An Intelligence System for Visual Cryptography Technique Relying on QR Codes: A Review

Ashutosh Tripathi, M.Tech. Scholar, Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India.
Amit Verma, Assistant Professor, Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India

Abstract— **The field of study known as image cryptography is still in its infancy. A number of different approaches have been utilized in the development of cryptography. A number of different methods of encryption have been utilized in order to conceal any visual information (images, text, etc.) that may have been contained within photographs. The fundamental concept of encryption is known as visual cryptography. This concept refers to the human eye's potential to decipher a message provided the appropriate key image is used.**
The abbreviation for the "Quick Response" code is the "Quick Response" code. The Japanese company Denso Wave Corporation was the one to develop it. A one-dimensional barcode cannot hold nearly as much information as a two-dimensional barcode, which is what a QR code is. In addition to being easily readable, codes can also be QR codes. As a result of its inception, there has been a rise in the use of QR codes as a result of their ability to be scanned and decoded by a smart phone. As a result of technological improvements in the realm of mobile internet access, online marketers, newspapers, and magazines are increasingly turning to QR codes as a means of product promotion. These codes have a variety of advantages over traditional barcodes, including an enhanced store capacity, faster readability, reading from 360 degrees, minuscule print size, mistake correction, language support, and resilience to soil and damage. As a direct result of these benefits, the utilization of QR codes has become increasingly widespread all over the world. The focus of this research will be on Quick Response (QR) codes, including their advantages and disadvantages, as well as their functionality and significance.
Index Terms—Visual Cryptography, Digital Image Processing, Meaningful Shares, QR codes.

I. INTRODUCTION

Since we are living in the 21st century at this point, we are dealing with massive amounts of data, and we use the internet for the transaction of such data. Due to the assaulting tactics employed by attackers, the transmission of information over networks is not safe. In the modern world, criminal activity committed online is swiftly gathering steam. The data that we send and receive through the internet is of a diverse nature. If the information is really sensitive, then an increased level of protection is necessary. Attacks that take place across a network can be split into two categories: passive and active. Passive attacks are those that don't actively do anything. When an attack is considered passive, there is no alteration of the data, but when an attack is considered active, there is alteration of the data.

In order to ensure the safety of sensitive information, numerous data-concealment strategies are now in development. Data can be concealed using a variety of methods, including steganography, watermarking, and cryptography [1]. These methods come with a number of different downsides. In the event that the information has been watermarked, the receiver will not simply be able to extract the original data. The practice of steganography involves concealing data beneath other data. The issue with steganography is that it is possible to circumvent its limitations by making use of a key in order to protect one's data. However, the safety of the key is the primary issue in this scenario.

Visual cryptography is a technique that Adi & Shamir developed in order to circumvent the limitations that are inherent in data concealment techniques [2]. The primary purpose of a hiding technique is not only to conceal the data but also to shift attackers' attention in the wrong direction. This is the major aim of the approach. The terms "sharing scheme" and "steganography" are utilized in visual cryptography to provide a high level of protection. As we just mentioned, giving an attacker the wrong impression is also very crucial. In the beginning of the process of visual cryptography, there is a phase called share generation that is misleading. The overall concept of visual cryptography is represented in Figure 1.

In general, there are three stages: the recovery of the original data, the generation of shares, and the storage of sensitive data. A significant part of the system is played by the second phase. It considers the monochrome image in the form of a matrix, denoted by the letter M. This matrix is composed entirely of ones and zeros. Pixels that are black are represented by the number 0, while pixels that are white are represented by the number 1. Now, a share will be generated for each pixel based on M's contributions. It will be possible to see the original data if you only overlap those shares.

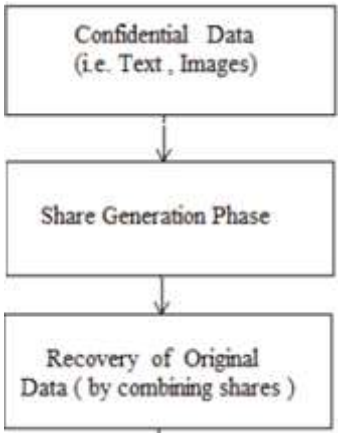

Figure 1: General Idea of Visual Cryptography (VC)

The disclosing of the original data is significantly aided by the process of superimposing the shares. Figure 2 demonstrates the superimposition of a black pixel on top of a white pixel. When we superimpose white pixels on top of each other, we do not acquire the full white share. Extended visual cryptography is utilized in the process of share generation.

