

## Article

# Secured Secret Sharing of QR Codes Based on Nonnegative Matrix Factorization and Regularized Super Resolution Convolutional Neural Network

Ramesh Velumani <sup>1</sup>, Hariharasitaraman Sudalaimuthu <sup>2</sup>, Gaurav Choudhary <sup>3</sup> , Srinivasan Bama <sup>4</sup>, Maranthiran Victor Jose <sup>5</sup> and Nicola Dragoni <sup>3,\*</sup> 

<sup>1</sup> Institute of Electrical and Electronics Engineers (IEEE), Aruppukottai 626101, India; velumaniramesh@ieee.org

<sup>2</sup> School of Computing Science and Engineering (SCSE), VIT Bhopal University, Bhopal 466114, India; hariharasitaraman@gmail.com

<sup>3</sup> DTU Compute, Technical University of Denmark (DTU), 2800 Lyngby, Denmark; gauch@dtu.dk

<sup>4</sup> Kalasalingam Academy of Research and Education Krishnankovil, Srivilliputtur 626128, India; haribama111@gmail.com

<sup>5</sup> Noorul Islam Centre for Higher Education Kumaracoil, Thucklay, Kanyakumari 673012, India; mvictorjose@yahoo.com

\* Correspondence: ndra@dtu.dk



**Citation:** Velumani, R.; Sudalaimuthu, H.; Choudhary, G.; Bama, S.; Jose, M.V.; Dragoni, N. Secured Secret Sharing of QR Codes Based on Nonnegative Matrix Factorization and Regularized Super Resolution Convolutional Neural Network. *Sensors* **2022**, *22*, 2959. <https://doi.org/10.3390/s22082959>

Academic Editors: Mikolaj Karpinski, Oleksandr O. Kuznetsov and Oleksandr V. Lemeshko

Received: 11 March 2022

Accepted: 8 April 2022

Published: 12 April 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Abstract:** Advances in information technology have harnessed the application of Quick Response (QR) codes in day-to-day activities, simplifying information exchange. QR codes are witnessed almost everywhere, on consumables, newspapers, information bulletins, etc. The simplicity of QR code creation and ease of scanning with free software have tremendously influenced their wide usage, and since QR codes place information on an object they are a tool for the IoT. Many healthcare IoT applications are deployed with QR codes for data-labeling and quick transfer of clinical data for rapid diagnosis. However, these codes can be duplicated and tampered with easily, attributed to open-source QR code generators and scanners. This paper presents a novel  $(n,n)$  secret-sharing scheme based on Nonnegative Matrix Factorization (NMF) for secured transfer of QR codes as multiple shares and their reconstruction with a regularized Super Resolution Convolutional Neural Network (SRCNN). This scheme is an alternative to the existing polynomial and visual cryptography-based schemes, exploiting NMF in part-based data representation and structural regularized SRCNN to capture the structural elements of the QR code in the super-resolved image. The experimental results and theoretical analyses show that the proposed method is a potential solution for secured exchange of QR codes with different error correction levels. The security of the proposed approach is evaluated with the difficulty in launching security attacks to recover and decode the secret QR code. The experimental results show that an adversary must try  $2^{58}$  additional combinations of shares and perform  $3 \times 2^{88}$  additional computations, compared to a representative approach, to compromise the proposed system.

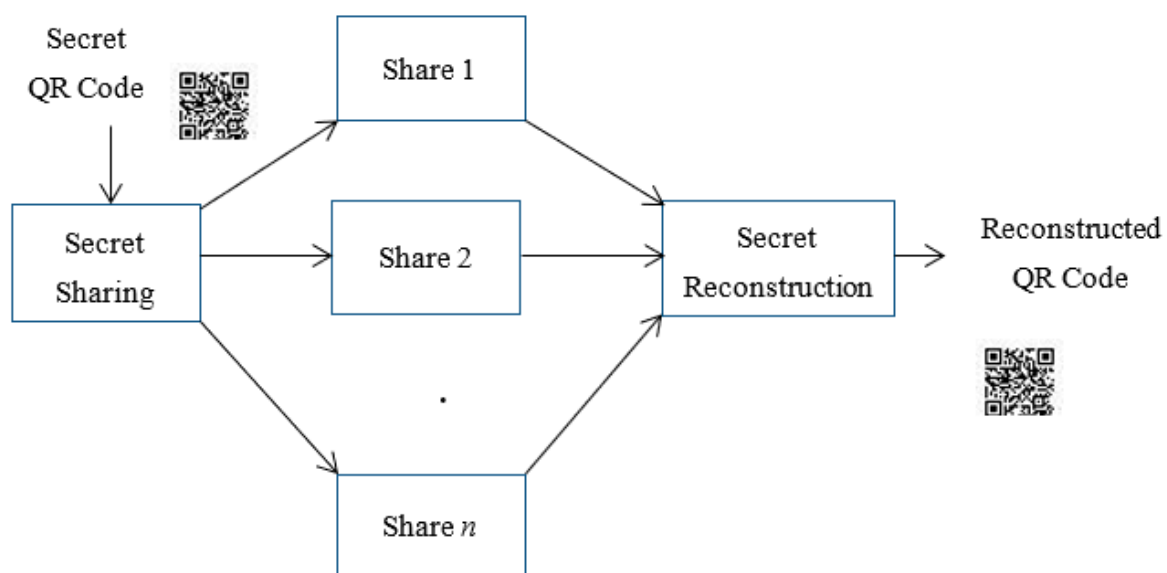
**Keywords:** secret sharing; quick response code; Nonnegative Matrix Factorization; super resolution; convolutional neural network; structural regularization; basis matrix; coefficient matrix

