Advanced Visual Cryptography Secret Sharing Schemes Based on QR Codes

Saurabh Kumar, M.Tech. Scholar, Department of Computer Science & Engineering, Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India.

Madhu Lata Nirmal, Assistant Professor, Department of Computer Science & Engineering, Vishveshwarya Group of Institutions, Gautam Buddh Nagar, India

Abstract— **The primary principle behind Visual Cryptography (VC) is to divide the original secret image into many parts and decrypt them using the human visual system. Despite the fact that the technique for secret exchange is secure, Visual Cryptography has security flaws. Previous study has demonstrated the possibility of VC cheating using various ways. Without being noticed by VC participants, attackers can perform both cheating and alteration of the VC process.**

Because of its straightforward decryption, visual cryptography has attracted a lot of academic attention and progressed quickly in recent years. However, VCS's practical applicability continue to be hampered by meaningless shares. In this paper, we suggest merging a (k, n)-VCS with QR codes. The probabilistic sharing approach is used to increase the maximum size of the secret image that can be shared. Based on this, a secret sharing method with a high relative difference is described, and ANN is used to enhance the secret image. We also use encoding redundancy to insert the first shares onto cover QR codes. Following that, each share has meaning and can be read by any QR code reader. In contrast to prior work, the covers' error-correcting abilities have been perfectly intact. It emphasises that our approach can be used to verify the security of QR codes obtained from unknown sources. Finally, experimental data and comparisons are shown to demonstrate the suggested scheme's viability and benefits.

Index Terms— Probabilistic sharing method, high relative difference, (k, n)-VCS, Encoding redundancy, meaningful shares, QR codes

I. INTRODUCTION

Digitalization has the greatest potential to change our lifestyles. Security is a major worry in today's digitally connected world. When information is sent from one node to another through the network, security issues begin to emerge. Because the number of threats is expanding at a faster rate, effective security solutions are required.

With the introduction of location-aware mobile technology, providing accurate context-aware information to individuals in need at a critical time has become simple. This technology, in conjunction with barcodes, can be used to convey accurate and important information to those moving through a crowd who may need it in the event of an emergency such as stampedes, health issues, rioting, overcrowding, or accidents. At the same time, the information's security and privacy should not be jeopardised.

This paper provides a safe real-time system based on Quick Response Code that is specifically built for busy areas where individuals need to be supported by delivering contextual information for navigating to their destinations. The same technology can be used in a variety of other situations, such as large shows, airports, retail malls, and even battlefields, where there is a risk of an individual becoming lost or in need of direction. The information is compressed, encrypted, and then encoded into a QR code.

One of the most important strategies for ensuring information security is cryptography. Traditional cryptography methods require a lot of computer power and intricate algorithms to encode and decode a secret message, which takes a lot of time and money.

Visual Cryptography [1-3] is a secret sharing scheme that takes a secret image as input (i.e. printed, handwritten) and encrypts it into a set of other images called shares in such a way that the original secret is revealed if the shares are printed on transparencies and superimposed or staked over one another. The simplest kind of visual cryptography, also known as visual secret sharing, takes a binary image as input and treats each pixel separately.

Naor and Shamir proposed the Visual Cryptography Scheme [1] (VCS) as a type of image sharing technique. VCS's basic model entails dividing a secret image into many shares. By stacking any qualified subset of shares, the secret can be visually decrypted, whereas banned subsets cannot. VCS has gained a lot of study attention because of its low-computation decryption, and related studies such as recovery effect promotion [2-4], access structure flexibility [5], image colour extension [6], and sharing strategy enrichment [7] have all been done. However, most schemes' shares are meaningless, which will easily draw suspicion from attackers when transmitted through public channels, and the difficulty of controlling these shares will also increase.