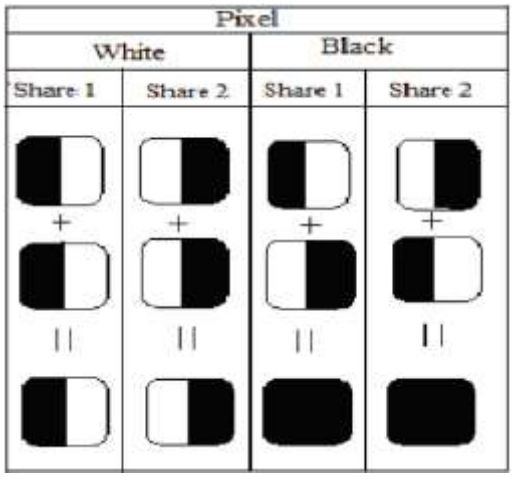

Figure 2: Superimposition of K-Shares

At the moment, information and digital data are transmitted via the Internet at a rate that is significantly higher than any time in the past. The accessibility and efficiency of worldwide computer networks, which allow for the transport of digital information and data, are largely responsible for the explosion in popularity of digital media. The process of acquiring, storing, transmitting, and modifying digital images, video, and audio has been revolutionized, which has resulted in a wide variety of applications in a variety of fields, including education, entertainment, the media, and the military, amongst others. Computers and capabilities for online networking have become more accessible and less expensive in recent years. The field of digital multimedia has reaped significant benefits as a result of the development of revolutionary systems for the storage, access, and dissemination of data, thanks to attributes such as distortion-free transmission, compact storage, and simple editing [3].

As our reliance on computers continues to expand across every aspect of our lives, the amount of personally identifiable and sensitive information that is being transferred and stored through the various computer systems and networks increases on a daily basis. This shift, however, has brought with it new threats and digital crimes, as evidenced by the increased prevalence of computer intrusions and break-ins. If vital information is duplicated, unauthorized individuals will have a greater chance of gaining access to it. On the other hand, given that there is only one copy of this information, there is no possibility of regaining access to it in the event that it is lost. As a direct consequence of this, there is an urgent requirement to manage data in a reliable and trustworthy manner. In circumstances like these, the exchange of secrets is of critical importance.

The digitalization of our lives has the most potential to bring about lifestyle shifts. In today's highly connected and digital world, there is a significant and growing concern regarding security. Concerns about data integrity and privacy arise whenever information is passed via the network from one node to another. Effective security solutions are essential since the number of potential dangers is increasing at a rate that is faster than before.

It is now much easier to provide folks who are struggling at a crucial time with precise information that is also aware of their context thanks to the development of location-aware mobile technology. In the event of a crisis, such as a stampede, a health emergency, rioting, overcrowding, or accidents, this technology, in conjunction with barcodes, can be used to communicate accurate and essential information to individuals moving through a crowd. These individuals may require this information in order to respond appropriately. At the same time, the confidentiality and protection of the information should not be compromised in any way.

E-coupons, also known as electronic coupons, have rapidly become a common form of cashless payment in recent years due to the rapid development of mobile Internet and mobile payment services. In recent years, there has been a proliferation of several kinds of electronic coupons, including cash coupons, discount coupons, prepaid cards, and rechargeable cards, among others. QR codes, also known as Quick Response codes, are frequently utilized by e-coupon providers. QR codes, also known as two-dimensional barcodes, are increasingly employed in a variety of contexts, including mobile payments, the verification of documents, the administration of commodities, the checking of inventories, and the tracking of packages, among other uses. QR codes are often utilized in e-coupon services due to the fact that it is simple to develop, manage, and utilize these codes at a low cost.

However, in recent years there has been an increase in the frequency of security issues involving QR codes, and the situation has gotten increasingly serious.

Forgery of QR codes, tampering with QR codes, unauthorized disclosure of private information, and the distribution of phishing websites are some examples of the security risks associated with QR codes. The open coding scheme of QR codes, the plaintext structure of the material in QR codes, and the absence of verification procedures are the primary causes of the dangers that have been described above. Cadger et al. [4] evaluated the results of deciphering QR codes by 12 different software packages. This is an example that has received a lot of attention. According to the findings of the study, not one of the 12 programmes is able to determine if a QR code has been altered, despite all of them being able to read the text.