## 1. Introduction

Modern commercial applications employ QR codes in brand promotion, enriching consumer usage experience, interactive labeling for sharing product information, including promotional videos, web links, etc. In addition, QR codes are integrated with service platforms of governments for the effective delivery of utilization and administrative services to the public. The simplicity of QR code generation and scanning with cheap smart phones and IoT has harnessed their extensive adaptation by commercial and nonprofit organizations [1]. For an example, QR codes allow the consumer to connect to the IoT with a simple smartphone or tablet scan. Having all objects marked with a QR code or

barcode means improving the retail environment for consumers because they will be more educated about the item before purchasing, and they will be able to check for an item's availability. On the other hand, they are also susceptible to tampering and duplications for illegal financial benefits and counterfeiting authentic goods [2]. Security investigations have reported huge losses to commercial organizations that are ascribed to the flooding of fake goods carrying authentic QR codes. Several mechanisms have been proposed so far for protecting the QR codes against attacks.

The primitive QR code security approaches embedded the QR codes within cover images in the spatial or frequency domain [3,4]. Later, watermarks were embedded in the frequency domain of the codes employing standard image transformations [5,6] such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). Later, spatial domain watermarking schemes exploiting the structure and error correction [7,8] capabilities of the QR codes were proposed. In these schemes, the QR codes with distortions were not readable and required additional morphological and interpolation operations to be recovered for reading. Further, if the error correction level was high and the embedded data was not encrypted, the QR code and the hidden data could be read by the attacker. In a similar method proposed by Chen [9], the QR code was embedded with message authentication code and cryptographic signature, exploiting the redundancy of error correction codes. Scanned with a conventional barcode scanner, this stego QR code revealed only the public information. The authentication data embedded within the code could be retrieved only if the barcode structure and embedding procedure was known. On successful extraction, the authenticity of the QR was verified. Of late, secret-sharing schemes are widely used in securing the QR codes from malicious attacks. These approaches share the QR code as secret shares among participants and recover the QR code from the shares. With these schemes, better robustness can be achieved. The schematic of the  $(n,n)$  secret-sharing scheme for sharing a QR code as a secret is shown in Figure 1.



**Figure 1.**  $(n,n)$  QR code sharing.

The effectiveness of QR codes in healthcare applications has been demonstrated by various researchers recently [10,11]. Earlier, Feng [12] and co-workers demonstrated the fabrication of an immune-chromatographic assay labeled with QR codes for rapid biomedical diagnosis with Google Glass. In this approach, a QR code generator creates a QR code identifier for one or more diagnostic tests. Attaching a QR code label facilitates the automatic identification of the test of interest and other relevant data such as the patient details. Jamu [13] and co-workers evaluated the feasibility of utilizing the QR codes in

capturing the real-time clinical data in an inpatient clinical environment and reported their effectiveness. A QR code-based diagnostic assay for detection and tracking of malaria has been proposed by Mthembu [14] et al. The QR codes signifying positive, negative and invalid test results integrated with diagnostic kits facilitate the immediate acquisition of clinical data from the point of study to the central laboratories, with the aid of Google Analytics. This approach is found to be effective in the surveillance investigations of diseases. In addition, many researchers have started exploring the integration of QR codes in various clinical applications.

