IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Secret Sharing in Visual Cryptography Using Secure QR Code Scheme and Adaptive Neuro-Fuzzy Inference System

Nisha Singh, M.Tech Scholar, Department of Computer Science & Engineering, Rameshwaram Institute of Technology & Management, Lucknow, India.

Shyam Dwivedi, Assistant Professor, Department of Computer Science & Engineering, Rameshwaram Institute of Technology & Management, Lucknow, India.

Abstract— **The core premise of Visual Cryptography (VC) is that the original secret image must be divided into numerous segments before the human visual system can be used to decrypt the image. However, despite the fact that visual cryptography is a foolproof means for sharing secrets, it still has flaws. Previous studies have demonstrated that VC can cheat utilising a variety of various methods. Attackers can discreetly manipulate the VC process' regulations and cheat without drawing the attention of other participants.**
Because it is so simple to decrypt visual cryptography, it has drawn a lot of attention from the academic community recently and achieved tremendous progress. On the other hand, meaningless shares continue to prevent the actual application of VCS. In this article, we suggest creating a single system that combines a (k, n)-VCS and QR codes. By using the probabilistic sharing strategy, it is possible to increase the size of the secret image that can be shared. A method for communicating a secret with a significant relative difference is established on the basis of this, and artificial neural networks are used to enhance the secret image. We also employ redundant encoding to place the first shares onto the cover QR codes. Following that, each sharing has a unique meaning that can be interpreted using any QR code reader. The covers' inherent ability to remedy errors has been fully retained, in contrast to earlier efforts. It draws attention to the possibility of using our method to check the security of QR codes gathered from unknown sources. In order to demonstrate the validity and advantages of the suggested technique, experimental data and comparisons are given in the conclusion. ANFIS

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

I. INTRODUCTION

The process of digitalizing our lives has the greatest potential to bring about changes in our lifestyles. There is a substantial and ever-increasing concern surrounding security in the modern world, which is characterized by high levels of digital connectivity. When information is transmitted from one node to another via the network, there is always a potential risk to the data's integrity as well as an invasion of the user's privacy. Effective security solutions are absolutely necessary in light of the fact that the number of potentially hazardous situations is growing at a rate that is higher than it was in the past.

Because of advancements in location-aware mobile technology, it is now much simpler to supply people who are having difficulty during a critical time with accurate information that is also aware of the context in which they are now operating. This technology, in conjunction with barcodes, has the potential to be utilized in the event of a crisis, such as a stampede, a health emergency, rioting, overcrowding, or accidents, in order to send precise and crucial information to persons travelling through a throng. It's possible that these persons need this information in order to reply in an acceptable manner. At the same time, the information's privacy and secrecy should in no manner be jeopardized in any way.

The cryptography scheme [1] (VCS) is a form of technology that makes it possible to trade images with one another. Naor and Shamir were the ones who initially came up with the idea. The key principle underlying the VCS paradigm is that a confidential image should be split up across a number of different shares. It is conceivable to visually decode the secret by stacking any qualified subset of shares; however, this cannot be done with forbidden subsets because it is impossible to stack them. As a consequence of the fact that its decryption requires a modest amount of computing, VCS has garnered a considerable amount of interest from researchers, and related topics have been the subject of ongoing research. These research involve the extension of image colour, the enhancement of recuperation effect, the flexibility of access structure, and the enrichment of sharing strategy [9-11]. Shares in the vast majority of schemes, on the other hand, have no real value, which makes it easier for adversaries to develop a suspicious mindset whenever information is exchanged across public channels. The administration of these shares is also a source of a bigger degree of inconvenient work. The basis matrices in [2] were expanded by adding several new columns in order to offer significant shares. These additional columns were introduced specifically for the purpose of carrying the cover information for each share, and they were used accordingly. The incorporation of technology that makes use of halftones into the design of the schemes [6] was done with

the intention of improving the visual effect. Despite this, there was still a significant amount of visible noise in the shares, which led to a poor visual appearance as a whole.

Naor and Shamir [1] made the announcement that Virtual Cryptography will be established, and it would be based on image cryptography. The approach of encrypting the original image into shared photographs would undoubtedly reveal the original image's concealed message or image after a sufficient number of shared photos have been stacked [6]. To put it another way, the objective is to produce shareable images that are generated from the initial image by only changing the pattern of each pixel to one that resembles noise or grey [7]. Now that we've covered the basics of venture capital, let's talk about how to actually change VC.