Despite the fact that research on QR code security and privacy protection has become increasingly popular in recent years, there is now no viable answer to the problem of ensuring that QR code-based electronic coupon transaction services are secure. A significant portion of research on QR code security is concentrated on link identification [5, 6], which can prevent users from accessing dangerous websites by means of QR codes [7]. Using methods like cryptography and steganography, there is also research being conducted [7, 8] that aims to make QR codes more private by concealing the information they contain.

However, due to the unique dangers posed by electronic coupon payment services, such as collusion attacks carried out by merchants and customers, tampering with or fabricating electronic coupons, and so on, the results of this research cannot be reliably applicable to those services.

II. Literature Review

A literature survey analyses old data and generates a mix of new and old data. As a result, this part contains a brief explanation of numerous research papers as well as the presence of research paper summary and synthesis.

The safety of QR codes has been an increasingly important issue in recent years due to the proliferation of QR code-based electronic coupon services. Lin et al. [9] presented a secret hiding technique that is based on QR code error correction with the intention of safeguarding the information contained within QR codes.

Tkachenko et al. [10] suggested a technique for sharing secret messages that is based on a two-layer QR code. This scheme replaces the black blocks that are found in a standard QR code with a particular pattern.

Although these strategies are able to effectively solve some of the security problems associated with QR codes, they are not quite suitable for the transaction associated with e-coupons because the security goals of e-coupon services, such as authentication and integrity, cannot be met by these strategies.

Take into consideration the issue of tampering and forgery, there are some viable solutions to this problem. A message authentication mechanism for vehicle communications was proposed by Zhang et al. [11]. A method for verifying top-secret information that is based on an authentication chain was developed by Hasan and colleagues [12]. The fact that preserving a chain for each QR code requires a lot of space makes this technique unsuitable for use in QR code services, despite the fact that it possesses the traceability and anti-counterfeiting characteristics.

Pandya and Galiyawala (2017) conducted a study on QR codes as part of their research and application. Within the context of the automotive sector, the Denso Wave in Japan conceptualized the QR code as a form of matrix barcode. QR codes have a faster readability and a bigger storage capacity when compared to UPC barcodes. Additionally, QR codes are smaller in size. This study goes through the principles of QR codes as well as their real-time applications in various aspects of everyday life. Specifically, it focuses on the use of QR codes in retail settings. The usage of QR codes was a fantastic method that was both rapid and effective in sending URLs to consumers who accessed their mobile phones. The QR code is comprised of both the architecture and the encoding. The function patterns were not utilized in the encoding of the data. The following is an explanation of each stage of the QR code approach:

- The bit stream was produced after the input data had been encoded using the approach that was determined to be the most effective.
- The bit streams were first broken down into code words, which were then split down into blocks, and error correcting code words were allocated to each individual block.
- The code words were entered into a matrix, and then, using a mask pattern, they were hidden from view.
- Various function patterns can now be found on the QR sign.

In addition to this, it offered a more advanced method for removing any scratches or damage that may have been caused to QR codes. The image could not be decoded by the decoding algorithm if there were any scratches on the QR code. The strategy for removing scratches involved a number of stages because it was necessary to distinguish the scratch from the damage. The QR code was able to be repaired after it was damaged thanks to an HSV simulation. The morphological image processing technique was then used to begin the process of dilatation. This technique altered the structure of the image and made the scratch visible to the user. After this, the procedure was started. The effectiveness of the decoding stage can be improved by using the median filter, which converts the image into a binary representation and gets rid of noise. In the realm of information

safety, a well-liked study topic was the two-dimensional barcode that included a digital watermark. There was a wide range of software that made use of QR codes, and one could use QR codes in a number of different ways. In order to enhance information security, recognition, the reduction of redundancy in order to save space, and the encoding capabilities of various forms of data such as audio and video, many tests were carried out.

Meruga et al. (2015) came up with the idea of using colour QR codes that were disguised in order to increase data capacity and security. The QR codes were designed with the intention of stacking a variety of colours one above the other. QR codes were put to use in a variety of contexts, including but not limited to marketing, inventory management, and product tracking. The addition of colour coding to QR codes dramatically increased the data capacity of these barcodes by three times that of ordinary QR codes, while the covert nature of QR codes afforded increased levels of protection. The utilization of these six fundamental hues was necessary in order to increase the data capacity of the QR codes.

