Steganography with Visual Secret Sharing Scheme Based QR Code Application

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—**Visual Cryptography (VC) is based on the idea of breaking the original secret image into several partitions called as shares and decrypting with the human visual system. Given the security aspect of the hidden sharing system, security is lacking in Visual Cryptography shares. Previous related research has demonstrated the possibility of cheating VC by various methods. Attackers can complete both the cheating and the modification of the VC process without the VC participants being noticed.**
Over the past few years, the visual cryptography scheme has attracted considerable research interest and has grown rapidly due to its easy decryption. Signless shares, however, remain a continuing obstacle for VCS to its realistic applications. In this work , we propose combining a (k, n)-VCS with QR codes. Probabilistic sharing model is used to expand the maximum allowed size of secret image. On the basis of this, the method of secret sharing is presented with high relative difference applying ANN to enhance the secret picture. In addition, we use encoding redundancy to embed the initial shares into covers QR codes. Every share is meaningful after that, and can be read by any regular reader of QR code. Unlike previous work, the capacities of the covers for error correction are perfectly preserved. This highlights that the protection of QR codes from some unknown sources can be authenticated using our scheme. Lastly, experimental results and comparisons are provided to demonstrate the viability and benefits of the proposed scheme.

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

I. INTRODUCTION

Digitalisation has the biggest potential to change our way of living. Security is a major concern in today's digitalised world era. As information is delivered from node to node over the network, security issues begin to become apparent. There has been an increase in the number of threats at a broader pace and strong security measures need to be used.
With the advent of location-conscious mobile technology it has become easy to provide precise context-conscious information for those in need at a critical time. This technology can be used in combination with barcodes to provide accurate and critical information to people in a crowd who may need it to deal with emergencies such as stamping, health issues, rioting, overcrowding, accidents, etc. At the same time, the security and privacy of the providing information should not be violated.
This research work presents a stable, real-time system based on Quick Response Code specifically designed for any crowded environments where people are required to be assisted by providing contextual information to navigate to their respective destinations. The same program can also be applied for any other situations such as major exhibits, airports, shopping malls or even battlefields where a person is likely to get lost or need guidance. The data is compressed, encrypted and encoded in QR code afterwards.
Cryptography is one of the prime methods for providing security of information. Huge computational power and complicated algorithms are common in traditional cryptographic methods which take a lot of time and money to encrypt and decode a secret message.
Visual Cryptography [1-3] is a secret sharing scheme that takes a secret image as input (i.e. printed, handwritten) encrypts the input image into a set of other images called shares in such a way that shares are printed on transparencies and superimposed or staked over each other. Simplest visual cryptography or visual secret sharing scheme considers binary image as input, and deals separately with each and every pixel.
Visual cryptography scheme[1] (VCS) is a kind of technology for the sharing of images which Naor and Shamir initially proposed. VCS 'basic model is to disperse a hidden picture into a set of shares. The secret can be decrypted visually by stacking any qualified subset of shares, while prohibited subsets can not. Due to low-computation decryption, VCS has attracted a lot of research attention and related studies have been continuously investigated including promotion of recovery effects[2-4], versatility of access structure[5], color extension of image[6] and enrichment of sharing strategy[7]. Nonetheless, shares in most schemes are worthless, which would easily lift the suspicion of attackers when communicating via public networks, and further, the difficulty of handling such shares is increased.