The first thing that has to be done is to create an original picture that also has a secret message hidden within it. For example, the original version of figure 2 contains the secret message "9768" hidden within the picture someplace. The only colours that should be used to create the picture are black and white. Research on VC had really already been done to encrypt halftone photos in addition to colour photographs before this point. On the other hand, we will discuss the principles of venture capital as they relate to this paper.

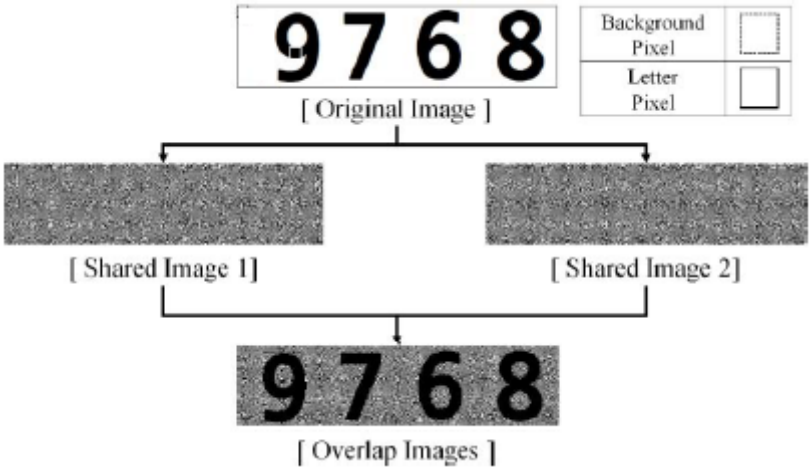

Figure 1: Visual Cryptography Process

It is important to establish some patterns that are capable of changing an original image in order to accomplish the task of encryption. The patterns are constructed out of pixel components that are arranged in a grid that has a grid size of 2 by 2. The upper half of the remaining subpixels are rendered fully transparent, while the bottom half of four pixels at the bottom of the image are made completely opaque. The application of this rule leads in the formation of six distinct patterns, including two shapes that are horizontal, two shapes that are vertical, and two shapes that are diagonal, such as the second row in figure 3. When constructing graphics based on VC, you can only use the forms as building blocks. Before filling the shared image with those shapes, VC picks pixels at random from the original image and converts them all to one of the shapes. This is done after it has filled the shared image with those shapes. When this happens, the images that are being exchanged give the impression of being a shade of grey to human eyes because the subpixels of the shapes transform into noise, which is a random combination of patterns that are made up of black and white.

On the other hand, the method that is utilized to construct the subpixels of the backdrop and the message in the shared image needs to be converted to the opposite manner in order for it to work correctly. If you want to transform a pixel from the background of the original image into one of the patterns that were used to build the shared image [11], you should refer to the background pixel matrix in figure 3.

For instance, if a background pixel in the original image is changed to pattern no. 3, which is a pattern that is chosen at random, then the subpixels of the position in the first shared image (share 1 in Fig. 2) should correctly form a left-vertical pattern. In the event that a second image is used, the subpixels that are situated in the exact same location as those in the first image should have the same pattern. As soon as all of the background pixels of the two shared photos have been made using this method, the backgrounds of the shared images that are going to be overlapped will look to be a grey that is constructed using black and transparent.

shape no	Background Pixel					Letter Pixel				
	Share1		Share2		overlap	Share1		Share2		overlap
1		+		=			+		=	
2		+		=			+		=	
3		+		=			+		=	
4		+		=			+		=	
5		+		=			+		=	
6		+		=			+		=	

Figure 2: Process to make pixel pattern in shared image

In a manner not dissimilar to this, the message part of the shared image is formed in accordance with the matrix of message pixel depicted in figure 3. If a message pixel in the original image is randomly transformed into a diagonal pattern (shape no. 5), then the subpixel of the first shared image needs to set the left-diagonal pattern exactly at the location where the message pixel used to be. Another image that has been distributed must have an unusual shape defined for it in the same location as the first image. By carrying out the aforementioned action, the entirety of the message part of the shared images will be filled. When the two photographs are correctly stacked on top of one another, transparent pixels are overwritten by the black of the pattern in another shared image and appear as black. As a result, the pixels of the secret message component of one of the photos turn black.

