Steganography with Visual Secret Sharing Scheme Based QR Code Application: A Survey

AKSHAY AWASTHI, M.Tech Scholar, Department of Computer Science & Engineering, Kanpur Institute of Technology Kanpur, India.
AKHILESH PANDEY, Assistant Professor, Department of Computer Science & Engineering, Kanpur Institute of Technology Kanpur, India

Abstract— **Image cryptography is research area emerging. Various techniques for cryptography have been developed. The many techniques for encryption were used to conceal the visual information (photos, text, etc.) in image features. The main idea of encryption is the probability of human vision decryption if the correct key image is used, called visual cryptography.**
QR code stands for the acronym 'Quick Response.' It was developed by Japanese company Denso Wave Corporation. QR code is a two-dimensional barcode that can encode more than one-dimensional barcode information. QR codes are readable easily, too. The advent of smart phones enhances the use of QR code, as a Smartphone has scanning and decoding capabilities of a QR code. The emergence of mobile internet access technology encourages online marketers, newspapers and magazines to use QR codes when advertising their goods. Such codes have different meanings over standard barcodes, such as improved storage capacity, fast readability, 360 degree reading, small print size, correction of errors, support for more languages, and soil and damage resilience. Because of these advantages, the use of QR code has spread around the world. The paper tries to highlight the QR codes, their features, their function, their meaning and their downsides.
***Index Terms*—**Visual Cryptography, Image Processing, Secret Sharing Scheme, QR codes

I. INTRODUCTION

Digital information and data are transmitted more often over the Internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have accelerated the popularity of digital media. Digital images, video and audio have been revolutionized in the way they can be captured, stored , transmitted and manipulated, and this gives rise to a wide range of applications in education , entertainment, media and military, as well as other fields. Computers and networking facilities have become less expensive and more widespread. Creative approaches to storing, accessing and distributing data have generated many benefits for the digital multimedia field, mainly due to properties such as distortion-free transmission, compact storage and easy editing [1].
With the increasing dependence on computers at all levels of our life, personal and sensitive information is increasingly being stored and transmitted using computer systems and networks every day. This revolution, however, has brought with it new threats and computer crimes as evidenced by the increased number of computer attacks and break-ins. Replicating important information will give greater chance to intruders to access it. On the other hand , having only one copy of this information means that if this copy is destroyed there is no way to retrieve it. Thus, there is a great need to handle information in a secure and reliable way. In such situations, secret sharing is of great relevance.
The Digitalization has the greatest potential to alter the way we live. In today's era of the digitalized world, security is an important concern. Security problems start to become evident as information is being transmitted from node to node over the network. The number of threats has been growing at a wider pace, thus, strong security measures need to be implemented.
With the advent of location aware mobile technology, providing accurate context aware information at a critical time for those in need has become easy. This technology in combination with barcodes can be utilized to provide accurate and critical information to people moving in a crowd who may require it to face emergencies like stampedes, health problems, rioting, overcrowding, accidents etc. At the same time security and privacy of the information provided should not be compromised.
This research work presents a secure real-time system based on Quick Response Code specifically designed for any crowded environments where there is a requirement for people to be assisted by providing contextual information for navigating to their respective destinations. The same system can also be implemented for any other scenarios like huge exhibitions, airports, shopping malls or even the battlefields where there is a chance of an individual getting lost or requires direction. Data is compressed, encrypted and then encoded in the QR code.