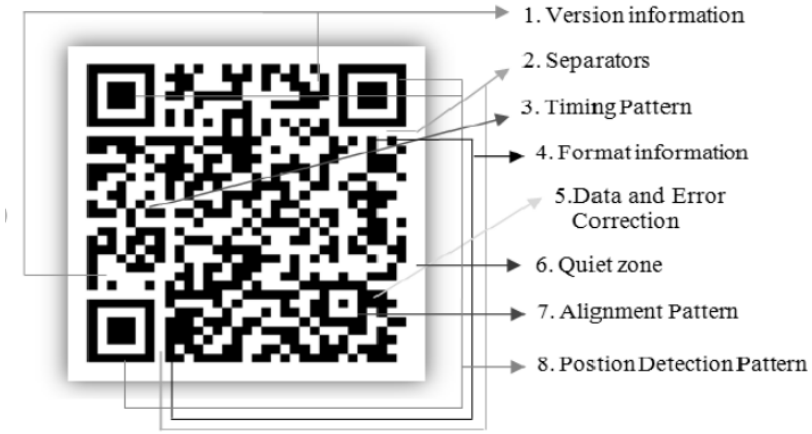

Figure 1: Structure of QR code

[1, 8] added some columns to the basis matrices to generate meaningful shares. These extra columns were utilised to store each share's cover information. Halftone technique was used into the design of schemes by [9] for a greater visual effect. However, there was still a lot of noise in the shares, which had a bad aesthetic effect. QR codes are a type of machine recognition code that was created by the Japanese Denso Wave Company and has since been approved as a worldwide standard by ISO [10]. QR codes have become widely employed in applications such as product promotion, electronic identity, and mobile payment since the introduction of intelligent cellphone technology. Human eyesight is almost impossible to decipher the message of a QR code due to its low visual recognition feature. In turn, because the dark and light modules are evenly scattered with a random appearance, the QR code can be a great mask for VCS. As a result, VCS and QR code pairings have received a lot of attention [10]. A strategy with two-level information storage was presented based on machine recognition characteristics [11].
Decoding shares was inconvenient in that approach unless an extremely acceptable scanning distance and angle could be found. Then, using the error correcting mechanism of QR codes, a (n, n) sharing approach was devised [12]. Later, a (k, n)-VCS was constructed in [14] under the random grids theory [13], where the relative difference of the retrieved secret requires further improvement. In this project, ANN is used to improve the secret image. Furthermore, because some code words were modified throughout the sharing procedure, the shares' error correcting capacities were reduced in [14]. This could affect the QR codes' resistance to symbol damage or loss.
In this paper, we suggest merging a (k, n)-VCS with QR codes. We offer a method for creating sharing matrix sets by classifying all minimal qualifying subsets. This scheme is based on a probabilistic sharing model, in which the unexpanded property allows for a greater secret size, and the secret picture is enhanced using ANN. It is also possible to acquire better, or even perfect, regained performance. We also make use of QR codes' encoding redundancy to insert original shares within their respective covers. Finally, a significant number of shares are obtained. Error correction capacities are totally preserved in this study as compared to previous work. The proposed scheme's effectiveness is demonstrated through experimental findings and comparisons.

II. Literature Review

A brief summary of the research relevant to the progressive collapse of building structures is offered here.
In their research and application, Pandya&Galiyawala (2017) surveyed QR codes. The Denso Wave in Japan defined the QR code as a type of matrix barcode for the automotive industry. When compared to UPC barcodes, QR codes have a faster readability and a larger storage capacity. The fundamentals of QR codes, as well as their real-time applications in everyday life, are covered in this survey. QR codes were an excellent technique for quickly and efficiently communicating URLs to users via mobile phones. The architecture and encoding make up the QR code. The data was not encoded using the function patterns. The stages of the QR code method are as follows:

- The bit stream was created after the input data was encoded in the most efficient method.
- The bit streams were broken down into code words, which were then broken down into blocks, with error correcting code words assigned to each block.
- The code words were placed in a matrix and masked using a mask pattern.
- The QR sign now includes function patterns.

It also looked into and offered an advanced approach for erasing scratches or damage from QR codes. If there were any scratches in the QR code, the decoding algorithm was unable to decode the image. In order to separate the scratch from the damage, the scratch removal approach included numerous processes. By mimicking the HSV, the QR code was recovered from the damage. The dilatation process was then started using the morphological image processing technique, which changed the structure of the image and made the scratch visible to the user. Using the median filter to transform the image to a binary image and remove noise improves the efficiency of the decoding stage. In the field of security, the 2D barcode with a digital watermark was a popular research topic. QR codes were utilised in a variety of applications, and there were numerous options