The conclusion demonstrates that the colour of the shared image 1 in figure 2 is grey. Figure 2 provides an illustration of the similarities that exist between the first image that was shared and the second image that was shared. However, the hidden message "9768" and the guidelines for how to assemble the shared image are never revealed in any image that is ever distributed. As illustrated in the bottom picture of Figure 2, the perspective of a human being is the only thing that can validate the message, and this is only possible when both photos that were transmitted are superimposed on each other. If the photographs that have been shared do not match from the beginning to the conclusion, or if even one of the images has been distorted, then you will not be able to view the message at all. This applies even if just one of the images has been damaged. Utilising typography that has a higher contrast compared to the background is the primary concept behind this. As a result, VC uses considerably less processing to encrypt data, while it doesn't require any work at all to decode it.

Liu, F., and Wu, C. [8] inserted several more columns in the basis matrices so that they could generate meaningful shares. The cover information that was connected with each share was stored in these additional columns, which were added for that purpose. [9] included the use of the halftone technique into the design of the schemes so that the final product would have a more arresting visual effect. In spite of this, there was still a large quantity of noise in the shares, which led to an unattractive visual impression being created as a result of this. [10] The International Organisation for Standardisation (ISO) has recognised the QR code as a global standard. The QR code is a type of machine recognition code that was developed by the Japanese Denso Wave Company. With the advent of more advanced cellphone technology, QR codes have found widespread use in a variety of applications, including mobile payment systems, electronic identities, and product advertising, among others. The ability of human eyesight to decipher the message contained within QR codes is quite limited. This is because QR codes have a low visual recognition feature. On the other hand, due to the uniform distribution of dark and light modules as well as their seemingly random appearance, the QR code can function as an efficient mask for VCS. The combination of vertical barcodes with quick response codes (QR codes) has attracted a lot of attention as a direct result of this [10]. A method that includes the storage of information on two levels was described [11], and it was developed on the basis of the features of machine recognition.

When using that method, decoding shares was tough, and it was necessary to find a scanning distance and angle that were completely appropriate. This was not always the case, unfortunately. Then, with the assistance of the error-checking mechanism that QR codes provide, a technique of information sharing known as (n, n) was devised [12]. In later years, a (k, n)-VCS was constructed in [14] in accordance with the random grids theory [13], and there is still opportunity for advancement in reference to the relative difference of the retrieved secret. ANN is being put to use in the context of this project in order to improve the concealed image. In addition, the error-correcting capabilities of the shares in [14] were reduced as a result of the fact that multiple code words were changed at various junctures all along the process of sharing. As a consequence of this, there is a possibility that the QR codes' resistance to symbol damage or loss will be diminished.

In this piece, we discuss how a (k, n)-VCS and QR codes could be combined into a single, more efficient system. We describe a method for constructing sharing matrix sets, which involves classifying any minimal qualifying subsets that might be present in the data. This approach is underpinned by a model of probabilistic sharing, which acts as its conceptual basis. In this particular model, the unexpanded attribute makes it possible to have a greater secret size, and artificial neural networks (ANN) are utilised to make the secret picture more accurate. It is also feasible to attain a level of restored performance that is superior to that which was previously achieved, or even perfect. In addition to this, we make use of the encoding redundancy that is provided by QR codes so that the original shares can be placed inside of their appropriate covers. Finally, a large amount of shares in the company have been purchased. In contrast to previous research, the capacity for error correction has been maintained in its whole over the course of this investigation. The results from experiments and comparisons drawn from those experiments demonstrate that the technique that has been proposed is effective.

II. LITERATURE REVIEW

A literary survey involves an investigation of historical material and the generation of a combination of new and historical information. As a consequence of this, this section includes a concise explanation of a number of different research studies, in addition to a research paper summary and a research paper synthesis.

In recent years, there has been a rise in the number of QR code-based electronic discount services, which has led to an increase in the concern regarding the security of QR codes. In order to maintain the integrity of the data that is encoded in QR codes, Lin et al. [9] suggested a method for covertly concealing information that is predicated on the repair of QR code errors.

Tkachenko et al. [10] proposed using a two-layer QR code as the basis for a method for exchanging confidential messages. This method is based on the QR code. A specific pattern is used in place of the black blocks that are seen in a typical QR code thanks to the implementation of this scheme.

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 that is associated with e-coupons. This is due to the fact that these strategies are unable to meet the security goals of e-coupon services, such as authentication and integrity.