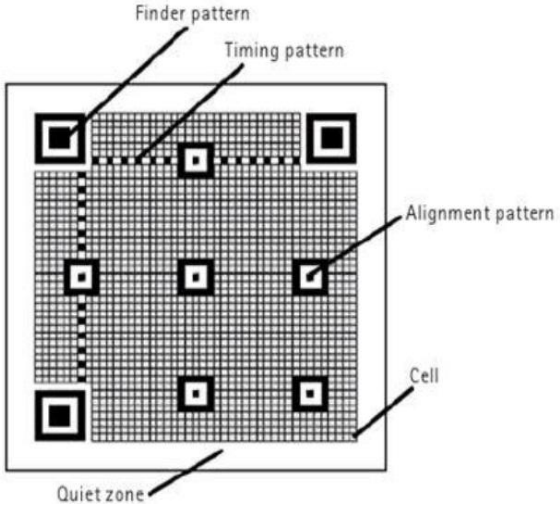

Figure 3.1: Structure of QR code

[1,8] added several columns to the base matrices to generate meaningful shares. Those extra columns were used to hold each share 's cover details. [9] has incorporated halftone technology into the design of schemes for better visual effect. Nevertheless, the shares with low visual effect still had much noise noticeable. QR code is a type of machine recognition code developed by the Japanese Denso Wave Company, and has now been adopted as an ISO universal specification[10]. QR code has been widely used with the development of intelligent handset technology in applications such as advertising marketing, electric identification, and mobile payment. Because of the low visual recognition feature, it's almost impossible to acquire a QR code message through human vision. The QR code, in effect, can be an excellent mask for VCS since its dark and light modules are distributed evenly with a random look. The variations of the VCS and QR codes have therefore been examined considerably[10]. A scheme of two-level information storage was proposed, based on the characteristic of machine recognition[11].

Decoding shares were uncomfortable in that scheme unless a scanning distance and angle were considered to be quite acceptable. And then, using the error correction mechanism of QR codes[12], a (n, n) sharing system was conceived. Later, a (k, n)-VCS was implemented under the theory of random grids[13] in[14], where the relative difference of the recovered secret requires further improvement. ANN to enhance the hidden picture applies in this work. In addition, the shares' error correction capacities were reduced in [14] as some code words were changed during the sharing process. That can affect the robustness of the QR codes to damage or loss symbols.

In this job, we propose combining a (k, n)-VCS with QR codes. We present a method of constructing sharing matrix sets by classifying all minimally eligible subsets. This design is based on the model of probabilistic sharing, of which the unexpanded property allows for larger secret size and applying ANN to enhance the secret image. In addition, it can achieve better, or even good, recovered efficiency. In addition, we use the encoding consistency of QR codes to insert initial shares into their respective covers. Finally, it obtains a number of meaningful shares. In this work, error correction capabilities are completely conserved compared to previous research. Experimental results and comparisons show that the proposed scheme is successful.

II. Literature Review

Specific literature relating to the progressive collapse of the building structures is reviewed and a brief review is given below. Pandya&Galiyawala (2017) surveyed the Research and Application QR codes. The QR code was the type of matrix barcode, developed by the Denso Wave in Japan for the automotive industry. The QR codes, as opposed to the UPC barcodes, have easy readability and greater storage capacity. The details of the QR codes, their real-time implementations in everyday life, are worked out in this study. The QR codes were the appropriate tool for conversing the URLs to the user quickly and efficiently, with the help of mobile phones. The QR code contains both the architecture and the encoding. The patterns of functions were not used for the data encoding. The QR code protocol comprises 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.

This 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. By removing the noise, the decoding stage's efficiency was improved by using the median filter to convert the image to the binary image. 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 several projects to enhance information protection, enhance identification, 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 primarily aimed at layering the QR codes with various colors. The QR codes have been used in a variety of applications including marketing, inventory management and stock 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 to develop smart systems with a robust QR code image. 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. (2012) analyzed the picture of the QR code based on the retinex theory. Also proposed was position and correction method, which was based on the algorithm for chain code monitoring. 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.
Vongpradhip&Rungraungsilp (2012) suggested a QR code, built into an invisible watermark. The DCT had been used to hide information within the QR code community. Using the block DCT based method the QR code was broken down into the different frequency bands and correlated with the mid-band coefficients. The coefficients were inserted into the middle frequency bands using the transparent watermarking techniques.
The technique for extracting the watermark from the QR code was performed using the extraction system for the watermark. The invisible watermark inside the QR code has been used to protect the details in the QR code. Information on the internet and the media should be secured by increasing security through the use of the Barcode, which was achieved in the security field with the digital watermark.
Baik (2012) introduced a new view of the applications and the activities that use the QR code to access human environment information. The QR code was an ambient media gate, as the new way to access the internet was shown. Recovery of knowledge was updated when the QR codes technology matured. The barcode technology has been used in many areas, such as:

- Logistics
- Merchant Management
- Customer Management, etc.