Even if there have been breakthroughs in technology, educational institutions have continued to employ ID cards and files that are handwritten. If the student identification card system was established in a methodical fashion, it was much simpler to identify the student and keep track of his or her progress. Within the scope of this project, the QR code was integrated into the student identification card. By scanning the QR code that was affixed to the student's identification card, we were able to get the student's personal information. The "bar code of the next generation" was how it was referred to. The identification card was a brilliant example of how contemporary technology may be put to use in less developed nations. The Quick Response (QR) code was an innovative form of matrix barcode that was developed exclusively for businesses. Its enormous storage capacity and its ability to be read in a short amount of time contributed to its meteoric rise in popularity and notoriety. The vast majority of the code was made up of black modules set against a white background, and these black modules were arranged in a square pattern. The data was encrypted using either kanji characters or alphanumeric symbols, depending on your preference. The algorithm that the QR code uses to perform its function is comprised of the following six key components:

- Three Position Detection pattern
- Timing pattern code
- Reed-Solomon Error Detection
- Data Area
- Buffer zone or Quite zone
- Alignment pattern

The barcode has a few drawbacks, such as the fact that it does not include every piece of information in minute detail. The barcode has been replaced by the QR code, which may quickly be linked to additional information or integrated into the document. The website link as well as the website URL was readily encoded using the QR code. There were a number of benefits that came along with putting the data inside the QR code. When the QR code was online, it was easy to read anything with the assistance of the camera and the sensor of a mobile device. This was possible thanks to the QR code.

Using a QR code came with a few problems, including the following examples:

- The user has to have a camera phone and the appropriate software installed on their mobile device in order to take pictures.
- Only the smart phones were able to read the QR code image since the QR code could only be read by smart phones.
- The use of camera phones resulted in additional costs.
- Using a smart phone was a major challenge for persons older than 40, and most people did not want to invest a lot of money on a device like that.
- It was impossible for any of the camera phones to read the QR code.

The Quick Response (QR) code has been put to use in a variety of applications, including the following:

- Used as the industry standard
- Applications in the field of electronic ticketing
- A system for collecting loyalty points
- Intelligent advertisement

III. VISUAL CRYPTOGRAPHY

The field of security that is known as cryptography has a rich history that is both lengthy and exciting. The management of sensitive images that include confidential information is a key priority in many different sectors. One example of this is the dissemination of maps by the military through the internet, which is also the case in many different corporate areas. To address the concerns over the safety of private photographs, a number of different methods for sharing images in secret have been devised. Visual cryptography, sometimes known as VC, is a method that was developed by Naor and Shamir [2] in 1995 to facilitate the communication of secret photographs.

VC is a method of encrypting a secret image that has confidential visible information in such a way that the decryption can be performed entirely by the human visual system (HVS) without the use of any computers at all. This is accomplished by encrypting the image in such a way that the human visual system is able to perform the decryption. VC is capable of encrypting any type of visual information, including but not limited to printed text, handwritten notes, and images. During the decryption procedure, it is no longer necessary to perform complex computations thanks to this solution, and the images can be recovered by stacking the shares. It combines the capabilities of producing perfect cyphers and transferring confidential information via

cryptography. In most cases, the hidden image will be broken up into two, three, or even more sections. When the necessary number of shares are printed on transparencies and then superimposed, the hidden images can be reconstructed.

The method known as VC was first presented by Naor et al. [2], and it involves decomposing the binary picture into an n-number of shares. The example shown in Figure 1 demonstrates how visual cryptography can be used to generate, communicate, and later recover a secret image. In the (k,n) scheme, the original hidden image is made visible when the shares are layered one on top of the other in ascending order. The Naor scheme is perfect for representing binary data in a picture. The shares of the original image are defined by randomly picking pairs of sub-pixel matrices for black and white pixels [9].