Take into account the issues of tampering and forging; there are various practical solutions to this issue that can be implemented. Zhang et al. [11] came up with the idea for a message authentication system that might be used in vehicle communications. Hasan and

his colleagues came up with a way for confirming top-secret material that is based on a chain of authentication [12]. This method is extremely secure. Despite the fact that it has the qualities of traceability and anti-counterfeiting, this method cannot be used in QR code services because it needs a significant amount of space to maintain a chain for each QR code. This renders the method unsuitable for use in QR code services.

In addition to this, it provided a better developed method for eliminating any scratches or damage that may have been caused to QR codes. This was one of the benefits of using this software. If there were any scratches on the QR code, the image could not be decoded by the algorithm since it contains the key to unlocking the code. Because it was required to differentiate the scratch from the damage, the process of eliminating scratches consisted of a number of stages. As a result of an HSV simulation, the broken QR code was restored to its original state after being fixed. After that, the process of dilatation was kicked off with the application of the morphological image processing technique. This method affected the structure of the image and allowed the user to see the scratch in the surface of the object. Following this, we got to work on the technique. By using the median filter, which transforms the image into a binary representation and eliminates noise at the same time, it is possible to increase the efficiency of the decoding stage. In the field of information security, a popular area of research is the two-dimensional barcode that incorporates a digital watermark. This type of barcode is used extensively. There was a broad variety of software that made use of QR codes, and one could use QR codes in a number of various ways. Additionally, one could make use of QR codes in a variety of other ways. Numerous experiments have been performed with the goals of improving information security, recognition, the reduction of duplication in order to conserve space, and the encoding capabilities of various types of data such as audio and video. These goals can be achieved by improving the encoding of audio and video data.

The researchers Meruga et al. (2015) came up with the idea of employing colour QR codes that were camouflaged in order to boost the data capacity and security of the system. The QR codes were created with the goal of stacking a range of colours one on top of the other when they were scanned. QR codes were utilised in a range of settings, including but not limited to marketing, inventory management, and product tracking, to name a few of these applications. While the covert nature of QR codes gave enhanced degrees of protection, the addition of colour coding to QR codes greatly improved the data capacity of these barcodes by three times that of standard QR codes. In order to expand the amount of data that can be stored by QR codes, it was required to make use of these six basic colour combinations.

Shen et al. (2014) presented a comprehensive illustration of a QR code with the intention of making a contribution to the development of intelligent systems. The advancement of information technology culminated in the introduction of the QR code, which has since found use in a broad number of situations and applications that are peculiar to the context in which they are utilised. The quick response code, sometimes known as a QR code, is a brand-new form of technology that can automatically detect objects. Researchers Rungraungslip et al. (2012) conducted study into the use of the retinex theory with the purpose of improving the perception of the QR code. The chain code tracking method served as the basis for the location and correction strategy that was also put forward as an option. The rectification approach included the morphological components of the QR code, which enabled precise identification and extraction of the QR code. This was made possible by the inclusion of these components in the rectification process. The results of the experiment show that the technique that was supplied was implemented correctly, and it was able to properly extract QR code images from the background.

With the assistance of the watermark extraction system, the watermark that was hidden within the QR code was effectively removed. An undetectable watermark was incorporated into the QR code itself, and this watermark served to protect the data that was contained within the QR code. The information that can be accessed on the internet and in the media may have a higher degree of protection if barcodes were used in the same manner as digital watermarks were used in the field of security. This would allow for an increase in the amount of protection that was previously granted to the material.

In his article "QR Code-Based Applications and Pursuits for the Purpose of Gaining Access to Information in the Context of the Human Environment," Baik (2012) presented a novel take on QR code-based apps and pursuits. The QR code was able to serve as a gateway for ambient media because it presented an alternative method of connecting to the internet. This enabled it to perform this role. When QR codes reached the level of their architecture when they were considered mature, the method of getting information was altered. There has been widespread adoption of barcode technology across many different business sectors, including the following industries:

- Logistics
- Merchant Management
- Customer Management, etc.

An attempt was made to target the market for internet portals with the analogue portal service that was proposed. This was done in order to compete with the disruptive effects that are caused by existing portals. Existing Internet portals have an inherent advantage that, due to their monopolistic character, might be described as a competitive disadvantage..

III. VISUAL CRYPTOGRAPHY

Through the use of the network, individuals are able to exchange information that is both valuable and private with one another. This kind of content includes things like medical reports, maps used by the military, financial records, medical photos, and QR codes, to name a few examples.