II. LITERATURE REVIEW

Literature survey interprets old information and generates a combination of new information with old information. So, in this section there is a brief description of various research papers and occurrence of summary and synthesis of research papers.
Quick Response (QR) code can be effectively used to hide information for secure data transfer. Extracting useful information from raw data is an interesting research area where the extracted information is used for real-time applications. The data encoded in QR code can be read easily using simple scanning devices like mobile phones by an end user to uses the information. Advantages of using QR Code are the data is hidden and at the same time available for the concerned user who is equipped with relevant devices and privileges to extract information. QR code was originally developed by an automobile

company in Japan but nowadays it is used throughout the world. It is freely available and easy to generate. It can be decoded by any scanning devices such as mobile phones.
In the early days only URLs were encoded into the QR code but later on other information like phone numbers, SMS, addresses, personal information, corporate announcements etc. were also stored using QR code. The structure of a QR code is very simple. It consists of a white background, square grid of black square dots which are arranged as per the information that is encoded.
Pandya&Galiyawala (2017) surveyed the QR codes in the research and the Application. The QR code was the type of matrix barcode, which was designated for the automotive industry by the Denso Wave in Japan. The QR codes have fast readability and greater storage capacity, when compared to the UPC barcodes. In this survey work, the basics of the QR codes, its real time applications in the day-to-day life. The QR codes were the adequate tool to quickly and efficiently converse the URLs to the user with the help of mobile phones. The QR code consists of the architecture and the encoding. The function patterns were not used for the encoding the data. The procedure of the QR code includes the following stages:

- The input data was encoded using the most efficient mode and the bit stream was formed.
- The bit streams were divided into the code words and the code words were divided into the blocks and the error correction code words to each block.
- The code words were put into the matrix form and were masked with a mask pattern.
- The function patterns were added to the QR symbol.

It also researched and implemented the advanced technique that existed on the QR code to remove the scratch or the damage. The QR code decoding algorithm could not decode the image, if the QR code contained some scratch. The scratch removal technique consisted of several processes to get the scratch out of the damage. By simulating the HSV the QR code was extracted from the damage. Then, to start the dilation process, the morphological image processing technique was applied, which changes the image structure and makes the scratch noticeable to the user. The decoding stage efficiency was enhanced with the use of the median filter to convert the image to the binary image by removing the noise. The 2D barcode with a digital watermark was a much-used area of security research. The QR codes were used in many areas, and the QR codes had so many possibilities. There have been many projects to enhance information security, enhance recognition, minimize redundancy to save space, encrypt the possibility of various types of data such as audio , video, etc.
For increased data capacity and security, Meruga et al.(2015) created the covert, color QR codes. QR codes is mainly aimed at layering the QR codes with different colors. The QR codes have been used in a number of applications including marketing, inventory management and product tracking. Color coding in QR codes effectively increased the data capacity by three times that of conventional QR codes, while the QR code's covert nature added more protection. The six base colors in the QR codes were used to further increase the data capacity.
Shen et al. (2014) proposed a robust QR code image for Smart Systems development. IT technology has contributed to the development of QR code, which has been used in numerous applications. The QR code emerged as a new automated recognition technology. Rungraungslip et al. analyzed the picture of the QR code based on the theory of the retinex. (2012). (2014). Also proposed was the location and the correction method, which was based on the algorithm for tracking chain code. The correction approach used the morphological features of the QR code to find and remove the QR code. Results of the experiment indicate that the proposed approach was used to reliably extract images of the QR code from the background.
Harini&Padmanabhan (2013) introduced 2CAuth, a new authentication factors that increased the secure use of application information and preserved the user's usability. The significant feature of the scheme was that the Mobile Network Operator (MNO) did not allow any synchronization. The QR code usually gives the scheme 's usefulness in terms of accessibility, and even the highest loads on mobile networks. The presented scheme had the double advantage of performing transaction verification which required the user's physical presence and those to be performed in the user's absence. The authentication schemes relied on password based schemes and increased agency ownership. The advantages of the proposed scheme were that there was no secret code to store on the Smart Card. The scheme used true authentication by requiring the user to have the smart card, secret key and the mobile phone registered. The server didn't require the user's certificate, which authenticates the user. The authenticated user in this scheme holds a legitimate smart card and a QR code capture device.
Langford & McCoy (2012) researched the generation of QR codes for patients and health care providers by scanning the QR codes using either of the scanning tools and a computer program. The QR codes were used to easily classify patients, and access to the patient's web-based electronic medical records. Haque&Dybowski (2014) had the QR code generation researched and implemented. Developing countries' educational institutions are seen as a large sector that is expanding rapidly. The educational institutions used the handwritten ID cards and files even though the technology has improved still. If the ID card program was implemented in a systemized manner then identifying the student and monitoring his or her progress became much easier. For this function the QR code has been paired with the student ID card code. The QR code was attached to the ID card, and personal information for the student were collected by scanning the QR code. This was said to be the bar code for next generation. For developed countries the ID card was a great application of modern technology. The QR code was the unique type of barcode matrix, created specifically for the factories. Because of its wide storage capacity and speedy readability it became more common and familiar. The code was usually rendered on the pure white backdrop of pure black modules, and the black modules were kept in a square pattern. The knowledge was encoded using the Kanji symbols or alphanumeric symbols. The QR code algorithm or function has 6 key parts, like:

- Three Position Detection pattern
- Timing pattern code
- Reed-Solomon Error Detection

- Data Area
- Buffer zone or Quite zone
- Alignment pattern

The barcode has some disadvantage such that it does not contain all the information in detail. The barcode was replaced by the QR code and easily inserted or made a link to more information. The QR code easily encoded the web link and the web address. There were several advantages in encoding the data inside QR code. When the QR code was online then it was capable of reading anything with the help of camera and the sensor of the cellphone.
There were some drawbacks of using the QR code such as:

- The user should have a camera phone and the right kind of software installed on the mobile phone.
- The QR code was used only by the smart phones to read the QR code image.
- The use of camera phones was expensive.
- It was a real problem of using a smart phone for the people above 40 years and the people was not interested in spending lots of money.
- All the camera phones were unable to read the QR code

The QR code was used in several applications, which includes,

- Used as current mainstream
- Applications in the field of E-ticketing
- System for Loyalty points
- Intelligent advertisement

Sreenivasagam&Velumani (2013) introduced a zero watermarking scheme for accessing patient medical information. The zero watermarking schemes implemented in this work were based on the Composite Transform (CT) and Singular Value Decomposition Domain (SVD) for medical image authentication. Patient record recognition was obtained using the watermarking system. The health care institutions adapted the cloud-based archiving of medical images, and they were effectively shared by the patient records. Access to these records and the protection of these records was regulated to prevent fraudulent activities and medical history errors. The patient was marked and patient information were encoded inside the QR code, which acted as the watermark.

III. Visual Cryptography

Within the security domain cryptography has a long and fascinating history. The management of classified images that contain confidential information is of primary concern in several agencies, such as the exchange of maps in the military and many other commercial sectors over the internet. Various secret image sharing schemes have been developed to manage the security problems of sensitive pictures. Naor and Shamir[1] created one of the techniques known as Visual Cryptography (VC) in the year 1995 to manage hidden image sharing.
VC is a method in which a secret image containing sensitive visible information is encrypted in a completely secure manner, so that the decryption can be carried out directly by the human visual system (HVS) without computer assistance. VC enables some visual information to be encrypted, such as printed text, handwritten notes, and photographs. Throughout the decryption process it prevents complicated computation, and the images can be restored by stacking operation on its shares. This incorporates the trait of creating perfect ciphers and exchanging secrets in cryptography. In general, the hidden picture is divided into two or more parts known as shares. The hidden images are retrieved when the appropriate number of shares is printed on transparencies and then superimposed.
Naor et al.[1] implemented the VC technique where the binary image is broken down into n number of shares. Figure 1.1 shows an example of using visual cryptography to build and retrieve a secret image by sharing. The initial secret image is shown in the (k, n) scheme, when stacked over one another. Naor scheme fits perfectly with a binary image. The shares created in the original image are determined by randomly selecting pairs of black and white pixel sub-pixel matrices [2].

