Private data sharing and document authentication using two level QR code

[1]P.Vasantha,[2]M.Sangeetha,[3]P.Rajeswari [4]Mr.P.Gopikannan

[1][2][3] UG Student , [4] Assistant Professor(CSE)

[1][2][3][4]P.S.R.Rengasamy College of Engineering for women, Sivakasi

Email: [1]malik0095150@gmail.com, [2] sangeethamalia20@gmail.com, [3]rajiparamasivan@gmail.com

Abstract:

The quick response (QR) code was designed for storage information and high speeds reading application . In this paper we present a new rich QR code that has two storage levels and used for document authentication. The two level QR code which means private level and public level . The public level is same as the standard QR code storage level and it is readable by any classical QR code applications . The private level allow us not only to increase the storage capacity of the QR code but also distinguish the original document from a copy. The experimental results show a perfect restoration of private information . It also highlights the possibility of using this new rich QR code for document authentication..

Keywords: QR code,two storage levels,private message,document authentication,pattern recognition,print_and_scan process.

I. INTRODUCTION

Quick response codes or QR codes are basically a flat of bar codes which are used day by day due to the technological advancements [1]. These codes have various applications. To name a few, these QR codes can be used for storing data (advertising, museum art description), web site redirecting, tracking and tracing (for transportation tickets or brands), Entity identification (passenger information, supermarket products), Uniform resource locator, Code payments, Virtual stores, Web login, Message sharing and document authentication. QR code is also known as matrix barcodes. QR code was invented by Denso Wave in Japan while working at automotive industry. Due to the technological advancements there are various QR codes which

are being used in the market. As a result of which the demand for QR codes scanner has also increased proportionally. The popularity of QR code is due to its robustness, easy to read features, higher encoding capacity and small size.

Although it has many pros but still has many downsides to be improved upon most common cons are: It is easily accessible to everyone even if it is ciphered and it is very difficult to distinguish between the originally generated the QR codes with its photocopy. So, in order to intrude the QR code, any third person can retrieve the information with the help of two level QR code scanner.Message sharing and document authentication are concerned the security of the QR code is our largest priority. In order to overwhelm these shortcomings we have proposed a two level QR code with enhanced encoding techniques. This enhancement is achieved by using textures patterns instead of black modules. These patterns are sensitive to the distortions produced by printing and scanning process.

Our proposed technique also lays emphasis on storage capacity apart from more security and privacy. Our proposed system contains public level QR code and a private level QR codes. The public level QR code can be accesses with the help of any standard QR code scanner but the public level QR code cannot be accessed from any standard QR scanner. Hence it gives a level of security against any possible intrusion to greater expanse. The first level keeps the strong characteristics of the QR code but the second level improves the storage capacity of the QR code. This project is as follows: we start with the overall of QR codes and in the subsequent divisions we will be mainly exploring the state of the art existing techniques along with the proposed technique. At the result of this paper we will compare our technique with the existing
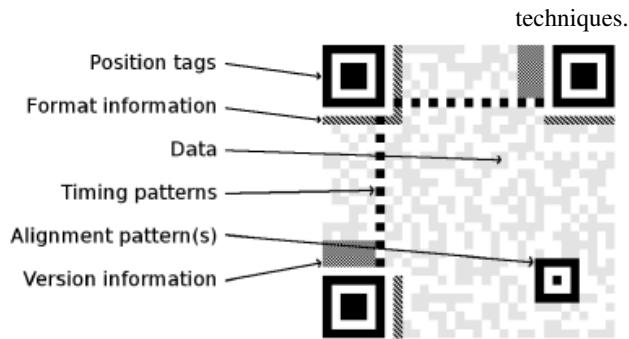
techniques.

Fig.1.QR Code.