Images captured in real time that contain sensitive information (SI) are what are referred to as "secret images," and the phrase "secret image" describes this type of image. In this day and age of digital communication, the exponential growth and rapid expansion of digital services have obliged us to give serious consideration to the problem of cyber security. This is due to the fact that cyber attacks are becoming increasingly commonplace. In especially in India, where the country's population of 462 million people are currently striving towards making the dream of a digital India a reality. Text, images taken in real time, audio recordings, and video are just some of the types of media that are among the millions of pieces of data that are processed by the network in the span of a single second. In point of fact, the matter of safety is one of the parts of this general notion that presents one of the greatest challenges. When passing along a SI, it is absolutely necessary to take into consideration the SI's level of security, in addition to the SI's quality and its

integrity. The process of protecting SI typically makes use of methods such as encrypting, decrypting, and concealing information among others.

Naor and Shamir were the ones who came up with the idea for the Visual Secret Sharing (VSS) technique, which is also known as Visual Cryptography (VC). Both terms refer to the same encoding scheme. It is utilised in the process of the transfer of confidential information (SI). VC is an abbreviation for the practise of encrypting sensitive information (SI) by dividing it up into a number of shares and communicating it to a wide variety of different individuals. The only human group that has the ability to recreate the SI is the one that has cracked the code. A traditional visual computing system with the parameters "k" and "n" denotes that the secret image (SI) is partitioned into n shares and that a group of k people or more with k or more shares is able to reconstruct the secret picture. Owning k or more shares is necessary in order to reconstruct the hidden image. Individual shares, as well as holders of fewer than k shares, provide no information about SI and cannot be used to infer anything about the company. In addition to digitally stacking the shares together, which is another technique [15], VC makes it possible for the human visual system to decode SI. This is done in place of the traditional method.

VC is a method of encrypting a secret image that contains confidential visible information in such a way that the decryption may be accomplished solely by the human visual system (HVS) without the use of any computers at all. This makes it possible for the human visual system to decode the image without the need for any computers at all. Encrypting the image in such a way that it can be decrypted by the visual system of a human being is the method that is used to achieve this goal. VC is able to encrypt any kind of visual information, including but not limited to photos, handwritten notes, and printed text, but it is not limited to only these types of information. Because of this method, it is no longer necessary to carry out laborious computations during the decryption process; in addition, it is now possible to reclaim the photos through the process of stacking the shares. It is able to produce flawless cyphers in addition to securely transmitting private information via cryptography. The secret image will typically be segmented into two, three, or even more parts, depending on the circumstances. The secret images can be retrieved after the required number of shares have been printed on transparencies and then layered on top of one another.

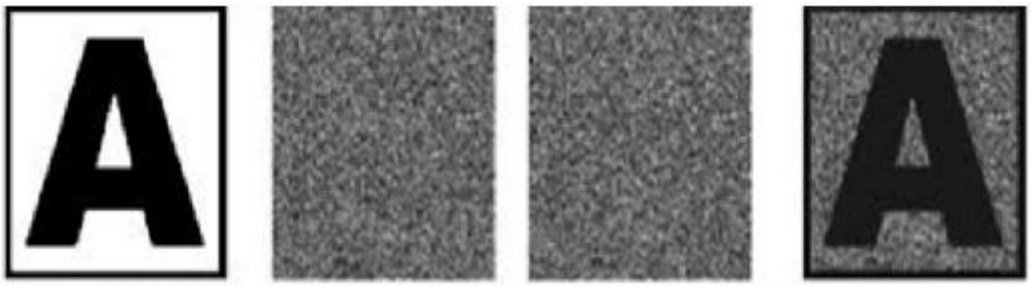

Figure 3: Original image, Halftone, Share-1, Share-2 and Decrypted image

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 was initially created in Japan for usage in the automotive industry. It is a type of two-dimensional barcode. A QR code uses four standardised encoding techniques (such as numeric, alphanumeric, byte/binary, and kanji) to efficiently and swiftly store information [8]. An encoding region and function patterns, such as finder, timing, and alignment patterns, are both components of every single QR Code. The function patterns, which were created expressly for that function, provide the robustness of the QR code recognition and decoding. Figure 4 illustrates the QR code's basic structure. Three different finder patterns are used to locate QR codes and correct their alignment. The coordinates of the module are set by timing patterns. Alignment patterns must be used in order to correct the distortion. The format information sections hold both the mask pattern and the error correction level. The error correction bits and the code version are both recorded in the regions reserved for version information.