In this intriguing context, this paper proposes a novel approach for sharing QR codes based on NMF [15] and SRCNN [16]. Particularly, we introduce variants of these classical approaches called the multi-layer NMF and structure regularized SRCNN in realizing the proposed system. The inherent characteristic of the NMF in creating component matrices with nonnegative elements is exploited in this work, in the creation of secret shares from QR codes at the sender side. These shares are combined to reconstruct the QR codes at the other end. The proposed scheme is featured as an  $(n,n)$  secret-sharing approach, in which all the shares are essential for reconstruction of the secret QR code. The structure regularization constraint ensures that the structural elements of the reconstructed QR code are intact. This scheme is ideal for sharing secret data as QR codes, to establish trust among a group of participants, creating a secured environment.

The contributions of this research are as below.

1. This paper proposes a novel secret-sharing mechanism for sharing QR codes as basis and coefficient matrices constructed by a multi-layer NMF as secret shares.
2. The QR codes are recovered by computationally less expensive Nonnegative Matrix Reconstruction operations and structure regularized SRCNN on the secrets.
3. The proposed approach eliminates the need for an explicit carrier image to embed the secret shares, as the individual shares do not carry significant information for an attacker.
4. This approach is free from pixel-expansion problems as the shares are not embedded for sharing.
5. The security of the secret can be improved by increasing the number stages of NMF for decomposition of the shares.
6. This approach is suitable for QR codes with different error correction levels as the secret-sharing and reconstruction operations are the same for all sizes of secrets.

Pixel expansion problems encountered in conventional secret-sharing schemes are completely averted in the proposed scheme, as NMF generates the shares by factorization. The SRCNN is applied to recover the QR code from the approximate version obtained from the secret shares. Experimental results with a standard dataset show that the proposed system is an eventual solution towards the realization of anti-counterfeit QR codes. This paper is organized with a review on conventional secret-sharing schemes and QR code-based secret-sharing schemes in Section 2. The mathematical foundations of the proposed system are described in Section 3 and the architecture of the proposed system is given in Section 4. The experimental results, comparative analyses, security analyses and interpretations are given in Section 5. The paper is concluded in Section 6.

## 2. Literature Review

Secret Image Sharing (SIS) schemes share a secret image as a number of secret shares or shadow images among the participants and recover the secret image, combining sufficient number of shares. Visual Secret Sharing (VSS) and Polynomial-based Secret Sharing (PSS) are the popular SIS approaches. VSS schemes reconstruct the secret image simply stacking the secret shares. These schemes based on the logical XOR operations are characterized by lossy recovery and low visual quality of reconstructed secret images [17]. In the earliest  $(k,n)$  PSS scheme proposed by Naor and Shamir [18], the secret image is divided into  $n$  shares, where at least  $k$  out of  $n$  shares are required for secret image reconstruction. Though this scheme is secure, it is characterized by storage overheads, as each shadow image is

of the size of the secret image. A variant of this scheme proposed by Thien and Lin [19] reduced the size of each shadow image by  $1/k$  of the secret image. However, in this method, traces of the secret image are evidenced in the shares and the secret can be reconstructed from insufficient number of shares, forsaking security. Though lossless recovery of secret image is achieved by this method, it suffers from random pixel expansion. Further, other PSS schemes have also been proposed featuring lossless recovery. The scheme proposed by Yang et al. [20] based on polynomials in the Galois Field, exhibits higher computational costs compared to other methods. Similarly, a lossless scheme proposed by Ding et al. [21] also suffers from limitations such as random shape changes, large shadow size and high computational complexity. In a  $(k,n)$  PSS scheme proposed by Zhou et al. [22], the shadow size is reduced to  $1/k - 1$  of the secret image. This method embeds the first  $k - 1$  coefficients to reduce the shadow size. A  $(n,n)$  visual secret-sharing scheme based on XOR operations is proposed in [23], which shares the secret as  $n$  meaningful shares among  $n$  participants. The authors of this paper claim that this method is superior to conventional methods as the drawbacks such as pixel expansion, alignment of shares for reconstruction, loss of contrast, need for an explicit codebook for construction, etc., are mitigated.

Though creation and recognition of QR codes are simple, incorporating them in the business workflow of enterprises poses severe security risks, as QR codes are vulnerable to copy-paste attacks. A QR code can allegedly be used as an attack vector for threatening the reputation of an organization. Sharing a QR code securely among a group of people as secret shares and recovering the QR code from the shares will be a potential solution to enforce trust among a group of people. The significant difference between sharing images and QR codes is that the QR codes must be decodable after recovery. This requirement imposes a stringent constraint on the implementation of the QR code secret-sharing schemes.