for QR codes. Many tests were carried out in order to improve information security, recognition, reduce redundancy in order to conserve space, and the encoding capability of various types of data such as audio and video.
The hidden, colour QR codes were invented by Meruga et al. (2015) for greater data capacity and security. The basic goal of the QR codes was to layer different colours on top of one other. QR codes were utilised in marketing, warehouse management, and product tracking, among other applications. QR codes' colour coding significantly enhanced data capacity by three times that of regular QR codes, while the QR code's covert nature offered more protection. To boost the data capacity of the QR codes, the six base colours were used.
For the development of intelligent systems, Shen et al. (2014) presented a resilient QR code image. The advancement of information technology led to the creation of the QR code, which has since been utilised in a variety of applications. A new technology for automatic identification appeared in the form of the QR code. Rungraungslip et al. investigated how the picture of the QR code could be improved using the retinex theory (2012). The location and correction approach, which was based on the chain code tracking algorithm, were also proposed. For identifying and extracting the QR code, the rectification approach incorporated the morphological elements of the QR code. The results of the experiment reveal that the proposed method was successfully employed to extract QR code images from the backdrop.
Vongpradhip&Rungraungsilp (2012) proposed an invisible watermark that contained a QR code. The DCT was employed to conceal information within the QR code group. The QR code was split down into several frequency bands and compared to the mid-band coefficients using a block DCT based approach. The coefficients were hidden in the middle frequency bands using invisible watermarking techniques.
With the help of the watermark extraction system, the watermark from the QR code was extracted. The information in the QR code was preserved using an invisible watermark within the QR code. Increase the protection of information on the internet and in the media by employing the Barcode, as was done with the digital watermark in the field of security.
Baik (2012) presented a novel perspective on QR code-based applications and activities for accessing information in the human environment. The QR code served as an ambient media gate since it demonstrated a new method of accessing the internet. When the architecture of QR codes matured, the retrieval of information was altered. The barcode technology has been applied in a variety of sectors, including:

- Logistics
- Merchant Management
- Customer Management, etc.

To combat the interruption of existing portals, the proposed analogue portal service was aimed at the internet portal market. Existing Internet portals have a strong monopolistic sort of position built in.

III. VISUAL CRYPTOGRAPHY

Within the security area, cryptography has a long and fascinating history. The handling of sensitive photographs containing classified information is a top priority in various departments, such as the military's distribution of maps via the internet and many other business industries. Various image secret sharing techniques have been developed to address the security issues with sensitive photographs. Visual cryptography (VC) is a technology invented by Naor and Shamir [1] in 1995 to manage secret picture exchange.
VC is a method of encrypting a secret image containing confidential visible information in such a way that the decryption may be performed entirely by the human visual system (HVS) without the use of computers. Any visual information, such as printed text, handwritten notes, and photographs, can be encrypted using VC. It removes the need for sophisticated computation during the decryption process, and the photos can be restored by stacking the shares. It combines the features of creating flawless cyphers and exchanging secrets in cryptography. The secret image is typically separated into two or more portions. The secret images are recovered when the required number of shares are printed on transparencies and then superimposed.

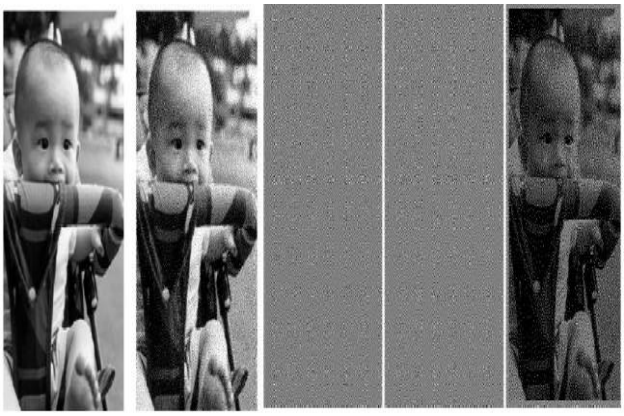

Figure 2: Original image, Halftone, Share-1, Share-2 and Decrypted image

Naor et al. [1] introduced the technique of VC in which the binary image is decomposed into n number of shares. Figure 2 shows an example of share creation and recovery of a secret image using visual cryptography. In the scheme of *(k,n)*, shares

when stacked over one another reveals the original secret image. Naor scheme is quite suitable for a binary image. The shares created in the original image are determined by randomly selecting pairs of sub-pixel matrices for black and white pixels [2]. VC scheme suggested by Naor et al. [1] requires no computer participation in any situation for decryption. Visual cryptography combines the notion of the perfect secret with a random image for the purpose of secret sharing [3]. The next section describes the common characteristics of VC schemes.