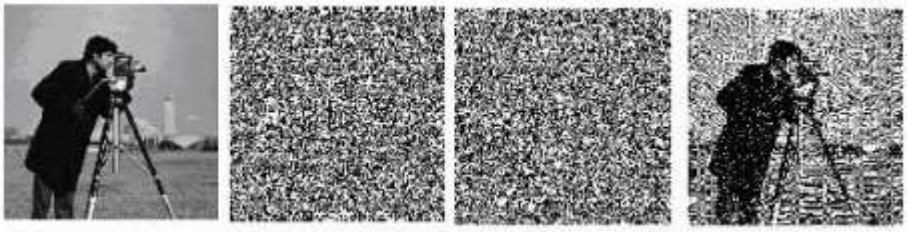

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

IV. Quick Response Codes

A QR code, which is an abbreviation for "Quick Response code," is a type of matrix barcode that was initially developed in 1994 for the Japanese automobile industry. A matrix barcode is another name for a two-dimensional barcode. A barcode is a type of optical label that can be read by machines and offers information about the object to which it is attached. Barcodes are typically rectangular in shape. In point of fact, most QR codes contain information that can be used as a locator, identifier, or tracker, which in turn sends people to a certain website or application. A QR code utilizes four distinct encoding modes (numeric, alphanumeric, byte/binary, and kanji), which allows it to store data in an efficient manner. Extensions may also be used. [13]

Outside of the automotive industry, the Quick Response system became quite popular due to the fact that its barcodes could be read more quickly and contained a greater amount of information than standard UPC barcodes. There are many different uses, some of which include product monitoring, item identification, time tracking, document management, and general marketing. A QR code consists of black squares arranged in a square grid on a white background. These squares are designed to be scanned by a camera and then subjected to Reed–Solomon error correction in order for the image to be correctly understood. The patterns that are found in the horizontal and vertical components of the image are then used to derive the vital information. [14]

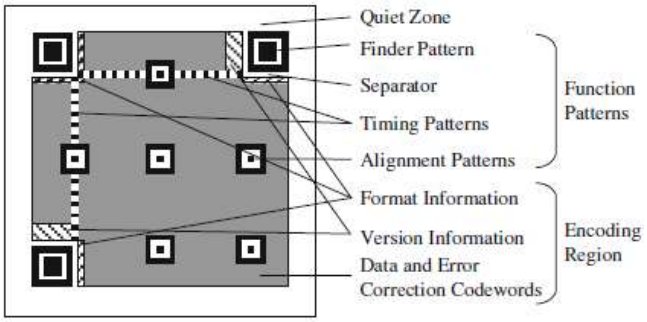

Figure 4: QR Code

Unlike older one-dimensional barcodes that were designed to be mechanically read by a narrow beam of light, a QR code is recognized by a two-dimensional digital image sensor and then digitally evaluated by a programmable processor. This is in contrast to older barcodes that were only one dimension and were designed to be read mechanically. The processor will first locate the three distinct squares at the corners of the image of the QR code. Next, it will normalize the image in terms of size, orientation, and viewing angle by deploying a smaller square (or several squares) near the fourth corner. Following this step, the dots that make up the QR code are converted into binary integers, and then an error-checking procedure is used to validate them [15].

In 1994, a Japanese businessman named Masahiro Hara of Denso Wave came up with the idea for the QR code technology. It was built to enable high-speed component scanning with the intention of achieving its primary purpose of tracking cars as they were being assembled. QR codes are presently used in a far wider variety of applications, including commercial tracking applications as well as apps that are geared toward providing ease of use for users of mobile phones (termed mobile tagging). It is possible to utilize a QR code to display text to the user, add a contact to the user's device in the form of a vCard, open a URI, connect to a wireless network, send an email or text message, or visit a website. QR code generators can be downloaded as software or used as web tools; depending on the generator, they can be used for free or need a subscription fee. The Quick Response (QR) Code is quickly becoming one of the most widely used two-dimensional barcodes due to its increasing popularity [13].

Data can be encoded in a two-dimensional format using a QR code, which is also known as a matrix code. This matrix code is readable by machines and is composed of squares of both black and white. It has the capability of storing URL (Uniform Resource Locator) information, contact information, links to videos or images, plain text, and a great deal more [14].
Structure of Quick Response Codes Each symbol that makes up a QR code has a pattern that looks like a square. This square pattern consists of two sections: the encoding region and the function patterns. Both of these regions are distinct from one another. The focal point of the function patterns is the location where the encoding region provides an indication of the data being encoded.
Figure 4 presents an illustration of the components that make up the QR code sign. The function pattern is comprised of finder patterns, timing patterns, and alignment patterns all working together. The three corners of a QR code symbol each include one of three recurring structures known as finder patterns. The Finder pattern is what's used to figure out which direction the sign should be facing. Timing patterns are utilized by the decoder software in order to establish which side of the pattern should be applied. In the event that the image is distorted, alignment patterns are utilized in order to guarantee that the decoder software correctly decodes the sign. The portion of the region that is not the function pattern is known as the encoded region, and it is responsible for storing data code words as well as error correcting code words [13]. The gap between the QR code and its immediate surroundings is referred to as the silent zone. It is essential in order for the scanning application to work properly.