The proposed analog portal service was targeting on the internet portal market to tackle the disruption of the existing portals. The existing Internet portals has a strongly built in monopoly type of positions.

III. VISUAL CRYPTOGRAPHY

In the security domain cryptography has a long and interesting history. The management of classified photos that contain proprietary information is of key concern in many agencies, such as the exchange of maps in the military and several other commercial sectors over the internet. Various hidden image sharing systems have been developed to manage the security problems of sensitive pictures. Naor and Shamir[1] created one of the techniques called Visual Cryptography (VC) in 1995 to manage hidden image sharing.
VC is an method in which a hidden image containing sensitive visible information is encrypted in a completely safe way, 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 making flawless ciphers and exchanging secrets in cryptography. In general, the hidden picture is divided into two or more parts known as shares. When the number of shares required is imprinted on transparencies and then superimposed, the secret images are recovered.

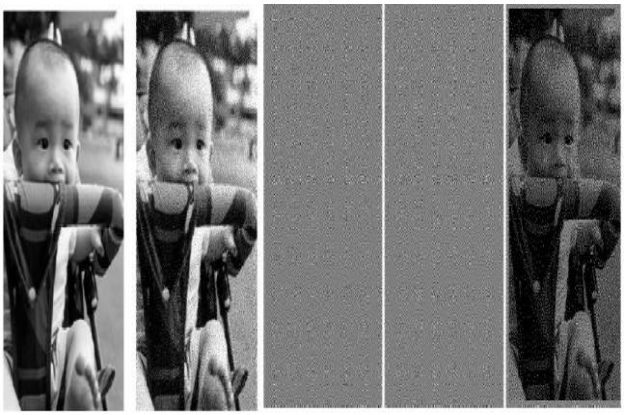

Figure 2: Original image, Halftone, Share-1, Share-2 and Decrypted image

Naor et al. [1] introduced the technique of VC in which the binary image is decomposed into n number of shares. Figure 1.1 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

QR code is a two-dimensional information encoding, which is often 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 images, plain text and much more. [13] [14]

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.

Figure 1 displays QR code symbol structure. 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. 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 function pattern, is the encoded area where words of data code and words of code that correct error are stored[16]. 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. 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.

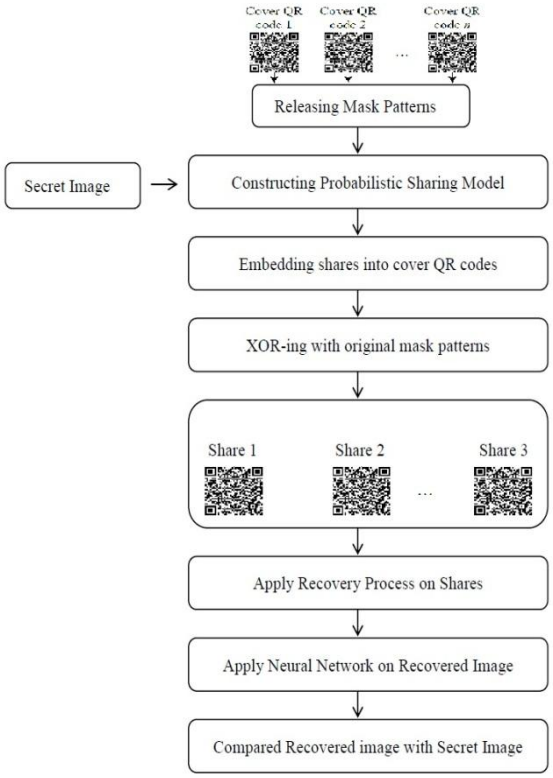

Figure 3: Illustration of the proposed scheme

A. Design of Matrix Sets

Figure 4 exhibits 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.

