An Intelligence System for Visual Cryptography Technique Relying on QR Codes

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— **Visual Cryptography (VC) is based on the fundamental idea that the original secret image must be segmented into many different sections before the human visual system can be used to decrypt the image. Visual Cryptography, on the other hand, contains vulnerabilities in spite of the fact that the method for exchanging secrets is foolproof. Previous research has shown that it is possible for VC to cheat using a variety of different techniques. Cheating and changing the rules of the VC process can be done covertly by attackers without attracting the attention of other participants.**

Visual cryptography has received a great deal of interest from the academic community in recent years and has made significant headway as a result of the ease with which it may be decrypted. Meaningless shares, on the other hand, remain to be a barrier to the practical implementation of VCS. In this article, we propose combining a (k, n)-VCS with QR codes into a single system. Increasing the maximum size of the secret image that can be shared is accomplished through the utilization of the probabilistic sharing approach. On the basis of this, a method for sharing a secret that has a high relative difference is defined, and artificial neural networks are utilized to improve the secret image. In order to insert the initial shares onto the cover QR codes, we also make use of encoding redundancy. After that, each sharing has its own significance, which can be deciphered using any QR code reader. In contrast to the work that came before, the error-correcting powers of the covers have been preserved in their entirety. It highlights the fact that our method may be used to verify the safety of QR codes collected from unidentified sources. In conclusion, both experimental data and comparisons are shown in order to establish the viability and benefits of the proposed strategy.

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

I. Introduction

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.

The cryptography scheme [1] (VCS) is a type of technology that allows for the exchange of images. It was initially conceived of by Naor and Shamir. Distributing a confidential image among a number of shares is the fundamental tenet of the VCS paradigm. By stacking any qualified subset of shares, it is possible to visually decode the secret, however it is impossible to do so with banned subsets. VCS has received a significant amount of attention from researchers as a result of its low-computation decryption, and related studies have been continuously investigated. These studies include the promotion of recovery effect [2-4], the flexibility of access structure [5], the extension of image colour, and the enrichment of sharing strategy [9-11]. However, shares in the majority of schemes are meaningless, which makes it simple for attackers to become suspicious when information is transmitted over public channels. In addition, the management of these shares causes a greater degree of inconvenience. In order to provide significant shares, the basis matrices in [2] were expanded by adding some columns. The cover information for each share was carried in these additional columns, which were added for that purpose. Technology that uses halftones was incorporated into the design of the schemes [6] so that the aesthetic effect would be improved. Despite this, there was still a great deal of visible noise in the shares, which resulted in a bad visual appearance.

Naor and Shamir [1] announced the establishment of VC, which was based on image cryptography. After stacking a sufficient number of shared photos, the method of encrypting the original image into shared images will definitely reveal the hidden message or image of the original image [6]. To put it another way, the goal is to generate shared images that are derived from the original image simply by turning each pixel to a pattern that looks like noise or grey [7]. Now we will teach the fundamentals of VC as well as how to change VC.

The first thing that needs to be done is develop an original image that contains a hidden message. For instance, the original version of figure 2 has the coded message "9768" somewhere in the image. White and black are the colours that should make up the image. In point of fact, research on VC had already been done to encrypt halftone images in addition to colour images. However, we describe the fundamentals of VC as they pertain to this paper.

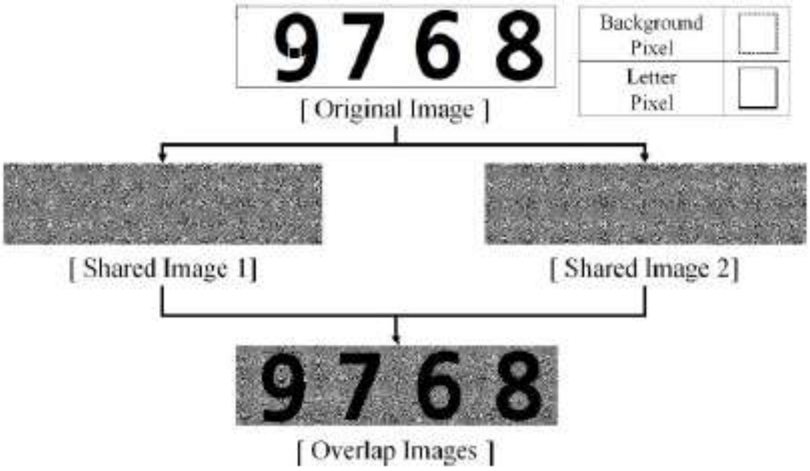

Figure 1: Visual Cryptography Process

For the purpose of encryption, it is necessary to prepare some patterns that can modify an original image. The designs are made up of pixel elements that are laid together in a grid that is 2 * 2. The bottom half of four pixels are made completely opaque, while the top half of the remaining subpixels are made transparent. This rule results in the creation of six different patterns: two horizontal shapes, two vertical shapes, and two diagonal shapes such as the second row of figure 3. Only the shapes can be used to build shared images that are based on VC. In practise, VC selects pixels at random from the original image and changes them all to one of the shapes before filling the shared image with those shapes. When this occurs, the shared images appear to be a shade of grey to human sight because the subpixels of the forms transform into noise consisting of a random combination of patterns that are made up of black and white.