IV. QUICK RESPONSE CODE

A QR code, also known as a matrix code, is a two-dimensional encoding of data. This machine-readable matrix code is made up of black and white squares. It can store URL (Uniform Resource Locator) information, contact information, links to movies or photographs, simple text, and much more. [13]
Architecture of QR Codes Each QR code symbol has a square pattern to it. There are two regions in this square pattern: the encoding region and the function patterns. The location where the encoding region indicates the data encoding is the focus of the function patterns.
The structure of the QR code symbol is shown in Figure 1. Finder patterns, timing patterns, and alignment patterns are all part of the function pattern. Finder patterns are three frequent structures found on the three corners of a QR code symbol. The Finder pattern is used to determine the symbol's proper orientation. The decoder software uses timing patterns to determine which side of the pattern to use. In the case of image distortion, alignment patterns are utilised to ensure that decoder software accurately decodes the symbol. Other than the function pattern, the rest of the region is the encoded region, which stores data code words and error correcting code words [16]. The quiet zone is the distance between the QR code and its surroundings. It is necessary for the scanning application to function properly.

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. METHODOLOGY

An overview of the proposed scheme is shown in Figure 3. In Figure 3, designing matrix sets of (k, n) probabilistic sharing and method of embedding are two key points of our study.

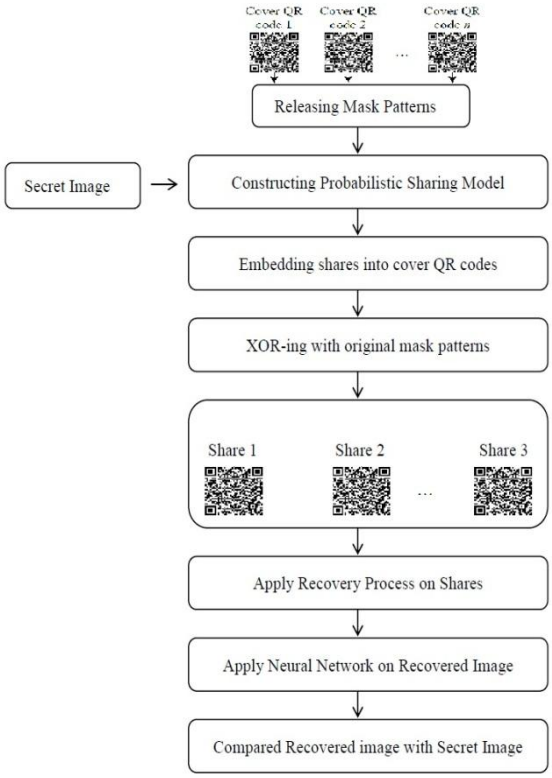

Figure 3: Illustration of the proposed scheme

A. Design of Matrix Sets

Figure 4exhibits the processes to construct matrix sets. By specifying equivalent relationship among participants, the initial collection is divided into several sub-collections. Then, basic matrices for each sub-collection can be obtained with two matrix units $M_{k,even}$and $M_{k,odd}$. After that, we connect these basic matrices and transform the result into the final matrix sets.

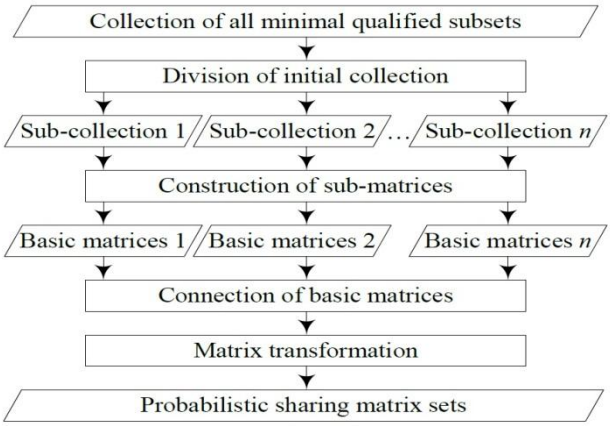

Figure 4: Processes of constructing probabilistic sharing sets

B. Design of Embedding Method

After initial sharing, meaningful shares are supposed in this section. According to [12], any QR code has a determined data and error correction capacity if its version and error correction level are given. In most cases, all code words of a block include three parts, as shown in Figure 5.