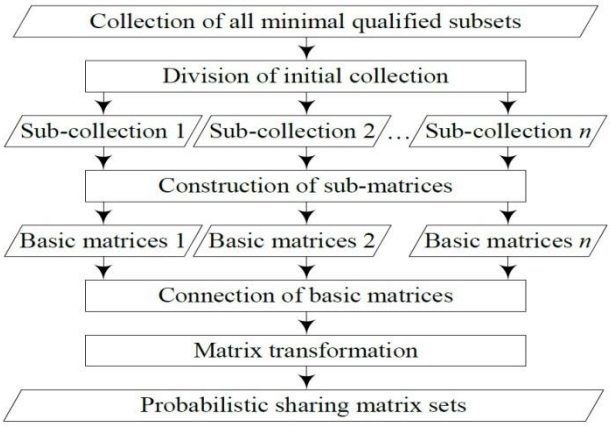

Figure 4: Processes of constructing probabilistic sharing sets

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.

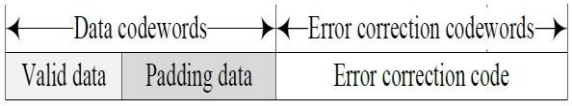

Figure 5: Three parts of data and error correction code words

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 [17].

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

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 [18].

VI. Results and Analysis

This work following figure 3, 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**