On the other hand, the approach that is used to construct the subpixels of the backdrop and the message in the shared image has to be switched to the opposite manner. You should refer to the background pixel matrix in figure 3 if you want to convert a pixel from the background of the original image into one of the patterns used to generate the shared image [11].
For instance, if a background pixel in the original image is converted to pattern no. 3, which is determined at random, then the subpixels of the position in the first shared image (share 1 in Fig. 2) should appropriately form a left-vertical pattern. In the event that a second image is shared, the subpixels that are located in exactly the same place should have the same pattern. When all of the backdrop pixels of the two shared photos have been formed using this procedure, the backgrounds of the shared images that are going to be overlapped appear to be a grey that is constructed using black and transparent.

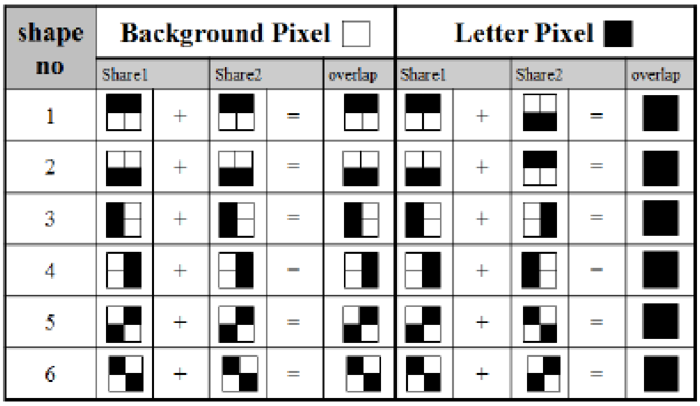

Figure 2: Process to make pixel pattern in shared image

In a similar fashion, the message portion of the shared image is generated in line with the matrix of message pixel shown in figure 3. If a message pixel in the original image is randomly changed into a diagonal pattern (shape no. 5), then the subpixel of the first shared image should set the left-diagonal pattern exactly at the spot where the message pixel was. Another image that has been shared has to have an atypical shape defined for it at the same spot. By doing so, the entirety of the message section of the shared photographs is filled. Because transparent pixels are overwritten by the black of the pattern in another shared image and seem as black, the pixels of the secret message component of one of the photos turn black when the two images are correctly stacked on top of one another.

The conclusion reveals that the shared image 1 in figure 2 appears grey. The similarities between the first shared image and the second shared image are illustrated in Figure 2 below. Nevertheless, the secret message "9768" and the rules for constructing the shared image are never disclosed in any image that is shared. Only when both photos that were transmitted are superimposed on one another can the view of a human validate the message, as shown in the bottom picture of Figure 2. You will not be able to view the message at all if the photographs that have been shared do not match from the beginning to the end, or if even one of the images has been distorted. The fundamental idea is to make use of lettering that has a higher contrast than the background. As a result, VC requires far less processing to encrypt data, yet it doesn't require any computation at all to decode data.

In order to produce meaningful shares, Liu, F., and Wu, C. [8] included several additional columns in the basis matrices. These additional columns were used to store the cover information associated with each share. For a more striking visual effect, [9] incorporated the usage of the halftone technique into the design of the schemes. Despite this, there was still a great deal of noise in the shares, which resulted in an unappealing visual impression. The Japanese Denso Wave Company invented the QR code, which is a sort of machine recognition code that has now been certified as a global standard by the International Organization for Standardization (ISO) [10]. QR codes have become widely utilised in applications such as product advertising, electronic identity, and mobile payment with the development of clever cellphone technology. Due to the fact that QR codes have a low visual recognition feature, it is nearly impossible for human eyesight to understand the message contained within them. In turn, the QR code can be an effective mask for VCS since the dark and light modules are evenly spread and have a random look. As a direct consequence of this, the coupling of VCS with QR codes has garnered a lot of interest [10]. On the basis of the characteristics of machine recognition, a technique including the storage of information on two levels was presented [11].