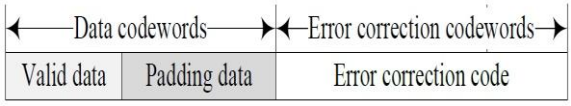

Figure 5: Three parts of data and error correction code words

To obtain the message of a QR code, valid data cannot be modified since it concerns all useful information of decoding. Padding data are added to fill encoding redundancy and error correction code words are designed to restore original data even if some errors exist. By analysis, we will use padding data to design meaningful shares.

First, the size of cover QR codes is determined. Suppose the original shares are T_{r1}, T_{r2}, ,$T_{rn}$with the size of $a \times b$. We calculate the least number of data code words.

$$s = (I_0 + a \times b)/8 \quad (1)$$

With a given error correction level, we can infer the required version h of QR codes. Further, check whether the region size of padding data is adequate for embedding an original share. If not, $h = h + 1$ until the size is large enough.

Next, embed original shares into their covers C_1, C_2,…, C_n. Suppose the top left corner of embedding region is (p, q). For any module $C_k(p + i - 1, q + j - 1)(1 \le i \le a, 1 \le j \le b, 1 \le k \le n)$, if it is a padding data, let

$$C_k(p + i - 1, q + j - 1) = T_{r_k}(i, j) \quad (2)$$

Finally, recalculate error correction code words for current data code words. Then, final messages before XOR-ing mask patterns are prepared, after error correction applies recovery process on shares then apply Neural Network on recovered image. At last here recovered image compared with secret image.

VI. Results and Analysis

Illustration of the proposed scheme, firstly select QR code image as cover image then it convert to Grayscale image.

1. **Select QR code image as cover image**

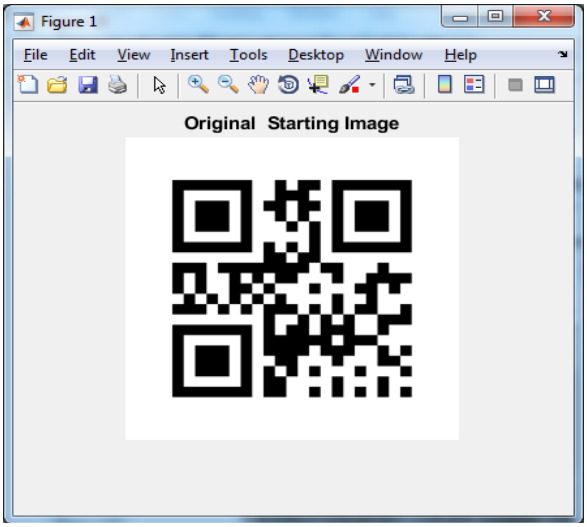

Figure 6: Original Starting Image

Figure 6 shows as original QR image as cover image and figure 7 shows a Grayscale QR image as cover image.