The many different versions of the QR code are referred to using the format "Version V-E," where "V" stands for the version number (1–40) and "E" for the error correction level (L, M, Q, or H). From 21*21 modules in Version 1 to 177*177 modules in Version 40, the size of the QR code continuously increases, totaling 177*177 modules. If between 7% (L) and 30% (H) of the codewords are incorrect, it is still possible to decode the QR code using the error correction level [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 [17-20].

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.

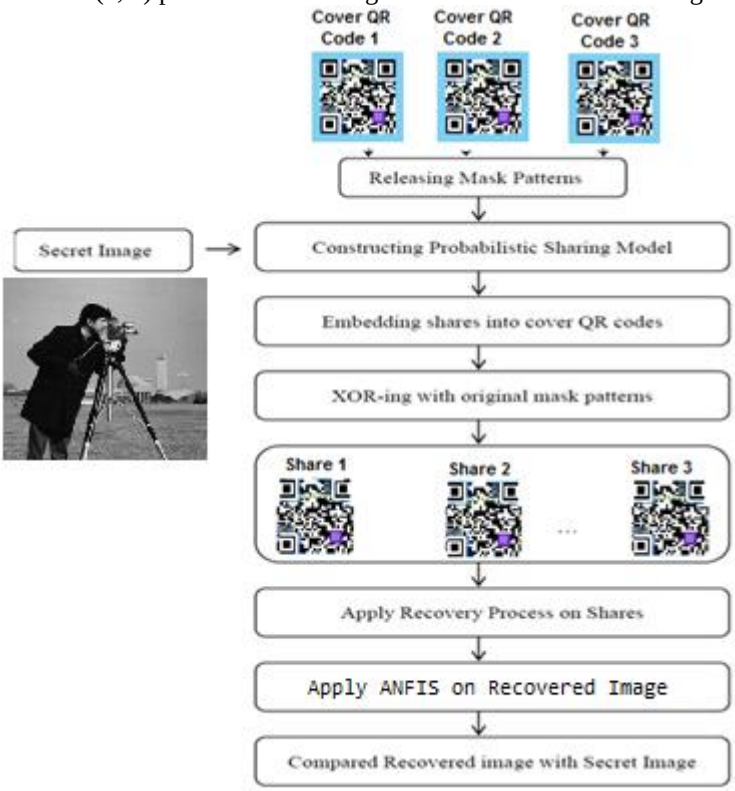

Figure 3: Illustration of suggested approach

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 [21-22].

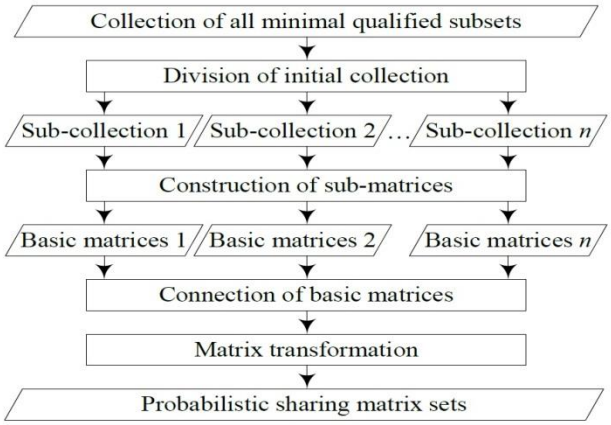

Figure 5: Processes of constructing probabilistic sharing sets

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 [23]. 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.

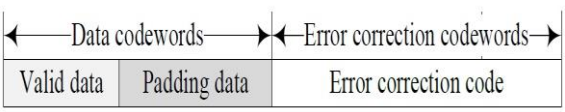

Figure 6: Three parts of data and error correction code words

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 [24].