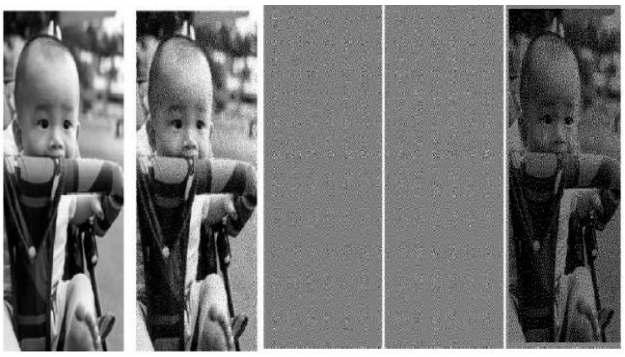

Figure 1: Original image, Halftone, Share-1, Share-2 and Decrypted image

IV. QUICK RESPONSE CODES

A QR code (abbreviated from Quick Response code) is a type of matrix barcode (or two-dimensional barcode) that was first developed in 1994 for the Japanese automotive sector. A barcode is an optical mark readable by computer, containing information about the object to which it is attached. For practice, QR codes also contain data that points to a website or application for a locator, identifier, or tracker. A QR code uses four uniform types of encoding (numeric, alphanumeric, byte / binary, and kanji) for efficient data storage; extensions can also be used. [4] [French version]

Thanks to its easy readability and greater storage capacity compared to standard UPC barcodes, the Quick Response system became popular outside the automotive industry. Applications include inventory tracking, identifying products, time tracking, handling records, and general marketing. A QR code consists of black squares placed on a white background in a square pattern, which can be read by a camera-like imaging system and processed using Reed – Solomon error correction before the image can be properly interpreted. The required data are then extracted from patterns present in both horizontal and vertical image components. [5]

Figure 2: QR Code

Unlike the older, one-dimensional barcodes designed to be scanned mechanically by a narrow beam of light, a QR code is detected by a 2-dimensional digital image sensor and then processed digitally by a programmed machine. The processor locates the three distinctive squares at the corners of the QR image code, using a smaller square (or several squares) at the fourth corner to normalize the image by size , orientation, and viewing angle. The small dots are then converted to binary numbers in the QR code, and checked with an algorithm that corrects errors. [6] [6] [6] [...]

Masahiro Hara, of the Japanese company Denso Wave, invented the QR code system in 1994. The aim was to monitor vehicles during production; it was designed to allow high-speed scanning of the components. In a much broader context, QR codes are now being used, including both commercial tracking applications and convenience-oriented applications for mobile phone users (desktop tagging).

QR codes can be used for displaying text to the user, adding a vCard connection to the user's device, opening a Uniform Resource Identifier (URI), connecting to a wireless network or writing an email or text message. There are several generators of QR code available as software or online resources which are either free, or require a paid subscription. The QR code has become one of the two-dimensional code types most in use. [13] [14]

QR code is a two-dimensional information encoding, and is also referred to as matrix code. This matrix code is readable by machine and consists of black and white squares. It can store information in the form of a URL, contact information, link to videos or photos, plain text and much more. [14] [13]

QR Code Architecture Each symbol with QR code looks like a square pattern. This square pattern is composed of two regions: region encoding and pattern operation. The role patterns concentrate on the positioning in which the encoding region represents the encoding of data.

The QR code symbol form is shown in Figure 2. The role pattern includes patterns for the finder, timing patterns and patterns for alignment. Three common structures are named finder patterns on the three corners of the QR code symbol. Finder pattern is used to determine which symbol is correctly oriented [15]. The decoder program uses timing patterns to figure out the side of sequence. Alignment patterns are used to correctly decipher the symbol by decoder software in case of image distortion. The rest of the region i.e., other than feature pattern is the encoded region where words of data code and words of code corrections are stored[13]. The Quiet zone is the spacing given to differentiate QR code from the surrounding environment. Essential for the scanning system.