2. **Grayscale QR image as cover image**

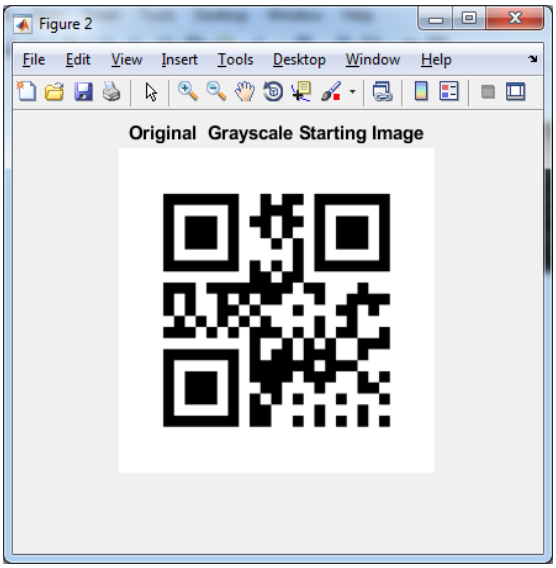

Figure 7: Original Grayscale Starting Image

3. **Image to be hidden into QR image (cover image)**

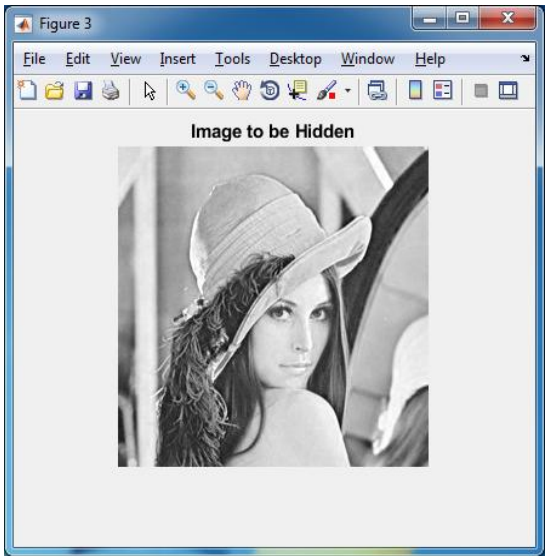

Figure 8: Image to be hidden into QR image

4. **Encrypted Image using Key**

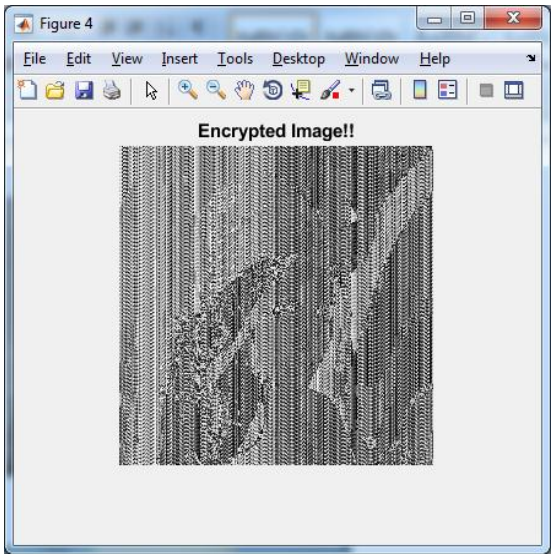

Figure 9: Encrypted image using Key

5. **Generate n-shares of image:** Since n = 3. So the 3 shares will be generated.