Several attack scenarios such as Cross-Site Request Forgery attack (CSRF) [24], Cross-Site Scripting (XSS) attack [25], social engineering, phishing and pharming attacks can be launched, making minimal changes to genuine QR codes. Various empirical studies on the use of QR code as an attack vector are demonstrated in [26]. In order to prevent these attacks, QR code-sharing schemes must avoid information leakage in the secret shares, making reconstruction difficult. In addition, limitations of conventional secret-sharing schemes such as pixel expansion, memory overheads and computational costs must also be reduced or overcome in these schemes. Further, readability requirements also make QR secret-sharing a challenging task. Hence, there are only very few works in this context, discussed in this section.

Lin [27] proposed an  $(n,n)$  secret-sharing scheme in which the secret is divided into  $n$  shadows. Each shadow along with the authentication code is embedded as a pair  $(s_i, v_i)$  into the data codewords of each cover QR code  $QR_i$ . At the other end,  $(s_i, v_i)$  pair is extracted from each  $QR_i$  and all the shares are combined to reveal the secret. This scheme verifies the integrity of each share with the verification code, generated using a master key and a hashing function. A  $(k,n)$  secret-sharing scheme proposed in [28] shares a secret image as  $n$  QR code shares and provides two approaches for revealing the secret, one by stacking the QR code shares and the other by performing XOR operations. This approach called a VSS-based QR code (VSSQR) scheme, exploits the error correction capabilities of the QR codes to generate QR code shares to share images. The secret image can be revealed by stacking a sufficient number of QR-code shares in low-resource settings. Further, this method also facilitates lossless recovery of a secret image by XOR operations among the shares. In an  $(n,n)$  secret-sharing mechanism proposed in [29], a secret message is encoded as a secret QR code and shared among  $n$  participants as QR code shares. The secret message is decoded from the QR code revealed by combining these  $n$  shares. Similarly, a cooperative secret-sharing protocol proposed in [30], embeds secret messages within QR codes and distributes them to  $n$  participants such that each QR code carries both public and private information. Public information is readable by conventional QR scanners while the private message is extracted using a symmetric key. This message is then decoded with the private key of a participant to extract the share. These shares are combined to extract the secret messages.

Liu et al. [31] have proposed a (3,3) threshold secret-sharing scheme called the VSS-QR code. This approach encodes the binary QR codes into three color shares and recovers the QR code by stacking them. Yu et al. [32] present a three-level QR coding scheme, embedding sensitive information within a carrier QR code in three steps, revealing only the public information of the carrier at the first layer.

Recently, Huang et al. [33] presented an  $(n,n)$  threshold QR code secret-sharing scheme, exploiting the error-correction capability of QR codes to enhance the security of the code. In this approach, a secret message encoded as a QR code is shared as  $n$  shares among  $n$  participants, where all the shares have the same version and error correction level similar to the secret QR code. A codeword is associated with each secret share such that each codeword comprises a data codeword and error-correction codeword. The secret is revealed by applying XOR operation on the codewords. This approach successfully decodes the secret from the tampered codewords, exploiting their error correction ability.

In a similar scheme, VSS is extended to the security of web services by Chen et al. [34]. WeChat is one of the most popular messaging apps to send messages, pay bills, share photos and browse news. WeChat Mini-Programs allow developers to run web services, get feedback from users and even monetize their services. By scanning a WeChat Mini Program code, the corresponding program can be accessed. Security of these codes is a concern for users and developers. An  $(n,n)$  Mini Program Visual Secret-Sharing Scheme (MPVSS) proposed by the authors is used for identification and control of the program users. In this scheme, a secret program code is encoded into  $n$  shares using  $n$  cover codes. The secret code is decoded by XOR operation on the shares, exploiting the error-correction abilities of the code. A comparison of the representative VSS schemes is presented in Table 1.

Researchers have shown that nonnegativity is a useful constraint for matrix factorization to learn parts representation of the data. The nonnegative-basis vectors obtained by factorization are used in distributed and sparse combinations to improve expressiveness in reconstructions. NMF is a classical mathematical tool employed in various domains to analyze data from different perspectives. Due to its demonstrated flexibility in the design of scalable and efficient approaches for solving large-scale problems and accuracy of solutions for real-world problems with noisy data, the Frobenius [35] norm-based NMF is widely applied as in [36].

Effectiveness of NMF in capturing the intrinsic geometric properties of images in image-classification problems was demonstrated by Cai and Sun [37]. Shan et al. [38] employed rank adaptive NMF in handwritten character recognition to extract local features of images. In combination with the Extreme Learning Machine (ELM) and k-Nearest Neighbor (KNN) algorithms, NMF was found to significantly reduce the image dimensions and improve classification accuracies. Symmetric Sparse NonNegative Matrix Factorization (ssNMF), a variant of NMF proposed by Li et al. [39], in combination with sparse coding was demonstrated to be effective in the detection of community structure of the brain from magnetic resonance images.