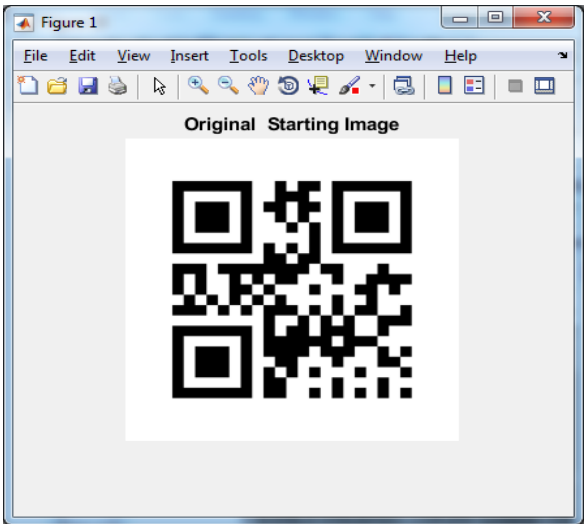

Figure 6: Original Starting Image

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**

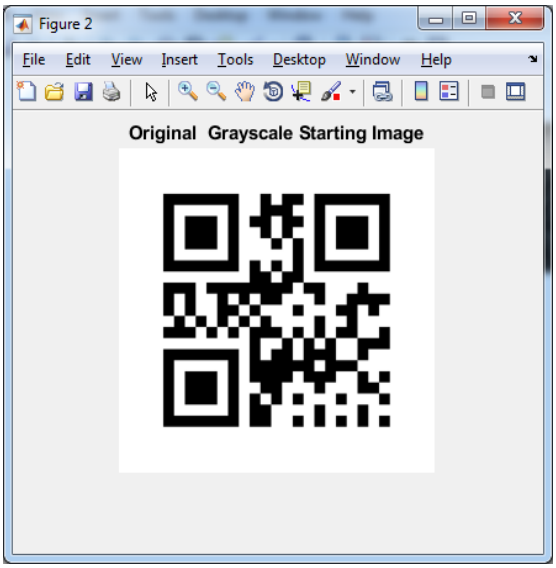

Figure 7: Original Grayscale Starting Image

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

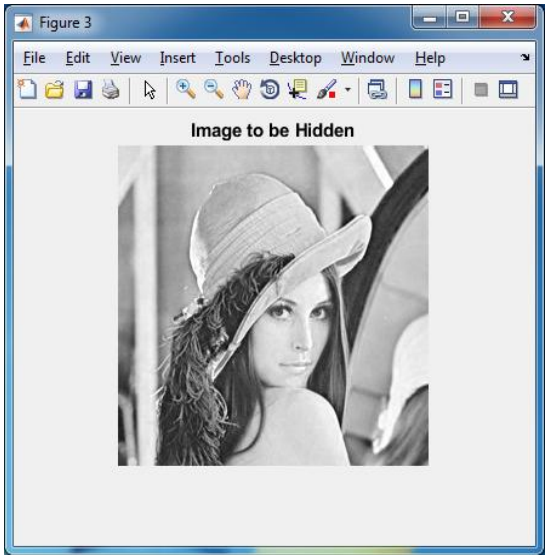

Figure 8: Image to be hidden into QR image

4. **Encrypted Image using Key**

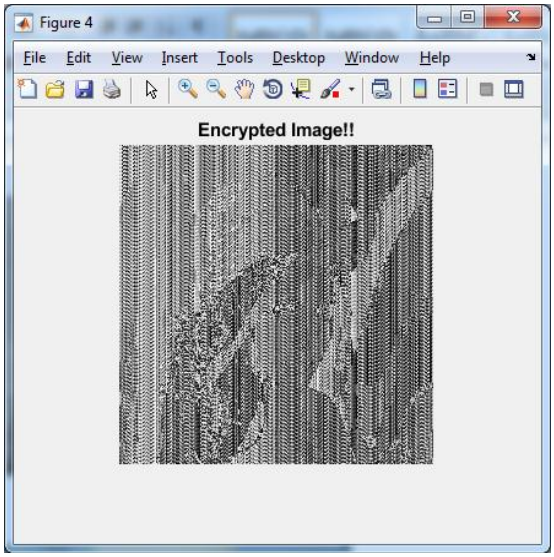

Figure 9: Encrypted image using Key