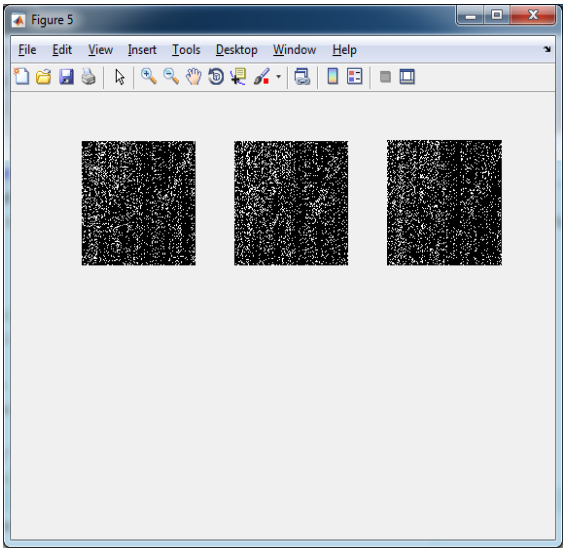

Figure 10: Generate n-shares of Image

6. **Generated watermarked images of all 3 shares**

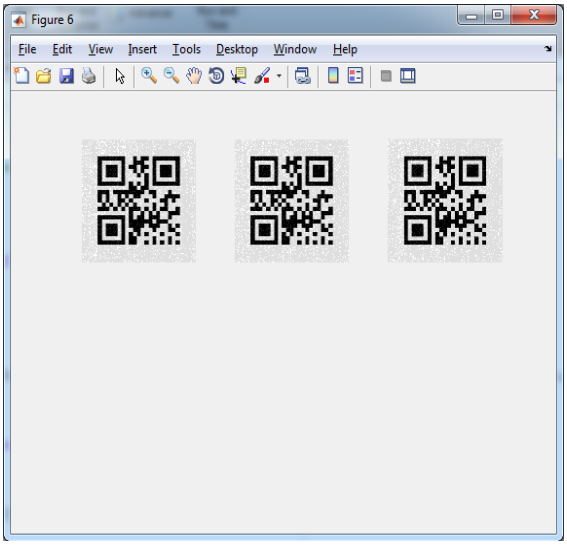

Figure 11: Generate Watermarked image of all 3 shares

7. **Recover watermark image from watermarked images of all 3 shares**

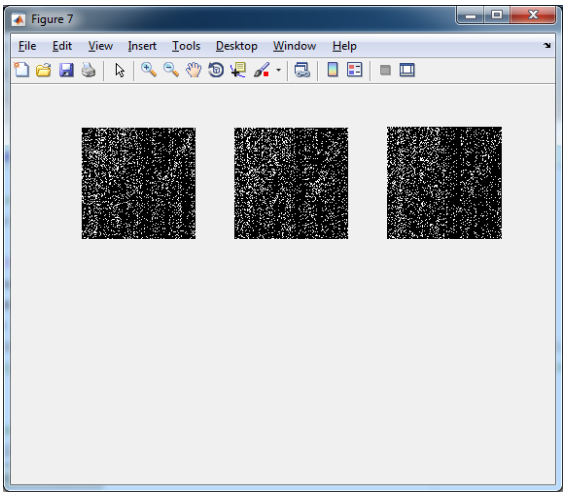

Figure 12: Generate Recover watermark image from watermarked images of all 3 shares

8. **Merged k shares**

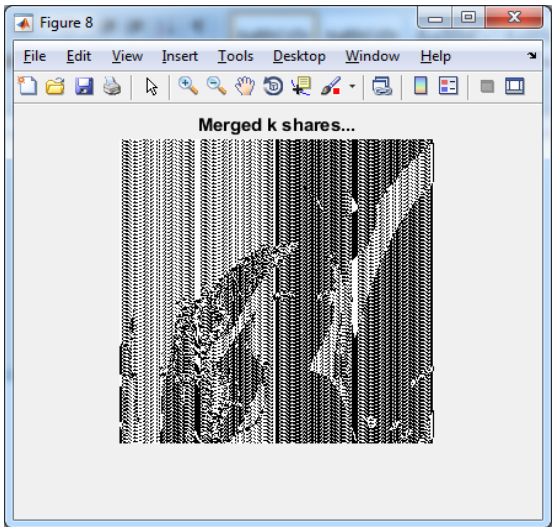

Figure 13: Merged k shares

9. Recover the secrete image

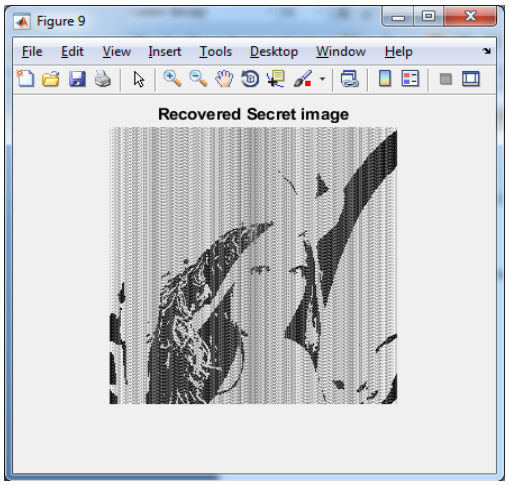

Figure 14: Recover the Secrete Image

10. Apply ANN to enhance the secret image

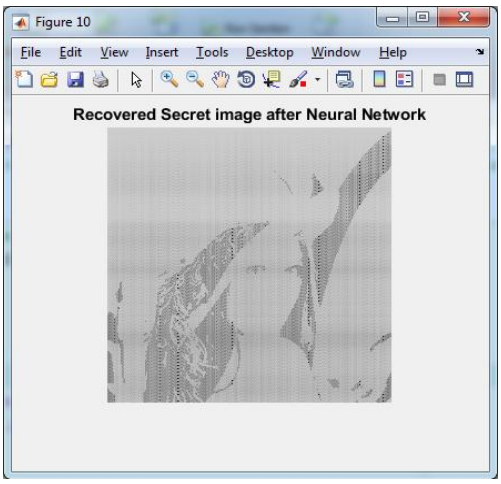

Figure 15: Recovered Secret Image after Neural Network

- The Peak-SNR value of Base is 29.3373
- The Peak-SNR value of Propose is 49.5135
- The Relative Difference value of Base is 0.4980
- The Relative Difference value of Propose is 0.4992

Figure 8 shows Image to be hidden into QR image as a cover image, Figure 9 shows Encrypted Image using Key, Figure 10 shows Generate n-shares of image, here n=3 and Figure 11 shows Generation watermarked images of all 3 shares. Figure 12 shows Generate Recover watermark image from watermarked images of all 3 shares, Figure 13 shows recover the Secrete Image and Figure 14 showsRecovered Secret Image after Neural Network.