Using that method made decoding shares difficult, unless an absolutely acceptable scanning distance and angle could be discovered. This was not always possible. Then, a method of information sharing known as (n, n) was developed with the help of the error-checking mechanism that QR codes provide [12]. Later on, a (k, n)-VCS was built in [14] under the random grids theory [13], and there is still room for development regarding the relative difference of the retrieved secret. Within the context of this project, ANN is being utilised to enhance the covert image. In addition, the mistake correcting capacities of the shares were diminished in [14] due to the fact that some code words were altered at various points throughout the method of sharing. Because of this, the QR codes' resistance to symbol damage or loss may be reduced as a result.

In this article, we propose combining a (k, n)-VCS with QR codes into a single system. We provide a method for building sharing matrix sets, which entails classifying any minimal qualifying subsets that may be present. A probabilistic sharing model serves as the foundation for this method. Within this model, the unexpanded property enables a larger secret size, and artificial neural networks (ANN) are used to improve the secret picture. It is also possible to get restored performance that is superior to what was previously achieved, or even flawless. In addition to this, we make use of the encoding redundancy that QR codes provide in order to put the original shares into their respective covers. At long last, a sizeable amount of shares has been acquired. In this study, error correcting capacities have been kept completely intact, in contrast to the work done in the past. The effectiveness of the strategy that has been proposed is proved through experimental data and comparisons.

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.

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 utilisation of these six fundamental hues was necessary in order to increase the data capacity of the QR codes.

Shen et al. (2014) provided a robust QR code picture with the purpose of contributing to the development of intelligent systems. The development of information technology resulted in the invention of the QR code, which has subsequently found use in a wide variety of contexts and context-specific applications. The quick response (QR) code is a new sort of automatic identifying technology that has just emerged. Rungraungslip et al. conducted research into the use of the retinex theory with the intention of enhancing the image of the QR code (2012). The location and correction strategy, which was also proposed, was founded on the chain code tracking algorithm. The rectification method contained the morphological components of the QR code, which allowed for the accurate identification and extraction of the QR code. The findings of the experiment demonstrate that the strategy that was provided was successfully used to extract QR code images from the backdrop.

The watermark contained within the QR code was successfully extracted with the assistance of the watermark extraction system. The information contained in the QR code was protected by an undetectable watermark that was embedded within the QR code itself. Utilizing the barcode in the same way that the digital watermark was utilized in the field of security will allow for an increase in the level of protection afforded to information that is found on the internet and in the media.

Baik (2012) offered an original viewpoint on QR code-based applications and pursuits for the purpose of gaining access to information in the context of the human environment. Due to the fact that it demonstrated a new way to access the internet, the QR code was able to function as a gate for ambient media. When QR codes reached their mature architecture stage, the process of retrieving information was modified. The barcode technology has been implemented in many different industries, including the following:

- Logistics
- Merchant Management
- Customer Management, etc.

The analogue portal service that was suggested attempted to target the market for internet portals in order to compete with the disruptive effects of current portals. Existing Internet portals have a built-in advantage that can be described as monopolistic in nature.

III. Visual Cryptography

People are able to share valuable and confidential information with one another over the network. Some examples of this kind of material are medical reports, military maps, financial records, medical photographs, and QR codes.
The term "secret image" refers to images taken in real time that contain sensitive information (SI). In this day and age of digital communication, the exponential growth and rapid expansion of digital services have compelled us to give serious consideration to the topic of cyber security. In particular in India, where a population of 462 million people are working toward the realization of the dream of a digital India. Over the course of a single second, the network processes millions of pieces of data, including text, photos captured in real time, audio, and video. In point of fact, the issue of safety is one of the most problematic aspects of this overall concept. When conveying a SI, it is vital to take into consideration the SI's level of security, as well as its quality and integrity. Techniques including as encryption, decryption, and information concealment are utilized frequently in the SI protection process.

The Visual Secret Sharing (VSS) technique, also known as Visual Cryptography (VC), is an encoding scheme that was developed by Naor and Shamir. It is employed for the transmission of secret information (SI). VC refers to the technique of encoding SI by splitting it up into a number of shares and relaying the information to a variety of different parties. The decipherable group of humans is the only one capable of recreating the SI. A conventional (k, n) scheme of VC represents that SI is divided into n shares and that a group of k individuals or more with k or more shares can reconstruct the secret image. Reconstructing the secret image requires owning k or more shares. No information can be gleaned about SI from individual shares or from those with fewer than k shares. VC makes it possible for the human visual system to decode SI, in addition to digitally stacking the shares together, which is another method [15].