II. VARIOUS APPROACHES FOR PRIVATE MESSAGE SHARING USING QR CODE:

A. CONTEXTUAL QR CODE:

Contextual QR code is one of the most famous QR code used now a days. Contextual QR code mainly used for attributes or contexts while designing QR code. It is basically a section of static QR code which is related to a particular context while designing a QR codes. Contextual QR code can be created by providing various contexts or parameters as input such as time, location, and IP address and device type for personalizing the output message by adding the name of the user or by changing the language and transfer user data and contexts along with the parameters to the server database. Contextual QR code is created by taking user attributes into consideration. Contextual QR code is mainly used for exchanging the ubiquitous computing into consideration. Context aware QR code is capable enough used to filter information so that the relevant information under the right time at the right place is extracted. QR codes are mainly used for context aware navigation. QR code also acts as a location source in which the physical location of the QR code is encrypted inside a uniform resource locator. Context based QR code can also consider proximity overcome the location. Proximity under QR codes can be very useful if the location of the user is very hard to find. As far as private message sharing and document authentication is concerned contextual QR codes keeps a record of the different user attributes. Very often, this change is related to private message. For example, a privacy-aware proximity detection service determines if two mobile users are near to each other without requiring them to disclose their exact place. Contextual QR can be used to collect database so it is known as Wi-Fi ―fingerprints‖. Each fingerprint stores the explanation of the location and it also contains the MAC addresses and the received signal strengths (RSSI) of nearby access points. This information could be

used for Wi-Fi based positioning and historical records for fingerprints let us discover user's behavioural pattern.

B. Code Steganography

Steganography is basically the process of hiding data into secret information. The QR code steganography hide the data or secret message into the QR code. The message to be hidden is termed as the secret message is used after encrypting it with the help of error correcting bits. This error correction capacity of the QR code is used to perform the steganography of the QR code. The secret message in the QR code does not disturb the reading process of the QR codes. The error capacity of the QR code Steganography is very poor. In Steganography QR code, the most secret message length is equal to 1215 Bytes for QR code version 40. We can also embed an disappeared watermark in the QR code which acts as the secret message. For such embedded disappeared watermarks, discrete cosine transformation and discrete wavelet transformation are used.
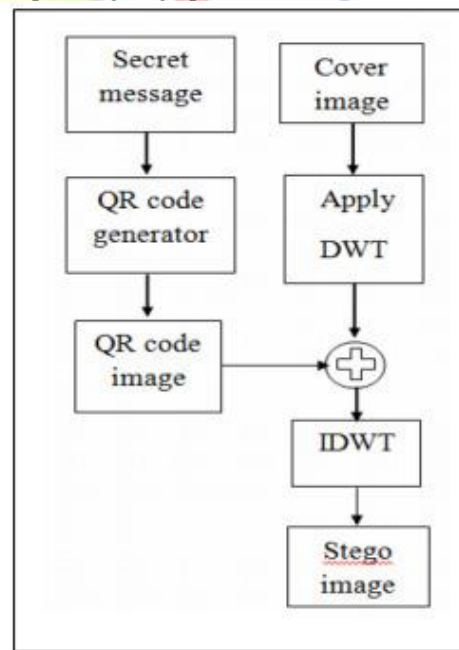
Encoding algorithm:
Step 1: Cover picture is taken as an input.
Step 2: creating the QR code with the secret code.
Step 3: Applying the discrete wavelet Transformation.
Step 4: Embed the QR code picture on the cover Step 5: To apply the inverse discrete wavelet transformation.
Step 6: Steganographed QR code is created.

Encoding Model.
Fig.2.QR code Steganography

C.Copy detection pattern QR code:

Copy detection pattern QR code is one of the most innovative and famous technique of QR generation. In this technique, with the help of secret key, password and random seed a maximum entropy image is created it is used as a graphical QR code. This copy detection technique is widely used for document authentication. The comparison of the original QR code along with the QR code present in the document is performed on the basis of which it is decided whether the document is authentic or not authentic. After performing the comparison the difference is noted, and if the difference between these two QR codes is greater than a threshold value.then we conclude that the data file is not authentic and is tampered. In other words, the length of the data is given beforehand. This technique is even useful for removing the demerites created by performing the print and scan process, which distorts the original QR code.

III. VARIOUS APPROACHES FOR FILE AUTHENTICATION USING QR CODE :

The image processing technique of document authentication using QR code is one of the widely used document authentication technique. In this the main emphasis is laid on the signature verification with the help of QR codes. This technique gives a state of the art solution of skilled and semi-skilled forgeries by robust mechanism. This method gives dynamic information gathering as a result of which the performance is enhanced. This method gives very high accuracy.