The effectiveness of NMF in digital-content security applications has also been demonstrated in various research papers. The earlier works in this context are digital watermarking schemes for audio, image and video data. In these schemes, NMF is combined with other mathematical transformations such as Singular Value Decomposition (SVD), DFT, DWT, etc., to physically embed a watermark. In a VSS scheme proposed by Wang [40] based on Discrete Fractional Fourier Transform (DFRFT) and NMF, the master and secret shares are constructed by applying NMF on the secret image. Similarly, a secret-sharing scheme for sharing Chinese characters represented as binary images was proposed in [41]. In this work, the authors employed a modified NMF in which the elements of  $W$  and  $H$  were closer to 1 or 0. Though this paper claims that the Chinese characters could be shared as multiple parts, experimental results were shown for 1-stage NMF only. Further, no quality metrics were reported in this paper. However, similar works were not reported so far in this context.

**Table 1.** Comparative analysis of visual secret-sharing schemes.

Reference	Method Employed	Pros	Cons
Naor & Shamir [18] (1994)	Polynomial	Secrets are converted into unconditionally secure shadow image	Requires additional storage as each shadow image is of the size of the secret image
Thien & Lin [19] (lossy) (2002)	Polynomial	Size of shadow image is smaller than secret image	<ul style="list-style-type: none"> <li>Traces of secret image are visible in the shadow images</li> <li>Method suffers from random pixel expansion</li> </ul>
Yang et al. [20] (2007)	Polynomials in the Galois Field	Lossless recovery without pixel expansion	High Computational Cost
Ding et al. [21] (2018)	Polynomial scheme and modular algebraic recovery	Fully lossless recovery	<ul style="list-style-type: none"> <li>Random shape changes</li> <li>Large shadow size</li> <li>High computational complexity</li> </ul>
Zhou et al. [22] (2018)	Polynomial sharing and generalized Arnold permutation	<ul style="list-style-type: none"> <li>Two adjacent pixels are used as secrets</li> <li>Leakage of secret information into the shares is prevented</li> </ul>	The model is not tested under attacks
Singh et al. [23] (2018)	Basis matrices and error diffusion	<ul style="list-style-type: none"> <li>No pixel expansion</li> <li>Alignment of shares not required for reconstruction</li> <li>No need of explicit codebook for construction</li> </ul>	Construction of the secret shares is performed in three steps adding to computational complexity
Huang et al. [33] (2021)	Basis matrices and error correction mechanism of QR codes	The approach is tested with a wide range of attacks	<ul style="list-style-type: none"> <li>The secret code and all the shares are of same version.</li> <li>Though it is the underlying working principle of the method, when the number of shares increase more memory and transmission bandwidth will be required</li> </ul>
Chen et al. [34] (2022)	$(n,n)$ threshold and error correction mechanism	Facilitates sharing of WeChat Mini Program codes	Robustness of the approach is demonstrated with attacks

An image-hashing approach proposed by Karsh et al. [42], employing Projected Gradient Nonnegative Matrix Factorization (PG-NMF) for capturing local features of an image was demonstrated to effectively localize the counterfeit area in an attacked image. In an image encryption and multiplexing system proposed by Chang et al. [43], NMF and digital holography were employed in the secured exchange of keys for protecting the digital images. In this method, NMF was applied on noise-like digital holograms generated out of the candidate image, resulting in basis and weighted image matrices. The basis images

were secured as encrypted data while the column vectors in the weighting matrix served as the keys distributed among participants. In a digital watermarking scheme proposed by Chen [44] et al., generalized NMF that does not impose a dimension-matching constraint, was employed to embed an image within an image. In this approach, the host image was factored into a basis matrix  $A$  and a coefficient matrix  $B$ . Though the authors claimed that the dimension of  $A$  was  $(1, n)$ , which reduces the number of basis components, it was found that each element in the row vector  $A$  was a 2-dimensional representation of the original host image. Watermark embedding was performed by directly replacing the smallest image component of  $A$ . This scheme resulted in severe pixel expansion.

Loss of resolution in reconstructed images is a major drawback of visual cryptographic schemes, as discussed in the work of Weir and Yan [45]. Effectiveness of super-resolution algorithms in the construction of High-Resolution (HR) images from Low-Resolution (LR) images in pan-sharpening of aerial images, medical image analysis for minimum invasive robotic surgery, sign and number plate reading, iris recognition, etc., is demonstrated in the literature. Loss of quality in a reconstructed image was attributed to pixel expansion rate and relative difference in weights of the shares generated from different color levels as discussed in the work of Wu et al. [46]. Loss of resolution of a reconstructed image can be reduced by minimizing pixel expansion and maximizing the relative difference between the weights of the shares. However, this issue can be resolved by improving the resolution of the recovered images with single-image, super-resolution algorithms. These algorithms are broadly classified as statistical, prediction-based, edge and patch or example-based methods.