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 ciphers 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 retrieved.

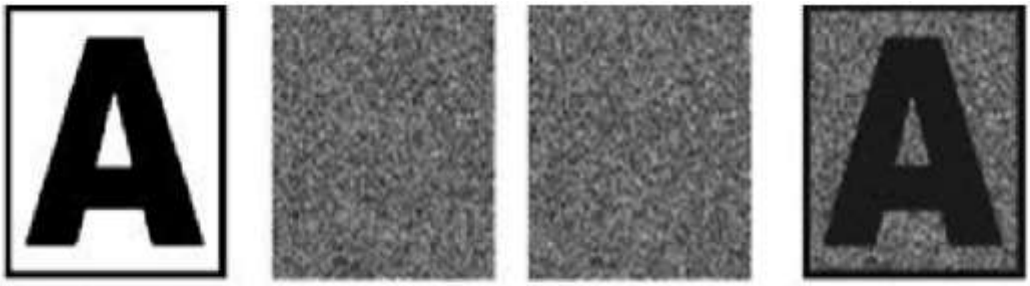

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

Naor et al. [1] introduced the technique of VC in which the binary image is decomposed into n number of shares. Figure 3 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 [12]. 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 [1]. The next section describes the common characteristics of VC schemes.

IV. Quick Response Code

The Quick Response (QR) code is a sort of two-dimensional barcode that was initially developed in Japan for use in the automotive sector. In order to store information quickly and effectively, a QR code makes use of four standardized encoding modes (such as numeric, alphanumeric, byte/binary, and kanji) [8]. Each and every QR Code is made up of an encoding region as well as function patterns [9], which include finder, timing, and alignment patterns. The resilience of the QR code's detection and decoding is ensured by the function patterns, which were built specifically for that purpose. The fundamental make-up of the QR code is depicted in figure 4. In order to detect QR codes and adjust their alignment, three different finder patterns are utilised. Timing patterns are responsible for setting the module coordinates. Adjustment of the distortion requires the application of alignment patterns. The error correction level and the mask pattern are both contained inside the format information regions. In the sections designated for version information, the error correction bits and the code version are both recorded.

The many versions of the QR code are referred to using the form "Version V-E," where "V" refers to the version number (1-40), and "E" refers to the error correction level (L, M, Q, H). The size of the QR code steadily grows from 21*21 modules in Version 1 to 177*177 modules in Version 40, making the total number of modules in the code 177*177. When using the error correction level, it is possible to decode the QR code when anywhere from 7% (L) to 30% (H) of the codewords are messed up [10].

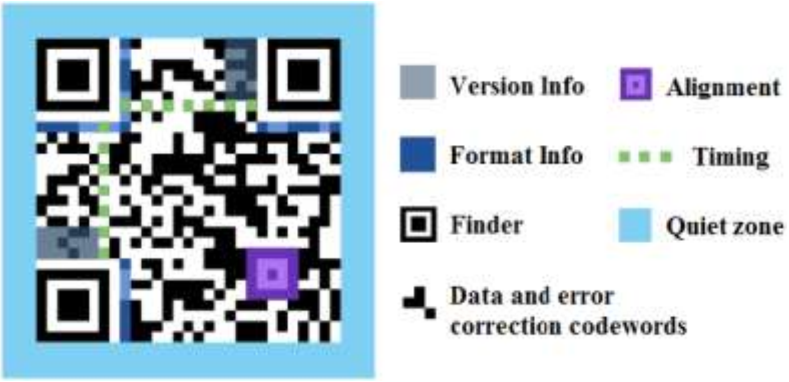

Figure 4: The basic structure of QR code

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 4. 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 utilized 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.

QR Code Attributes and Qualities

1. High Storage Capacity

In comparison to a 1-D barcode, the information that can be stored in a QR code symbol is far greater. A QR code may store up to 7,089 characters of data.

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. It is easier to find the QR code if you use 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 capability to rectify errors is ordered from weakest to strongest, with level L having the weakest capability and level H having the highest [17].

V. Methodology

Figure 3 provides a summary of the overall plan that has been suggested. Two important aspects of our research are illustrated in Figure 3: the designing of matrix sets of (k, n) probabilistic sharing and the method of embedding.