B. Feature Extraction:

In this technique, there are generally two phases of document authentication using QR codes. In first phase the input is acquired. The second phase consists of pre-processing, in which the different noises are removed and is further processed to pre-processing. In this technique, meaningful data will be extracted from pre-processed signature for classification. Afterwards, the features extracted in the previous stage are useful to match the input signature shape and the training samples. The result is used to decide the authenticity of the input signature for reducing forgeries. Then the comparison of training information with features is performed. Then a threshold is set, and according to the threshold we will divide whether the document is authentic or not. But the results were not satisfactory as the extraction of exact signatures from testing data pictures produces error in verifying the signatures.
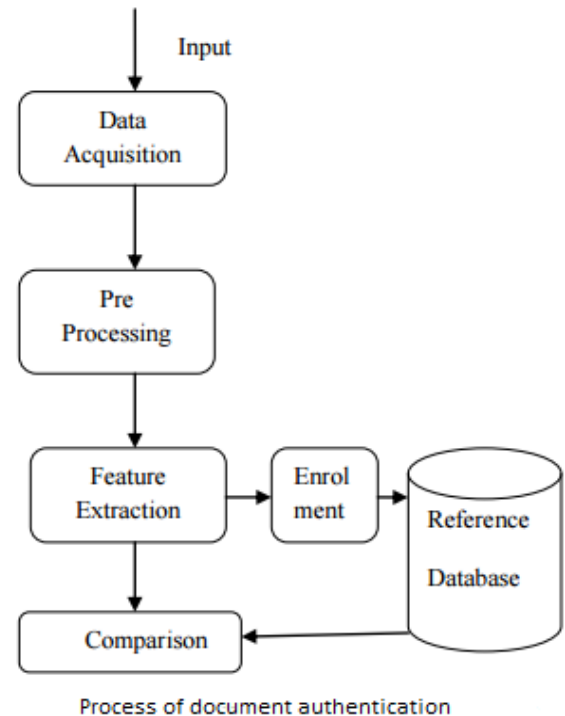

Fig. 3. Process of document authentication

EXISTING SYSTEM AND DISADVANTAGES:

Existing framework in view of seeking social values in between P&S un helpful examples and related examples. The Capacity limit can be eminently extended by code letters in order q or by expanding the finished example measure. Existing framework comes about demonstrate reclamation of private information. It highlights the likelihood of utilized this QR code for record verification. In this work private level improved by supplanting dark modules by particular surface. For example current work utilizes rich graphical code. Private information are embedded by including distortion in print and sweep technique. These rich graphical codes increased hugeness by enhancing tasteful

Perspective of QR code.

Merits:-
Increase storage capacity of QR code to differentiate original document.
Demerits:-
1) Information stored in a QR code is can be easily readable to camera containing, although it is not plain text and therefore is

Only readable to authorized user, likewise watch and read. It is impossible to divide an originally document in QR code from its copy due to their insensitivity to the Print and Scan process.

IV. PROPOSED SYSTEM AND ADVANTAGES

Proposed framework utilizes two levels QR for data stowing away. This 2LQR code has taking two levels
1. Public level
2. Private level.

People in general level QR code can read the content or report effectively with peruse but the private level needs a particular gadget with encoded information. This 2LQR code can be used for private message sharing or for verification system. The private level is made by supplanting white modules with finished examples from cover image. This finished example is considered as white modules by standard QR code peruser. With the goal that private level is covered up to QR code perusers, Propose framework for private level does not influence in any type the examining open information of people in general level. The proposed 2LQR code extents the capacity limit of the established QR code because of its supplementary perusing level. The capacity limit of the 2LQR code can be enhanced by extending the quantity of finished examples used or by diminishing the finished example measure. Cover image to conceal data, our calculation shroud the source surface image and implants mystery messages through the procedure of surface combination. This permits us to concentrate mystery data and the source surface from a stego engineered surface.

Advantage:-
1. Secure encoding of document, text etc.
2. Two level user authentication
3. Text steganography for data encoding
4. stego synthetic texture for QR code hiding.

Two Level QR (2LQR) Code Generation:

The standard QR code, the 2LQR code has the same specific structure, which consists of position tags, alignment patterns, timing patterns and format patterns. However, in the standard QR code, we have white and black modules and in the 2LQR code we have white modules and textured modules in place of black modules. This replacement of black modules by textured modules is not disrupting the standard QR code reading process. But it allows us to a second storage level, which is disappeared to the standard QR code reader. This second level consists of the private message, enwith q-ary code with error correction capacity .The textured modules are also named textured patterns in the rest of this paper. These textured patterns have specific features and are useful for private message *Mpriv* storage in the proposed 2LQR codes. In private data sharing scenario, the black modules of these

