codes ,” Procedia Technology 3 (2012) 241 – 250.

[2] M. Kim, C. Koc, A simple attack on a recently introduced hash-based strong-password authentication scheme. International Journal of Network Security, 2005, 1(2):77–80.

[3] J. Shen, C. Lin, H. Yang, Cryptanalysis of a new efficient make up for wireless communications. International Journal of Network Security 2005, 1(2): 118–121.

[4] 7 things you should know about QR Codes
http://www.educause.edu/eli

[5] QR code Tutorial
http://www.thonky.com/qr-code-tutorial/

[6] BruiceSchneier, “Applied Cryptography- Protocols, Algorithms and Source code in C”, 2nd Edition, Wiely India Pvt Ltd, ISBN 978-81-265-1368-0.

BIOGRAPHIES

Deepen C. Saha

Student, MET Bhujbal Knowledge City IOE, Full stack developer and freelancer.

Shubham D. Sonar

Student, MET Bhujbal Knowledge City IOE, Python enthusiast and freelancer.

Lalit Jadhav

Student, MET Bhujbal Knowledge City IOE, Web Developer and freelancer.

Praful D. Telore

Student, MET Bhujbal Knowledge City IOE, Web Developer.