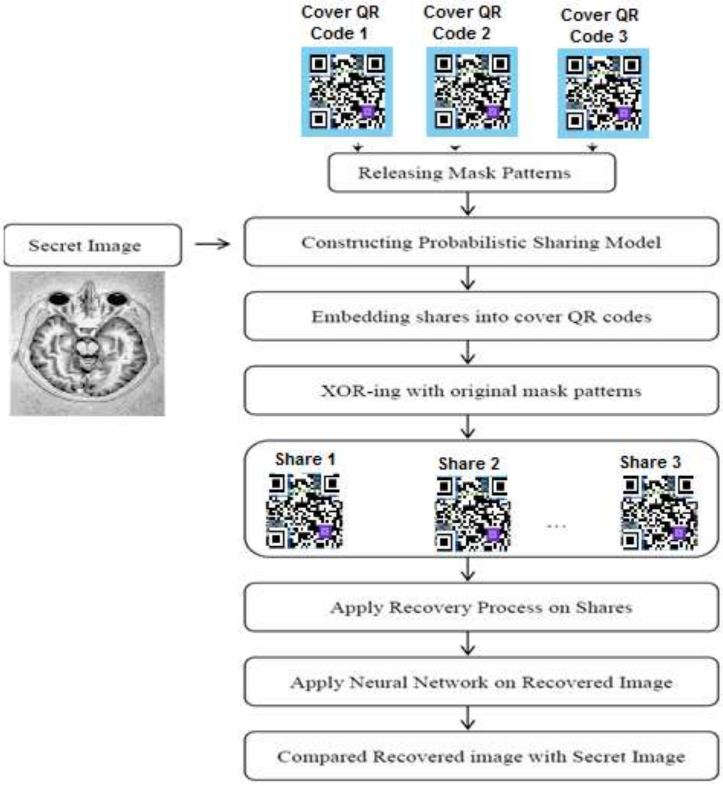
Cover QR Code 1
Cover QR Code 2
Cover QR Code 3
Releasing Mask Patterns
Secret Image
Constructing Probabilistic Sharing Model
Embedding shares into cover QR codes
XOR-ing with original mask patterns
Share 1
Share 2
Share 3
Apply Recovery Process on Shares
Apply Neural Network on Recovered Image
Compared Recovered image with Secret Image

Figure 3: Illustration of suggested approach

A. Development of Matrix-Set Designs

The steps involved in constructing matrix sets are illustrated in Figure 5. The initial collection is then separated into many sub-collections by stating the analogous relationship that each participant has with the other participants. After that, one can obtain the basic matrices for each sub-collection by using the two matrix units $M_{k,even}$and $M_{k,odd}$. Following this step, the foundational matrices are connected, and the result is then transformed into the final matrix sets.

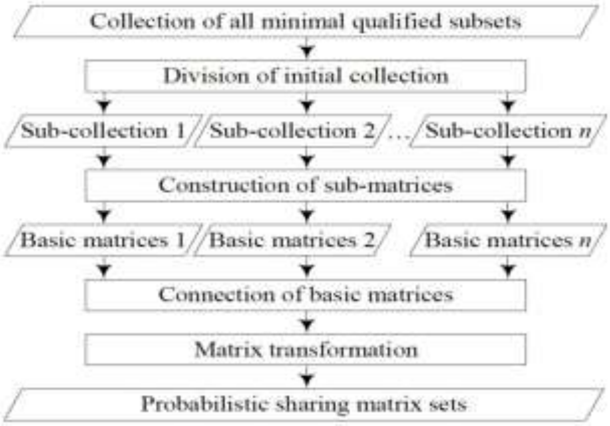
Collection of all minimal qualified subsets
Division of initial collection
Sub-collection 1
Sub-collection 2
...
Sub-collection n
Construction of sub-matrices
Basic matrices 1
Basic matrices 2
Basic matrices n
Connection of basic matrices
Matrix transformation
Probabilistic sharing matrix sets

Figure 5: Processes of constructing probabilistic sharing sets

B. Design of the Methodology for Embedding

After the initial round of sharing, there are expected to be significant exchanges in this part. If its version and error correction level are known, any QR code can have its data capacity and error correction capability determined, as stated in [18]. As can be seen in Figure 6, the majority of the time, each code word that makes up a block is composed of three individual components.

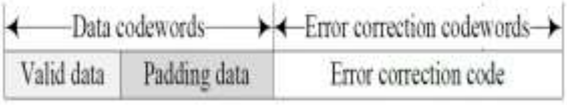

Figure 6: Three parts of data and error correction code words

It is not possible to get the information that a QR code is attempting to communicate by altering lawful data because the QR code itself provides all of the information that is necessary for decoding. Error correcting code words are designed to recover the original data even if there are some errors in the data being encoded, whereas padding data are added into an encoding to fill in redundancies in the encoding. In order to safeguard against the loss of data, both of these procedures are carried out. In order to create appropriate shares, we are going to do research on the padding data [19].