A thorough investigation of these methods by Yang et al. [47] showed that example-based methods reported in [48,49] achieve state-of-the-art performance. Conventional example-based methods exploit the internal similarities of a given image to perform a mapping between LR images and relevant HR images in a dataset for construction of HR images. Sparse coding is a kind of example-based, super-resolution method, which employs dictionaries in the construction of HR images. In this method, initially, overlapping patches densely cropped from the LR image are encoded into an intermediate sparse representation using an LR image dictionary. HR images are reconstructed from HR image patches estimated from HR dictionaries, using sparse coefficients. This method involves optimization of learning operations from dictionaries and mapping functions, which is realized using the SRCNN, which optimizes the learning, mapping and patch aggregation operations.

Our extensive review reveals that QR codes are employed mostly as carriers in QR code-based secret-sharing schemes. Further, the structure of the cover QR codes and the nature of error correction mechanisms play a vital role in determining the embedding capacity of the cover QR codes, which requires lengthy computations. It is also evident that NMF-based VSS schemes have not been explored extensively. In pursuit of new secret-sharing approaches, the proposed work intends to exploit the property of NMF in representation of image parts for creating secret shares from a QR code and recovering it from the shares. Further SRCNNs are demonstrated to effectively capture the relationship between LR and HR patches.

### 3. Materials and Methods

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

#### 3.1. Dataset and Implementation Details

The proposed system is tested with the dataset accompanying [50], which contains 34 QR codes with error-correction levels L, M, Q and H. The QR codes are of dimensions  $29 \times 29$ ,  $33 \times 33$ ,  $41 \times 41$ ,  $45 \times 45$ ,  $53 \times 53$ ,  $57 \times 57$ ,  $61 \times 61$  and  $77 \times 77$  in PNG format. Demonstrating the ability of the proposed QR code-sharing approach to reconstruct the

QR codes of varied sizes from the secrets shared is essential to demonstrate the robustness of the system. This evaluation is required to prove the flexibility, reliability and generalization ability of the secret-sharing scheme. Further, it also facilitates the identification of prospective applications of the system based on the requirements of applications such as medicine, science, engineering and finance. The size of the QR codes is a major concern in realizing security mechanisms such as privacy, data integrity and authentication. This dataset has QR codes of sufficiently varying sizes with different error-correction levels to test the system.

The secret-share construction and secret-reconstruction processes of the proposed system are implemented with Matlab2020b software. The Zxing [51] library is used for decoding the reconstructed QR codes super-resolved with the structure regularized SRCNN.

### 3.2. Multi-Layer Nonnegative Matrix Factorization

NMF is a class of techniques for approximately factorizing a matrix  $V$  of size  $m \times n$  into two nonnegative matrices  $W$  and  $H$ , each of size  $m \times k$  and  $k \times n$  as shown in Equation (1), where  $W$  is the basis matrix and  $H$  is the coefficient matrix. In linear algebra, a basis vector is used to represent a concise and finite description of an infinite vector space. The reconstruction of  $V$  is shown in Figure 2.

$$V \approx WH \quad (1)$$

Figure 2. NMF reconstruction.

The factorization of  $V$  into  $W$  and  $H$  is not unique, as different values of  $k$  yield different  $W$  and  $H$  matrices. It has been shown empirically that for any matrix  $V$ , better approximation of  $V$  is achieved when the condition is satisfied as in the expression (2).

$$k \leq \min(m, n) \quad (2)$$

The smallest value of  $k$ , resulting in  $V = WH$  is called the nonnegative rank of  $V$ , expressed as  $\text{rank}_+(V)$  as in (3).

$$\text{rank}(V) \leq \text{rank}_+(V) \leq \min(m, n) \quad (3)$$

Based on the cost functions used in the divergence measure between  $V$  and  $WH$ , there exist variants of NMF. The squared-error version of NMF employs iterative update rules for minimizing the divergence as given in Equation (4).

$$F(W, H) = \|V - WH\|_F^2 \quad (4)$$

where  $F$  is called the Frobenius norm.