11. Image after relative difference of base algorithm

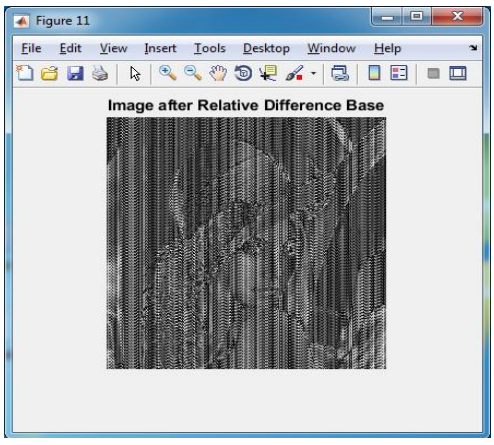

Figure 16: Image after Relative difference of base algorithm

12. Image after relative difference of proposed algorithm

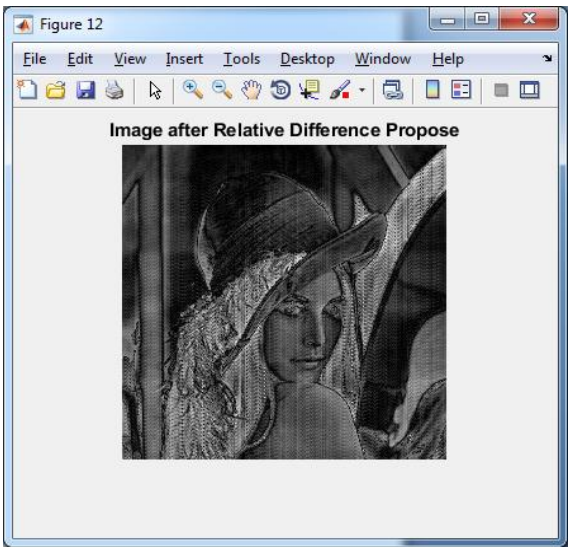

Figure 17: Image after Relative difference of proposed algorithm

In figure 16 shows Image after relative difference of base algorithm and figure 17 shows Image after Relative difference of proposed algorithm.

VII. CONCLUSION

The privacy of the information stored is safeguarded because it can only be accessed by authorised employees. At the same time, anyone eager to help has access to the essential information needed to assist the participant in an emergency. The system's robustness can be determined by the fact that it necessitates the use of highly secure instruments such as a mobile phone with a camera, a QR Code, and an application to scan the QR Code. As a result, unlike other systems with extensive infrastructure, there is no risk of the system failing. The technique is generic and can be used in any location where a big number of people are gathered.

This paper offers a new (k, n)-VCS in which each share is a legitimate QR code with a specified meaning. When shares are delivered through public channels, it minimises the risk of being suspected by potential attackers. Furthermore, even when shares are incorporated, the error-correcting capabilities of cover QR codes are kept. In terms of practical applications, our approach can be used to check the security of QR codes obtained from unknown sources. Despite the fact that we employed the probabilistic strategy to avoid pixel inflation, the hidden image's size is still limited. The question of how to improve the secret payload of QR codes remains unsolved.

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] Arumugam, S., Lakshmanan, R., & Nagar, A.K. (2014, Apr.). On (k, n)*-visual cryptography scheme. Designs, Codes and Cryptography, 71(1), 153-162.

[6] 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.

[7] 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.

[8] Liu, F., & Wu, C. (2011, Jul.). Embedded extended visual cryptography schemes. IEEE Transactions on Information Forensics and Security, 6(2), 307-322.

[9] 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.

[10] 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.

[11] ISO/IEC 18004:2015. (2015). Information - Automatic identification and data capture techniques - QR Code barcode symbology specification.

[12] Yang, C. N., Liao, J. K., Wu, F. H., & Yamaguchi, Y. (2016, Aug.). Developing visual cryptography for authentication on smartphones. In Wan J., Humar I. & Zhang D (Eds.), 2016 International Conference on Industrial IoT Technologies and Applications: Vol. 173. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (pp. 189-200). Berlin Heidelberg, Germany: Springer-Verlag.

[13] 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.

[14] 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.

[15] 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.

[16] 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.