To begin, the dimensions of the cover QR codes are figured out. Let's say the original shares were T_{r1}, T_{r2}, ,T_{rn} and so on, and each one had a size of $a \times b$. We determine the fewest possible data code terms using our formula.

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

We are able to deduce the required version h of QR codes based on the error correction level that has been provided. In addition, it is important to determine whether or not the region size of the padding data is sufficient for embedding an original share. If this is not the case, then h = h + 1until the size is sufficient [20].

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 $C_k(p+i-1, q+j-1)(1 \leq i \leq a, 1 \leq j \leq b, 1 \leq k \leq n)$, if it is a padding data, let

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

Recalculating the error correction code words for the data code words that are now being used is the last step, but it is certainly not the least. Then, the messages that will be utilized as the final pass before the XORing mask patterns are constructed. Following the execution of the error correction process, the recovery technique is carried out on the shares, followed by the application of the neural network to the image that has been recovered. At this point, the final step is to contrast a recovered image with one that has already been categorized.

VI. Performance Parameter

The given table demonstrates the complete execution of the image as indicated by the table topical channel is the best channel for clamour removable procedure,

$$PSNR\ in\ dB = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad (3)$$

$$MSE = \frac{\sum_i \sum_j (\gamma(i,j) - \gamma(i.j)^2)}{M \times N} \quad (4)$$

VII. Results and Analysis

As an illustration of the proposed plan, first choose the QR code image to use as the cover image, and then have it converted to a grayscale image.

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

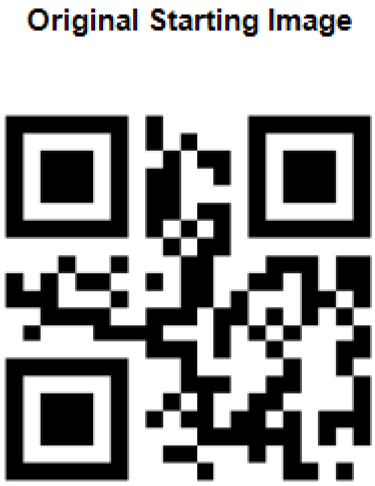

Figure 7: Original Starting Image

Figure 7 shows as original QR image as cover image and figure 8 shows a Grayscale QR image as cover image.