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

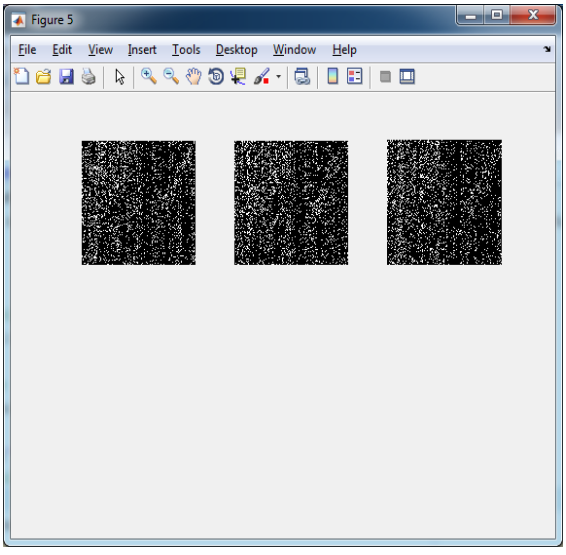

Figure 10: Generate n-shares of Image

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

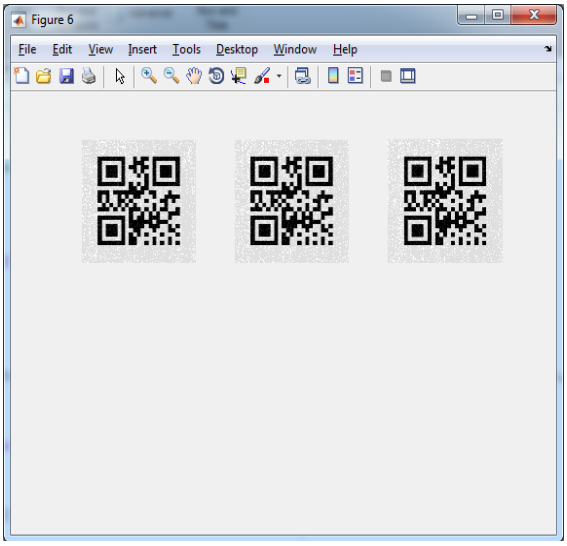

Figure 11: Generate Watermarked image of all 3 shares

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

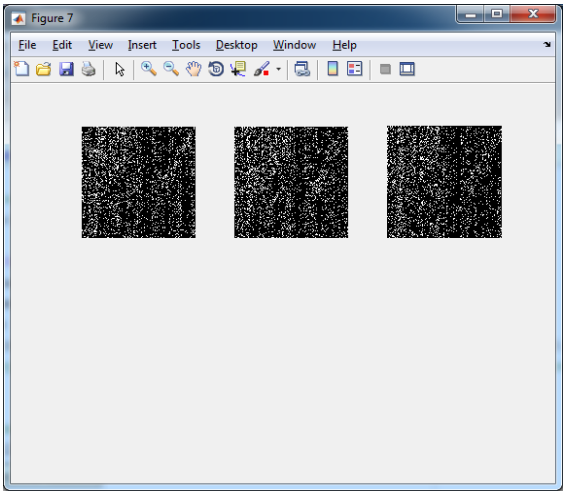

Figure 12: Generate Recover watermark image from watermarked images of all 3 shares