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

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

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,

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

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

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)**

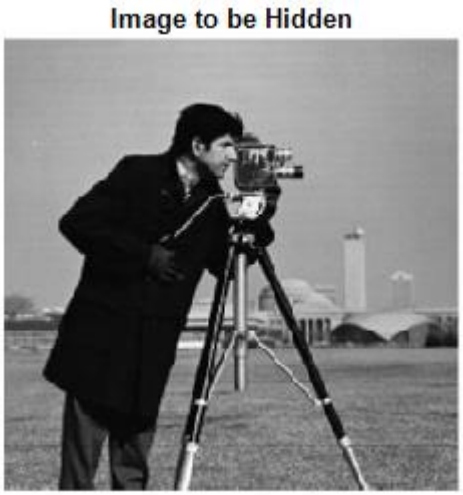

Figure 9: Image to be hidden into QR image

4. **Encrypted Image using Key**

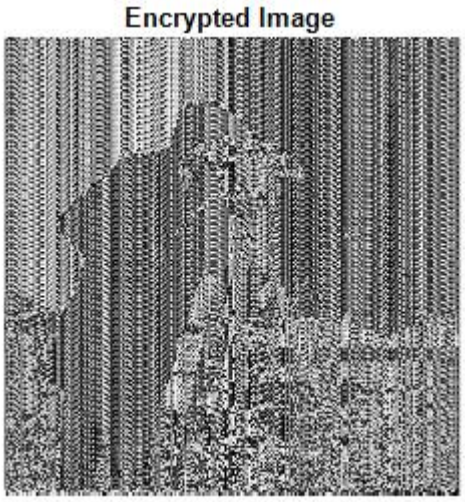

Figure 10: Encrypted image using Key Since n = 3. So the 3 shares will be generated.

5. **Generate n-shares of image:**

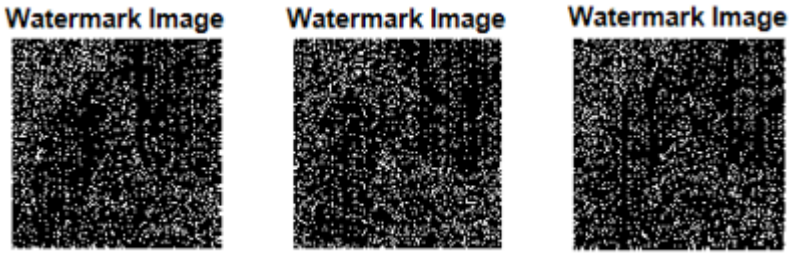

Figure 11: Generate n-shares of Image

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**

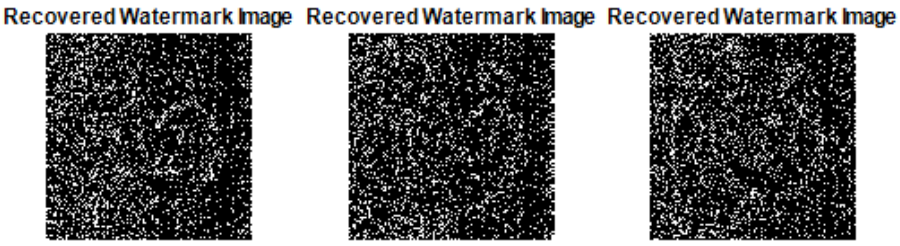

Figure 13: Generate Recover watermark image from watermarked images of all 3 shares