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

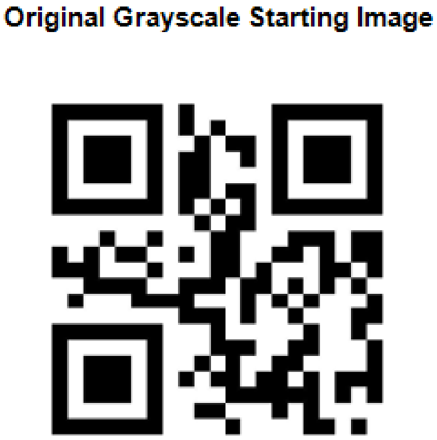

Figure 8: Original Grayscale Starting Image

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

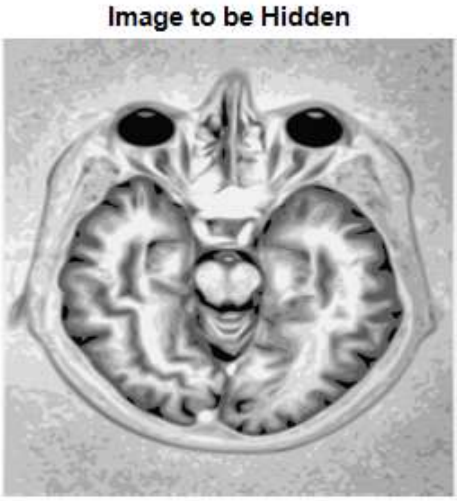

Figure 9: Image to be hidden into QR image

4. **Encrypted Image using Key**

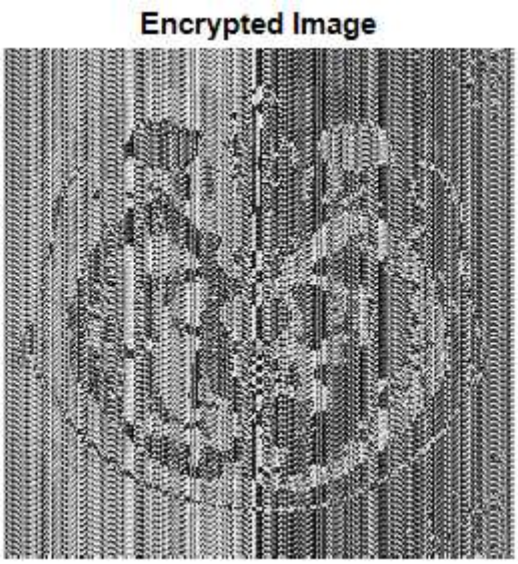

Figure 10: Encrypted image using Key

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

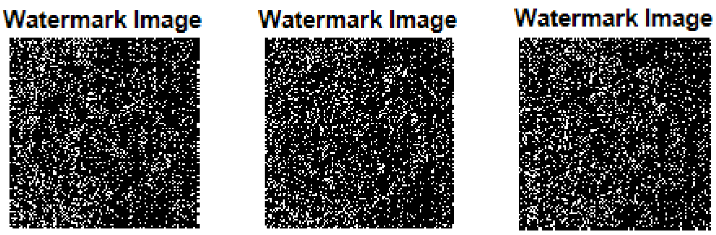

Figure 11: Generate n-shares of Image

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

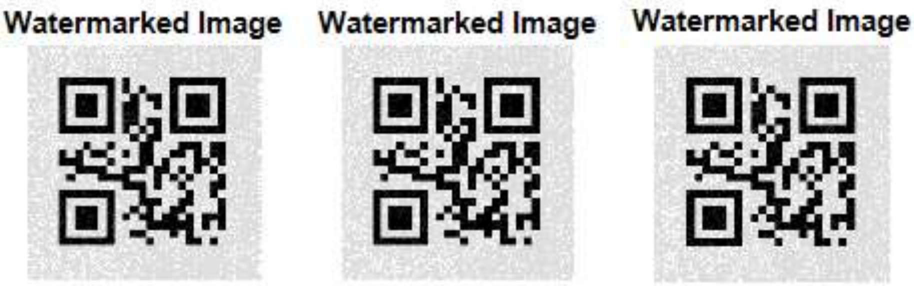

Figure 12: Generate Watermarked image of all 3 shares

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

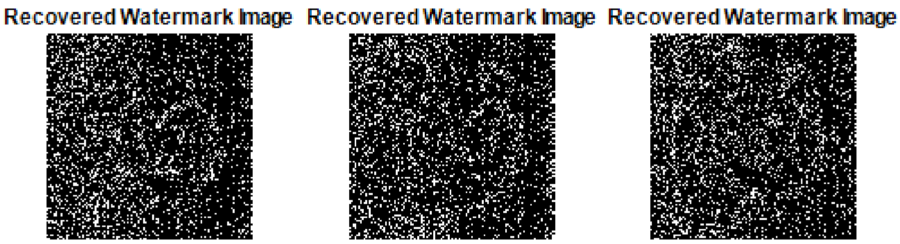
Recovered Watermark Image
Recovered Watermark Image
Recovered Watermark Image

Figure 13: Generate Recover watermark image from watermarked images of all 3 shares