Characteristics of QR Code

1. **High Storage Capacity**

   A QR code symbol can store up to 7,089 characters of information, which is a huge amount as compared to 1-D barcode.

2. **Encodable Character Set**
   - Numeric data (Digits 0-9)
   - Alphanumeric data (upper case letters A-Z; Digits 0 - 9; nine other characters: space, : % * + - / _ $)
   - Kanji characters

3. **Small Printout Size**

   The information in QR code is stored in both horizontal and vertical directions. Due to this feature, for the same amount of data, space acquired by QR code is one fourth times less than the space acquired by 1-D barcode.

4. **360 Degree Reading**

QR code is readable from any direction. This feature is provided by the finder patterns present at three corners of the symbol. The finder pattern helps to locate the QR code.

5. Capability of Restoring and Error Correction

If the part of code symbol is damaged or dirty, data can be recovered. The error detecting procedure can focus on the region of correct information. There are four levels of error correction of QR code that are L, M, Q and H. The level L has the weakest and level H has the strongest error correction capability [10].

V. USES OF QR CODE

In consumer advertising QR codes have become popular. A smartphone is usually used as a QR code scanner, showing the code and translating it to some useful form (such as a standard URL for a website, thereby eliminating a user's need to type it into a web browser). QR code has become a priority for advertising strategy, as it provides a way to access the website of a company quicker than by entering a URL manually. The value of this function, beyond mere convenience to the customer, is that it improves the conversion rate: the probability that interaction with the advertisement can translate to a transaction. With little pause or effort, it coaxes interested prospects further down the conversion funnel, taking the viewer directly to the advertiser's website, where a longer and more focused sales pitch can lose interest from the viewer.

While initially used in vehicle manufacturing to track components, QR codes are used over a much wider range of applications. These include export monitoring, ticketing for entertainment and travel, sales and loyalty marketing, and product marking in-store. Examples of marketing include where a company's discounted and percent discount can be captured using a QR code decoder which is a mobile app, or where information such as address and related information can be stored alongside its alpha-numeric text data, as can be seen in the Yellow Pages directory [16].

QR codes that store addresses and URLs will appear in newspapers, posters, buses, business cards or almost any item that users might want information about. Users with a camera phone that is fitted with the appropriate reader application can scan the QR code image to display text, contact information, link to a wireless network or open a web page in the browser of the computer. This act of linking from objects of the physical world is called hard linking or hyperlinking. QR codes may also be linked to a location where a code has been scanned for tracking. Either the application scanning the QR code obtains geo information using GPS and cell tower triangulation (aGPS), or the URL encoded in the QR code itself is associated with a position.

Mobile operating systems

QR codes can be used on various mobile device operating systems. iPhones running on iOS 11 and higher and some Android devices can natively scan QR codes without downloading an external app. The camera app is able to scan and display the kind of QR code (only on iPhone) along with the link (both on Android and iPhone). These devices support URL redirection, which allows QR codes to send metadata to existing applications on the device. Many paid or free apps are available with the ability to scan the codes and hard-link to an external URL. [10]

1) *URLs*

URLs improved advertisement conversion rates back in the pre-smartphone era, although there were many drawbacks during those years: ad viewers typically had to type the URL and sometimes didn't have a web browser in front of them when they first saw the commercial. The chances were high they would later forget to visit the site, not bother typing a URL, or forget what URL to type. Semantic URLs reduced but did not remove all threats. With the advent of smartphones, the issue of viewers not being able to access a website suddenly became less of a concern, but the trouble of typing in URLs persisted and so QR codes were used to allow quick access to redirect to URLs. Many generators of QR codes give an additional feature-Dynamic QR codes. Dynamic QR codes can be changed repeatedly because they use a placeholder URL which also makes scanning simpler and quicker than their counterpart-Static QR codes[10].

2) TOTP use

QR codes are also used in scanning TOTP secrets to generate time-based one-time passwords.