Characteristics of QR Code

1. High Storage Capacity

In contrast to 1-D barcodes, which can only carry a maximum of 576 characters of data, QR codes have the capacity to hold up to 7,089 characters.

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 that is stored in a QR code is organized in a grid that can be read both horizontally and vertically. Because of this feature, the amount of space required to store the same amount of data using a QR code is one fourth times less than the space required to store it using a 1-D barcode.

4. 360 Degree Reading

QR codes can be read in whichever direction they are aimed. The finder patterns that are located in the three corners of the symbol are responsible for providing this functionality. Locating the QR code is made easier by the finder pattern.

5. Capability of Restoring and Error Correction

Data can be recovered even if the part of the code symbol that contains the data is broken or unclean. The process of looking for errors can direct its attention to the section that has accurate information. L, M, Q, and H are the four different levels of error correction that are available for QR codes. The level L has the least effective error correction capabilities, whereas level H has the most effective system [10].

V. Application of QR Code

Over the past few years, QR codes have seen a meteoric rise in popularity within the realm of consumer advertising. Smartphones are frequently used as QR code scanners because of their ability to show the code and convert it to a format that can be utilized (such as a standard URL for a website, thereby obviating the need for a user to type it into a web browser). The QR code has emerged as a central component of advertising strategy in recent years due to the fact that it allows users to reach the website of a company more quickly than putting in the URL manually. In addition to the fact that it is more convenient for the customer, the value of this capability lies in the fact that it increases the conversion rate, which can be defined as the percentage of people who come into touch with an advertisement that ultimately results in a sale. It rapidly and with little effort takes interested prospects further up the conversion funnel, ultimately driving the viewer to the advertiser's website, where a longer and more targeted sales pitch would cause the viewer to lose interest [15].

QR codes, which were initially used to track parts in the manufacturing of automobiles, are today utilized in a significantly wider variety of applications than they were when they were first introduced. A few examples of the services that fall within this category include commercial tracking, tickets for entertainment and transit, product and loyalty marketing, and in-store labeling of merchandise. Using a QR code decoder, which is a mobile app, to collect a company's discounted and percent discount is one example of marketing, as is saving a company's information, such as address and related information, with its alpha-numeric text data, as seen in the Yellow Pages directory. Another example of marketing is using a QR code decoder, which is a mobile app, to collect a company's discounted and percent discount.

Publications, signs, buses, business cards, and virtually anything else that customers would be interested in learning more about can all use QR codes that include addresses and URLs for consumers to access further information. Users who have a camera phone and an application that is capable of reading QR codes can scan the image of the code to view text, obtain contact information, connect to a wireless network, or open a web page in the browser on their phone. Hard linking, also known as hyperlinking, is the process of creating a link from an item that exists in the real world. You are also able to check where a QR code has been scanned because it is possible to correlate QR codes to specific locations. The geo information can either be

collected by the QR code scanning application through the use of GPS and cell tower triangulation (GPS), or the URL that is contained within the QR code can be associated with a specific location.

Mobile operating systems

There are a variety of operating systems for mobile devices that are compatible with QR codes. Native QR code scanning is available on iPhones running iOS 11 and higher, as well as on select Android smartphones, and it does not require the download of additional software. The camera app is able to read and display the type of QR code (only on iPhone), as well as the URL, although this feature is only available on the iPhone (both on Android and iPhone). These devices have the capability of URL redirection, which enables QR codes to convey metadata to programmes that are already installed on the device. There are a great number of programmes, both commercial and unpaid, that have the capability to scan the codes and directly link to an external URL [10].