This paper proposes a QR code secret-sharing scheme realized with a two-layer NMF model as shown in Figure 3. This model is based on the multi-layer NMF [52], mathematically represented as in Equation (5).

$$V \approx WH_1H_2 \dots H_n \quad (5)$$



where

$$\begin{aligned}
 [W, H] &= NMF(V) \\
 [H_1, H_2] &= NMF(H) \\
 [H_3, H_4] &= NMF(H_2) \\
 [H_5, H_6] &= NMF(H_4) \\
 &\dots \\
 [H_{n-1}, H_n] &= NMF(H_{n-2})
 \end{aligned}$$

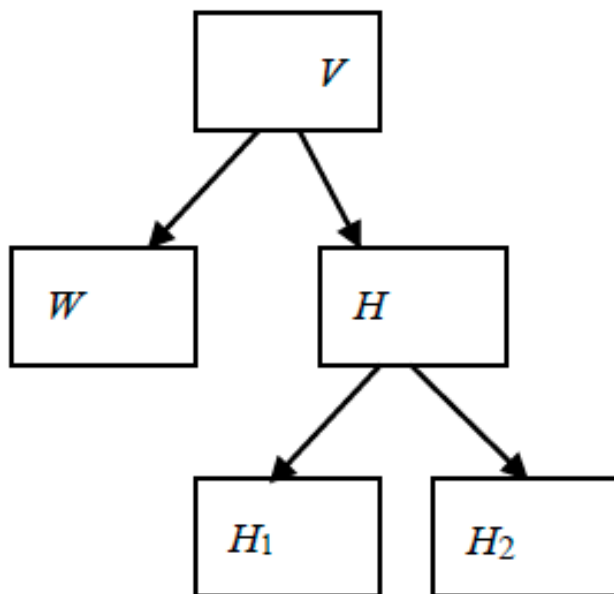


Figure 3. 2-stage NMF.

From the above it can be seen that, in every stage of decomposition, the basis components are preserved and the coefficient matrices are factorized. By generalization, the mathematical model of the 2-stage NMF is given in Equation (6).

$$V \approx WH_1H_2 \tag{6}$$

### 3.3. SRCNN with Structural Regularization

The SRCNN features a simple convolutional neural network structure, which directly learns an end-to-end mapping between LR and HR images, without the need of any pre- and post-processing operations. Given a ground-truth image  $X$  and its LR representation  $Y$ , the SRCNN constructs an HR image  $Y'$  from  $Y$  such that it is equivalent to  $X$ . Image super resolution is performed by the SRCNN in three steps as below, illustrated with Figure 4.

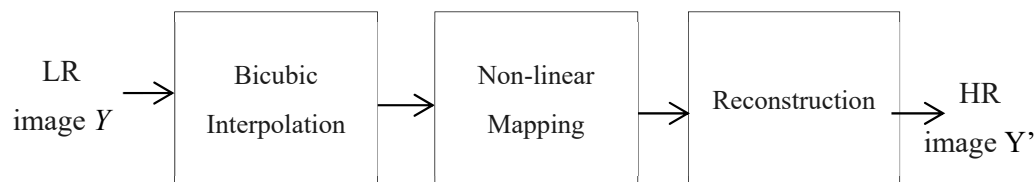


Figure 4. SRCNN architecture.

**(1) Patch extraction and representation:** In this operation, patches called feature maps representing essential features of  $Y'$  are created by convolving a filter with  $Y$  and are represented as a high-dimensional vector.

**(2) Nonlinear mapping:** This operation nonlinearly maps each feature map into a high-dimensional space.

In this step, a convolution filter introduces a high degree of non-linearity to achieve higher accuracy.

**(3) Reconstruction:** This operation aggregates the feature maps to generate the final HR image  $Y'$ , which is expected to be similar to the ground-truth image  $X$ .

In this research, we introduce a structural regularization constraint to ensure that the structural details captured from  $Y$  to  $Y'$  are intact. The problem of reconstruction of  $Y'$  from  $Y$  is formulated as in (7), where  $D$ ,  $S$  and  $N$  refer to the down-sampling operator, blurring operator and the noise, respectively.

$$Y = DSY' + N \quad (7)$$

The super-resolved image  $Y'$ , which closely matches the ground truth  $X$ , is obtained by minimizing the mathematical model of (7) as in Equation (8). The first term in this equation is called the fidelity term, which penalizes the difference between the reconstructed image  $Y'$  and the LR image  $Y$ . The second term is called the structural regularization term, where  $R_s$  is regularization factor and  $\lambda_s$  is the weight factor that balances the trade-off between fidelity and structural similarity.

$$X = \min_{Y'} (\|DSY' - Y\|^2) + \lambda_s R_s \quad (8)$$

We enforce structural similarity between  $Y$  and  $Y'$  by defining  $R_s$  as a cross-gradient term in Equation (9), which aligns the gradients of the individual image patches in  $y_i$  and  $y_i'$  of the images  $Y$  and  $Y'$ .

$$R(y_i, y_i') = \frac{1}{2} \int_{\Omega} |\nabla_{y_i} \nabla_{y_i'}|^2 dy \quad (9)$$

SRCNNs focus only on the details within a patch without considering the structural relationship between an image patch and neighboring regions. Introduction of the structural constraint ensures that the structural components from the LR image are preserved in the HR image.