8. **Merged k shares**

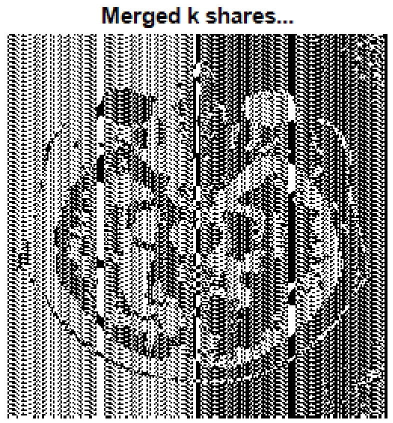

Figure 14: Merged k shares

9. **Recover the secrete image**

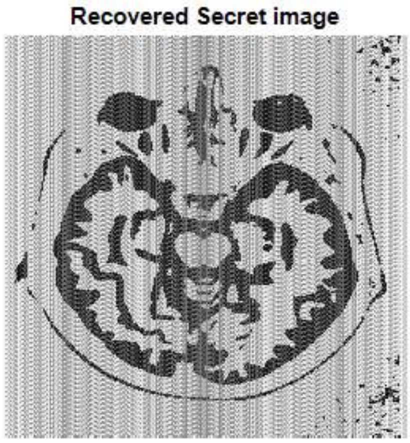

Figure 15: Recover the Secrete Image

10. **Apply ANN to enhance the secret image**

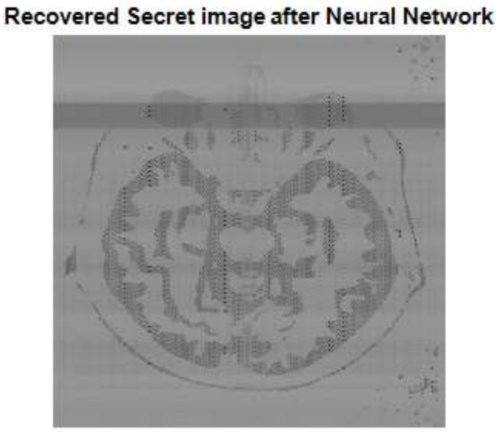

Figure 16: Recovered Secret Image after Neural Network

11. **Image after relative difference of proposed algorithm**

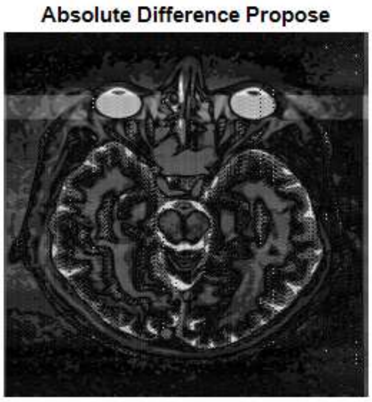

Figure 17: Absolute Difference by proposed method

Table 1: Comparison of Three Parameters

Method	**MSE**	**PSNR**	**Relative Difference**
Base Work	0.0465	28.6955	0.4980
Proposed Work	0.0089	34.2027	0.4431

Figure 9 shows Image to be hidden into QR image as a cover image, Figure 10 shows Encrypted Image using Key, Figure 11 shows Generate n-shares of image, here n=3 and Figure 12 shows Generation watermarked images of all 3 shares. Figure 13 shows Generate Recover watermark image from watermarked images of all 3 shares, Figure 14 Merged k shares, Figure 15 shows recover the Secrete Image and Figure 16 shows Recovered Secret Image after Neural Network.

Table 1 shows the comparison of three parameters like MSE, PSNR and Relative Difference of the two methods. It can be seen that our proposed work is better than base work.

VIII. Conclusion

Due to the fact that only authorized staff members are able to access the stored information, the confidentiality of the data is protected. During this time, anyone who is willing to help has access to the vital information that is required to aid the participant in the event of an emergency. The resilience of the system may be assessed by the fact that it requires the use of highly secure instruments, such as a mobile phone equipped with a camera, a QR Code, and an application that can scan the QR Code. In other words, the system requires all three components. As a consequence of this, in contrast to other systems that rely on substantial infrastructure, the system does not run the risk of failing. The method is not location-specific and can be implemented in any setting in which a sizable number of individuals are congregated.

The purpose of this paper is to present a novel (k, n)-VCS in which each share consists of a valid QR code that has a predetermined meaning. When shares are distributed through public channels, there is less of a chance that potential attackers may notice anything suspicious. In addition, the error-correcting capabilities of cover QR codes are maintained, even after shares have been incorporated into the system. In terms of its application to real-world scenarios, our method can be utilized to verify the safety of QR codes collected from unidentified sources. Even though we used the probabilistic technique to avoid pixel inflation, the size of the hidden image is still constrained to a certain extent. The issue of how to enhance the secret payload of QR codes is still one that has not been resolved.

References

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

[2] Blundo C, De Santis A (1999) Visual cryptography schemes with perfect reconstruction of black pixels. J. Computers Graphics, Special issue: BData Security in Image Communication and Networking. 22(4):449–455.

[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] Blundo C, D'Arco P, De Santis A, Stinson DR (2003) Contrast optimal threshold visual cryptography schemes. SIAM J Discret Math 16(2):224–261.

[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] Bose M, Mukerjee R (2010) Optimal (kn) visual cryptographic schemes for general k. Des Codes Crypt 55(1):19–35.
[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] Cimato S, de Prisco R, de Santis A (2005) Optimal colored threshold visual cryptography schemes. Des Codes Crypt 35(3):311–335.
[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] De Bonis, De Santis A Randomness in visual cryptography, STACS 2000, LNCS, Vol. 1770:627–638.
[16] Grajam RL, Knuth DE, Patashnik O (1988) Concrete mathematics, a foundation for computer science. Addison Wesley, Boston.
[17] Lin SJ, Chen SK, Lin JC (2010) Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. J Vis Commun Image Represent 21:900–916
[18] Liu F, Wu CK, Lin XJ (2008) Colour visual cryptography schemes. Institution of Engineering and Technology (IET) Inf Security 2(4):151–165
[19] Liu F, Wu C, Lin X (2010) Step construction of visual cryptography schemes. IEEE Transaction of Informationa Forensics Security 5(1):27–38
[20] Myodo E, Takagi K, Miyaji S, Takishima Y (2007) Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In: ICME, p 2114–2117.