1) ***URLs***

Even in the pre-smartphone era, URLs helped increase marketing conversion rates. However, during those years, URLs were constrained by a number of factors, including the fact that users typically had to manually type in the URL and frequently did not have a web browser open when they initially viewed the advertisement. There was a good risk that individuals would either forget to go to the website at a later time, not bother to type in the URL, or forget what URL they were supposed to type in. These dangers were mitigated to some degree by using semantic URLs, although they were not eliminated entirely. However, the inconvenience of typing in URLs still existed, and thus QR codes were utilized in order to allow redirecting to URLs that enable instant access. The problem of viewers not being able to access a website immediately has become less of an issue since the emergence of smartphones. A number of different QR Code Generators provide users with an additional option to generate Dynamic QR Codes. Because they make use of a placeholder URL, Dynamic QR Codes are capable of being edited an infinite number of times. In addition, scanning Dynamic QR Codes is much simpler and quicker than scanning 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

4) QR codes can be scanned with a verified smartphone and used to log into websites: a QR code is displayed on the login page on a computer screen, and when a registered user scans it with a verified smartphone, they are automatically logged in. The smartphone contacts the server and performs authentication. In January 2012, Google experimented with such a login mechanism.

5) ***QR code payment***

The information needed to access a bank account or credit card can be stored in a QR code, or the codes can be designed specifically for use with the software offered by a particular payment provider. The use of QR codes for making payments is now being evaluated in a variety of locations all around the world. In developing nations like India and China, using a QR code to make a payment is becoming an increasingly widespread practice because of how convenient it is [12].

VI. CONCLUSION

In this article, we suggested a visual secret sharing scheme for use in applications involving QR codes. The scheme improves primarily on two aspects: the level of security provided as well as the degree of flexibility provided to access structures. The security flaw that existed in the earlier work is addressed and resolved in our study. In addition, by conducting additional research into the error correcting process of QR codes, we increased the size of the access structure from n to k in order to accommodate more data. Two different strategies for division are presented, both of which effectively improve the sharing efficiency of the (k, n) method. In this study, we investigate the relevance of QR codes as well as the various applications for which they might be used. The purpose of this section is to familiarize the reader with QR codes by presenting an explanation of how QR codes work. A QR code is capable of storing a substantial amount of data in a very small area. As more people become aware of the usefulness of these codes, it is possible that more public domains will begin to implement them.

References

[1] Song Wan ,Yuliang Lu, Xuehu Yan and Lintao Liu, "Visual secret sharing scheme with (k, n) threshold based on QR codes", IEEE 2016.

[2] M. Naor and A. Shamir, ―Visual Cryptography, Advances in Cryptology ,EUROCRYPT-94, LNCS-950, pp. 1–12, Springer, Berlin, Heidelberg, 1994.

[3] 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

[4] F. Cadger, K. Curran, J. Santos, and S. Moffett, "A survey of geographical routing in wireless ad-hoc networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 621–653, 2013..

[5] A. Kharraz, E. Kirda, W. Robertson, D. Balzarotti, and A. Francillon, "Optical delusions: A study of malicious QR codes in the wild," in Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. IEEE, 2014, pp. 192–203.

[6] K. Krombholz, P. Fr¨uhwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl, "QR code security—How secure and usable apps can protect users against malicious QR codes," in Availability, Reliability and Security (ARES), 2015 International Conference on. IEEE, 2015, pp. 230–237.

[7] X. Zhang, H. Li, Y. Yang, G. Sun, and G. Chen, "LIPPS: Logistics information privacy protection system based on encrypted QR code," in Trustcom/BigDataSE/ISPA, 2016 IEEE. IEEE, 2016, pp. 996–1000.

[8] S. Sharma and V. Sejwar, "Impementation of QR code based secure system for information sharing using Matlab," in Computational Intelligence and Communication Networks (CICN), 2016 8th International Conference on. IEEE, 2016, pp. 294–297.

[9] P.-Y. Lin and Y.-H. Chen, "High payload secret hiding technology for QR codes," EURASIP Journal on Image and Video Processing, vol. 2017, no. 1, p. 14, 2017.

[10] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J.-M. Gaudin, and C. Guichard, "Two-level QR code for private message sharing and document authentication," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 571–583, 2016.

[11] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357–3368, 2008.

[12] R. Hasan, R. Sion, and M. Winslett, "The case of the fake Picasso: Preventing history forgery with secure provenance." in FAST, vol. 9, 2009, pp. 1–14.

[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] L. Li, R. L. Wang, C. C. Chang, "A Digital Watermark Algorithm for QR Code," vol. 2, no. 2, pp. 29-36, 2011.