3) Website login

QR codes can be used to log into websites: a QR code is shown on the login page on a computer screen, and when a registered user scans it with a verified smartphone, they will automatically be logged in. Authentication is performed by the smartphone which contacts the server. Google tested such a login method in January 2012.

4) *QR code payment*

QR codes can be used to store bank account information or credit card information, or they can be specifically designed to work with particular payment provider applications. There are several trial applications of QR code payments across the world. In developing countries like India and China, QR code payment is a very popular and convenient method of making payments. [12]

VI. CONCLUSION

Within this paper QR codes are studied from their context and uses perspective. The QR code process is addressed to familiarize readers with the QR codes. QR code can store complex pieces of information in a small code. As understanding of the utility of such codes increases, we may anticipate their use in more public spheres.

References

[1] M. Naor and A. Shamir, ―Visual Cryptography,‖ Advances in Cryptology ,EUROCRYPT-94, LNCS-950, pp. 1–12, Springer, Berlin, Heidelberg, 1994.
[2] Yang, C. N., & Wang, D. S. (2014, Feb.). Property analysis of xor-based visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology, 24(2), 189-197.
[3] Shen, G., Liu, F., Fu, Z., & Yu, B. (2017, Oct.). Perfect contrast xor-based visual cryptography schemes via linear algebra. Designs Codes and Cryptography, 85(1), 15-37.
[4] Shyu, S. J., & Chen, M. C. (2015, Jan.). Minimizing pixel expansion in visual cryptographic scheme for general access structures. IEEE Transactions on Circuits and Systems for Video Technology, 25(9), 1557-1561.
[5] Sridhar, S., Sathishkumar, R., &Sudha, G. F. (2017, Jan.). Adaptive halftoned visual cryptography with improved quality and security. Multimedia Tools and Applications, 76(1), 815-834.
[6] Hu, H., Shen, G., Fu, Z., Yu, B., & Wang, J. (2016, Jan.). General construction for XOR-based visual cryptography and its extended capability. Multimedia Tools and Applications, 75(21), 1-29.
[7] Liu, F., & Wu, C. (2011, Jul.). Embedded extended visual cryptography schemes. IEEE Transactions on Information Forensics and Security, 6(2), 307-322.
[8] Kang, I., Arce, G. R., & Lee, H. K. (2011, Jan.). Color extended visual cryptography using error diffusion. IEEE Transactions on Image Processing, 20(1), 132-45.
[9] Yan, X., Wang, S., Niu, X., & Yang, C. N. (2015, Dec.). Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digital Signal Processing, 38(C), 53-65.
[10] ISO/IEC 18004:2015. (2015). Information - Automatic identification and data capture techniques - QR Code barcode symbology specification.
[11] Liu, Y., Fu, Z., & Wang, Y. (2016, Nov.). Two-level information management scheme based on visual cryptography and QR code. Application Research of Computers, 33(11), 3460-3463.
[12] Wu, X., Liu, T., & Sun, W. (2013, Jul.). Improving the visual quality of random grid-based visual secret sharing via error diffusion. Journal of Visual Communication and Image Representation, 24(5), 552-566.
[13] Yan, X., Liu, X., & Yang, C. N. (2015, Oct.). An enhanced threshold visual secret sharing based on random grids. Journal of Real-Time Image Processing, 1-13.
[14] Wan, S., Lu, Y., Yan, X., Wang, Y., & Chang, C. (2017, Mar.). Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions. Journal of Real-Time Image Processing, 9, 1-16.
[15] Akhilesh Pandey, Amitash ” Digital watermarking for image using 3-level DWT and PSO algorithms” International Journal of Advanced Research and Technology” Volume (7) Issue (2) June 2019.
[16] Akhilesh Pandey, Nisha Pal, Dr Dinesh Goyal ” A Survey on MRI Brain Image Segmentation Technique” International Journal of Advance Engineering, Management and Science” Volume (2) Issue (12) December 2016.