pattern are also replaced by textured patterns. Now we describe the 2LQR code creation steps as illustrated. The input data is the public message *Mpub* and the private message *Mpriv*. The output is the 2LQR codes.
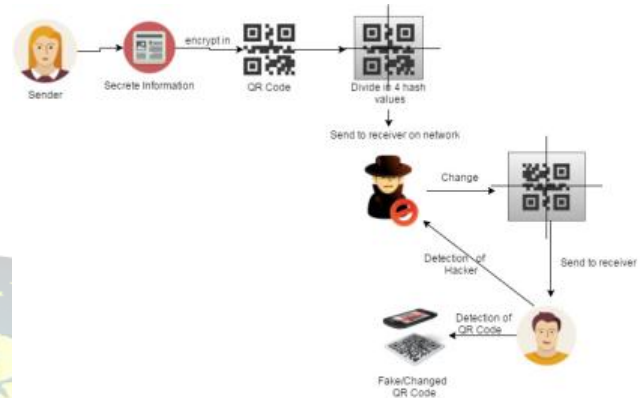
System Architecture

ALGORITHM:
Our system can be represented as a set
$X = \{I, O, S_C, F_C, C\}$
Where,
I=set of inputs
O=set of outputs
S_C= set of outputs in success cases
F_C = set of outputs in failure cases
C = set of constraints
$I = \{U_D, I_S\}$
Where,
U_D = Set of user details
I_S = Set of Images.
$O = \{I_S, S_M, F_M\}$
Where,
I_A = set of Images
S_M = Success messages.
F_M = Failure message.
$S_C = \{I_{Un}\}$
Where,
I_{Un} = valid set of images uploaded
$F_C = \{I_{Un}, NULL\}$
Where,
I_{Uo} = invalid set of images uploaded
NULL represents no output
$C = \{C_1\}$
Where,
C_1 = "System only accepts images of file types such as bmp, jpeg, png"
I_U, I_{Uo}, I_{Un} are in the form
$I = \{I_1, I_2 \dots I_n\}$
where,

I_1, I_2… I_n are images

CONCLUSION:

In this paper a new rich code called two level QR Code is proposed. This 2LQR code has two levels: a public level and a private level. The public level can be read by any QR code reading application, while the private level needs a specific application with specific input information. This 2LQR code can be used for private message sharing or for authentication scenarios. The private level is created by replacing black modules with specific textured patterns.

These textured patterns are considered as black modules by standard QR code reader. Thus the private level is invisible to standard QR code readers. In addition, the private level does not affect in anyway the reading process of the public level. The proposed 2LQR code increases the storage capacity of the classical QR code due to its supplementary reading level. Experiment results show that the storage capacity is improved by up to 28% (transition from message size equal to 272 bits to a message length of 380 bits). The storage capacity of the 2LQR code can be improved by increasing the number of textured patterns used or by decreasing the textured pattern size. All experiments show that even with a pattern size of 6x6 pixels and with an alphabet dimension q=8, it is possible to obtain good pattern recognition results, and therefore a successful private message extraction. However, we are facing a trade-off between the pattern size, the alphabet dimensions and the quantity of stored information during the 2LQR code generation. Attackers use various QR codes in phishing attacks. An attackers could create thousands of business cards purporting to be from Subway that say, 'Free foot long if you join our QR Club' printed next to the various malicious code. When they scanning the code and enter the link, the site could simply reply,joining the club' while silently installing a Trojan. To avoid this problem by propose the Enhance attack detection algorithm in our future work. In this algorithm automatically analyses the receiving QR code. If the message contain attacker then automatically block corresponding QR code message and which is add to the spam list. In this manner we are prevent from attacker activities.

REFERENCES

[1] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in Proc. IEEE 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520-523.

[2] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hiding mechanism using QR barcode,"in Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22-25.

[3] S. Vongpradhip and S. Rungraungsilp, "QR code using invisible watermarking in frequency domain," in Proc. IEEE 9th Int. Conf. ICT Knowl. Eng. (ICT Knowledge Engineering), Jan. 2012, pp. 47-52.

[4] M. Querini, A. Grillo, A. Lentini, and G. F. Italiano, "2D color barcodes for mobile phones,," Int. J. Comput. Sci. Appl., vol. 8, no. 1, pp. 136155,2011. [5] R. Villan, S. Voloshynovskiy, O. Koval, and T. Pun, "Multilevel 2-D bar codes: Toward high-capacity storage modules for multimedia security and management," IEEE Trans. Inf. Forensics Security, vol. 1, no. 4, pp. 405-420, Dec. 2006.