8. **Merged k shares**

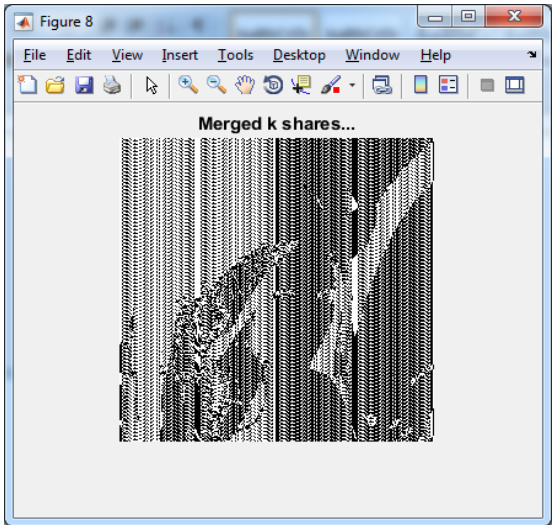

Figure 13: Merged k shares

9. **Recover the secrete image**

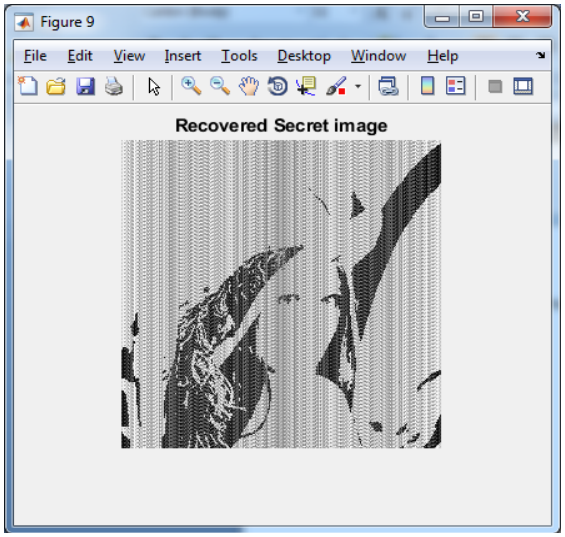

Figure 14: Recover the Secrete Image

10. Apply ANN to enhance the secret image

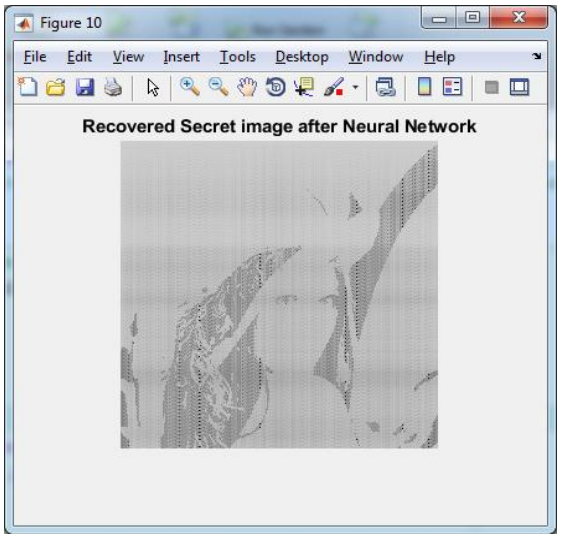

Figure 15: Recovered Secret Image after Neural Network

- 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 shows Recovered Secret Image after Neural Network.

11. Image after relative difference of base algorithm

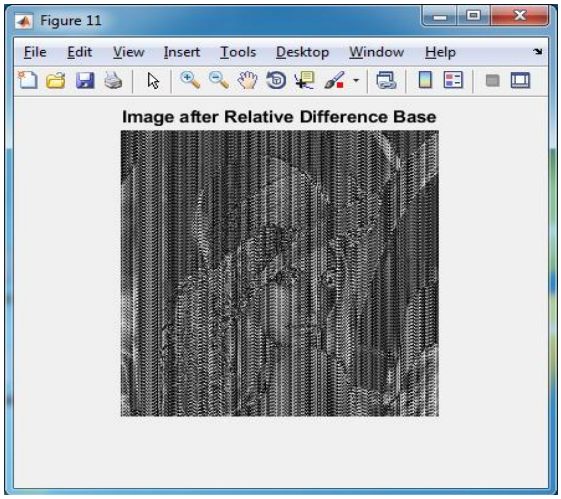

Figure 16: Image after Relative difference of base algorithm

12. Image after relative difference of proposed algorithm

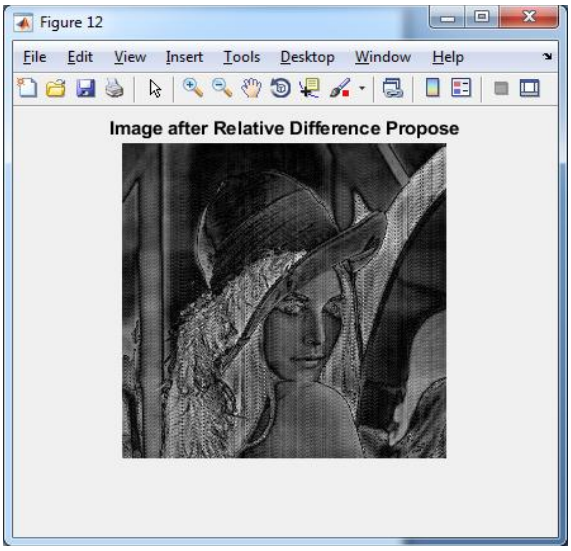

Figure 17: Image after Relative difference of proposed algorithm

At last 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 stored information is secured, as only the authorized personnel can retrieve this information. At the same time, the basic information required to assist the client during emergencies is accessible to anyone willing to assist. The system's robustness can be calculated by the fact that it needs very simple tools such as a camera-equipped mobile phone, the QR code and a QR code scan program. Hence, there is no fear of system breakdown as in the case of other systems with huge infrastructure. The program is standardized, and can be applied anywhere large numbers of people are gathered.

This work proposes a novel (k, n)-VCS in which all the shares are valid QR codes with a specific significance. It reduces the likelihood of potential attackers being accused when the shares are spread across public channels. Additionally, the capacities of cover QR codes to correct errors are maintained even when shares are embedded. Our scheme can be used to evaluate the protection of some QR codes from unauthorized sources, despite practical applications. Because we used the probabilistic method to implement no expansion of pixels, the size of secret image is still small. How to boost QR codes' hidden payload remains an open problem to overcome.

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.
[17] 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.
[18] 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.