8. **Merged k shares**

Figure 14: Merged k shares

9. **Recover the secrete image**

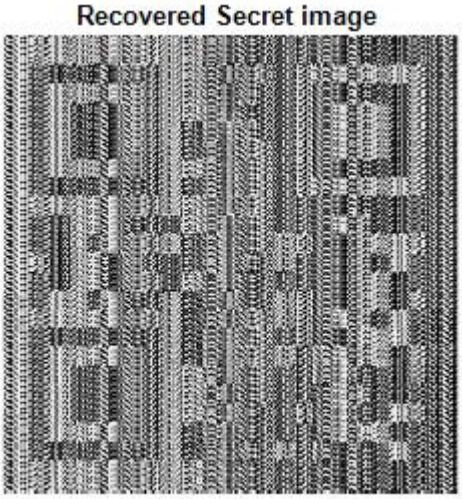

Figure 15: Recover the Secrete Image

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

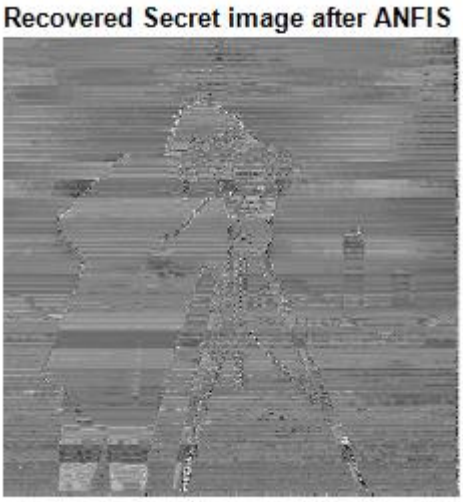

Figure 16: Recovered Secret Image after Neural Network

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

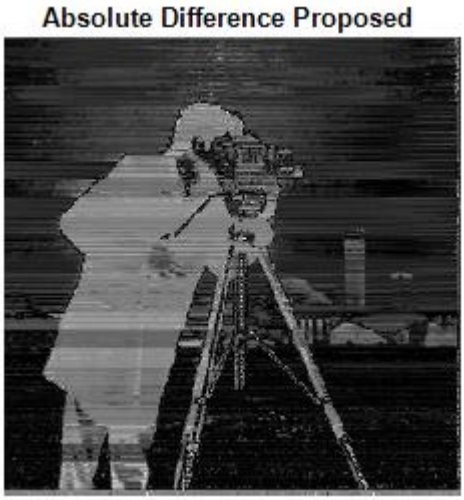

Figure 17: Absolute Difference by proposed method

Table 1: Comparison of Three Parameters

Method	MSE	PSNR	Relative Difference
Base Work	0.1492	24.8127	0.9961
Proposed Work	0.0694	27.3649	0.9294

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

The confidentiality of the data is safeguarded since only authorised staff members have access to the information saved. Anyone who wants to assist gets access to the crucial information needed to support the participant in an emergency during this period. By requiring the usage of highly secure tools like a mobile phone with a camera, a QR Code, and an application that can scan the QR Code, the system's resilience may be evaluated. In other words, the system needs each of the three parts. As a result, the system does not run the risk of failing, unlike other systems that depend on significant infrastructure. The approach can be used whenever there is a significant gathering of people because it is not location-specific.

In this paper, a novel (k, n)-VCS is presented, where each share consists of a valid QR code with a predefined meaning. Shares are distributed through open channels, which reduces the possibility of potential attackers spotting anything fishy. Additionally, even after shares have been added to the system, cover QR codes' error-correcting powers are kept. Our method may be used to check the security of QR codes obtained from anonymous sources, which is applicable to real-world settings. The size of the hidden image is still limited to some extent even if we employed the probabilistic strategy to prevent pixel inflation. The problem of how to improve the hidden payload of QR codes has not yet been solved.

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] Thanh, T. M. & Tanaka, K. An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. Multimed. Tools Appl. 76(11), 13455–13471. https:// doi. org/ 10. 1007/ s11042- 016- 3750-2 (2017).

[10] Selva Mary, G. & Manoj Kumar, S. A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication. Meas. Sci. Technol. 30(12), 125404. https:// doi. org/ 10. 1088/ 1361- 6501/ ab2faa (2019).

[11] Naor, M. & Shamir, A. Visual cryptography. In)Advances in Cryptology—EUROCRYPT'94 , vol 950 (ed. De Santis, A.) 1–12 (Springer, 1995). https:// doi. org/ 10. 1007/ BFb00 53419.

[12] Cai, H., Liu, X. & Yan, B. Beautified QR code with security based on data hiding. In Advances in Computational Intelligence Systems, vol 1043 (eds Ju, Z. et al.) 423–432 (Springer, 2020). https:// doi. org/ 10. 1007/ 978-3- 030- 29933-0_ 35.

[13] Chu, H.-K., Chang, C.-S., Lee, R.-R. & Mitra, N. J. Halftone QR codes. ACM Trans. Graph. 32(6), 1–8. https:// doi. org/ 10. 1145/ 25083 63. 25084 08 (2013).

[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.

[21] Askari, N., Heys, H. M. & Moloney, C. R. An extended visual cryptography scheme without pixel expansion for halftone images. In 2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Regina, SK, Canada, May 2013, pp 1–6. https:// doi. org/ 10. 1109/ CCECE. 2013. 65677 26.

[22] Wang, Y. Intelligent Invoice Identification Technology Based on Zxing Technology. In Innovative Computing vol 791 (eds Hung, J. C. et al.) 87–93 (Springer, 2022). https:// doi. org/ 10. 1007/ 978- 981- 16- 4258-6_ 11.

[23] Hore, A., & Ziou, D. Image Quality Metrics: PSNR vs. SSIM. In 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, Aug. 2010, pp. 2366–2369. https:// doi. org/ 10. 1109/ ICPR. 2010. 579.

[24] Zhang, D., Zhu, H., Liu, S. & Wei, X. HP-VCS: A high-quality and printer-friendly visual cryptography scheme. J. Vis. Commun. Image Represent. 78, 103–186. https:// doi. org/ 10. 1016/j. jvcir. 2021. 103186 (2021).