#### 4. Proposed System

The proposed work is implemented in three phases viz. secret-share construction, secret reconstruction and image super resolution, described in the following subsections with schematic diagrams and algorithms.

##### 4.1. Secret-Share Construction

Construction of secret shares from the QR code is illustrated with Figure 5. Initially, the QR code  $Q$  is scrambled with Arnold Transform to generate the scrambled QR code  $Q_A$  and the rank of the matrix  $k_1$  is determined.  $Q_A$  is then factored into basis matrix  $W$  and coefficient matrix  $H$  of dimensions  $m \times k_1$  and  $k_1 \times n$ , respectively. The basis component  $W$  is secured as secret share  $S_1$ . The rank  $k_2$  of  $H$  is determined and it is further factored in to  $H_1$  and  $H_2$  of dimensions  $k_1 \times k_2$  and  $k_2 \times n$ , respectively, which are secured as secret shares  $S_2$  and  $S_3$ , respectively. The steps for implementation of this process are given as Algorithm 1.

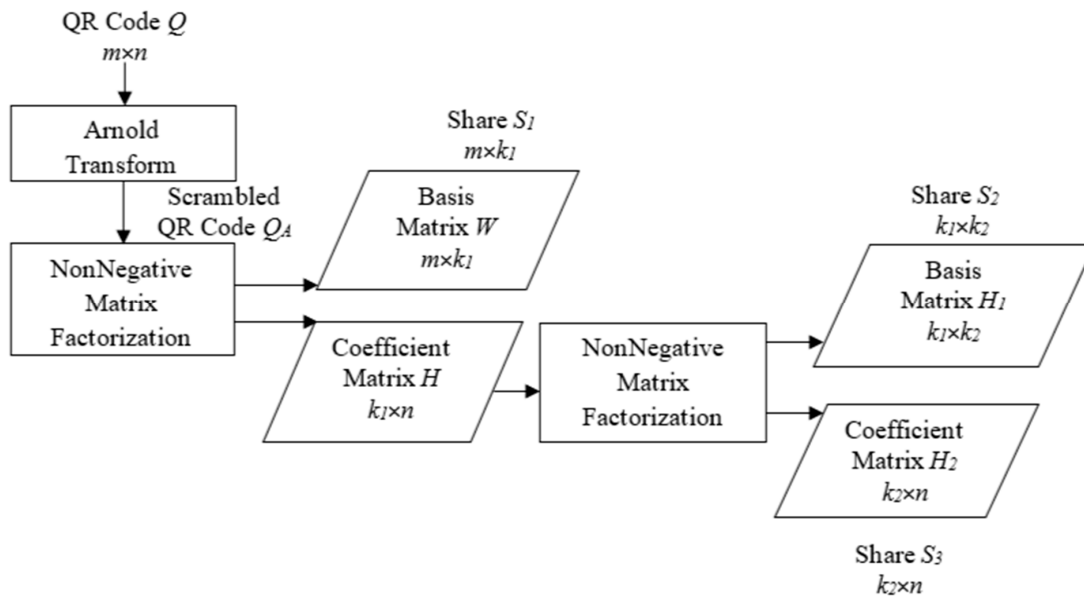


Figure 5. Secret-share construction.

---

#### Algorithm 1. Secret Sharing

---

Input: QR code  $Q$ , number of iterations  $i$

Output: Secret shares  $S_1$ ,  $S_2$  &  $S_3$

Method:

1. Apply Arnold Transform on  $Q$   
 $Q_A \leftarrow \text{Arnold Transform}(Q, i)$
  2. Find the rank of  $Q_A$   
 $k_1 \leftarrow \text{rank}(Q_A)$
  3. Factor  $Q_A$  into base and coefficient matrices  
 $[W, H] \leftarrow \text{NMF}(Q_A, k_1)$
  4. Find the rank of  $H$   
 $k_2 \leftarrow \text{rank}(H)$
  5. Factor  $H$  into base and coefficient matrices  
 $[H_1, H_2] \leftarrow \text{NMF}(Q_A, k_2)$
  6. Construct the Secret Shares
    - a.  $S_1 \leftarrow W$
    - b.  $S_2 \leftarrow H_1$
    - c.  $S_3 \leftarrow H_2$
- 

#### 4.2. Secret Reconstruction

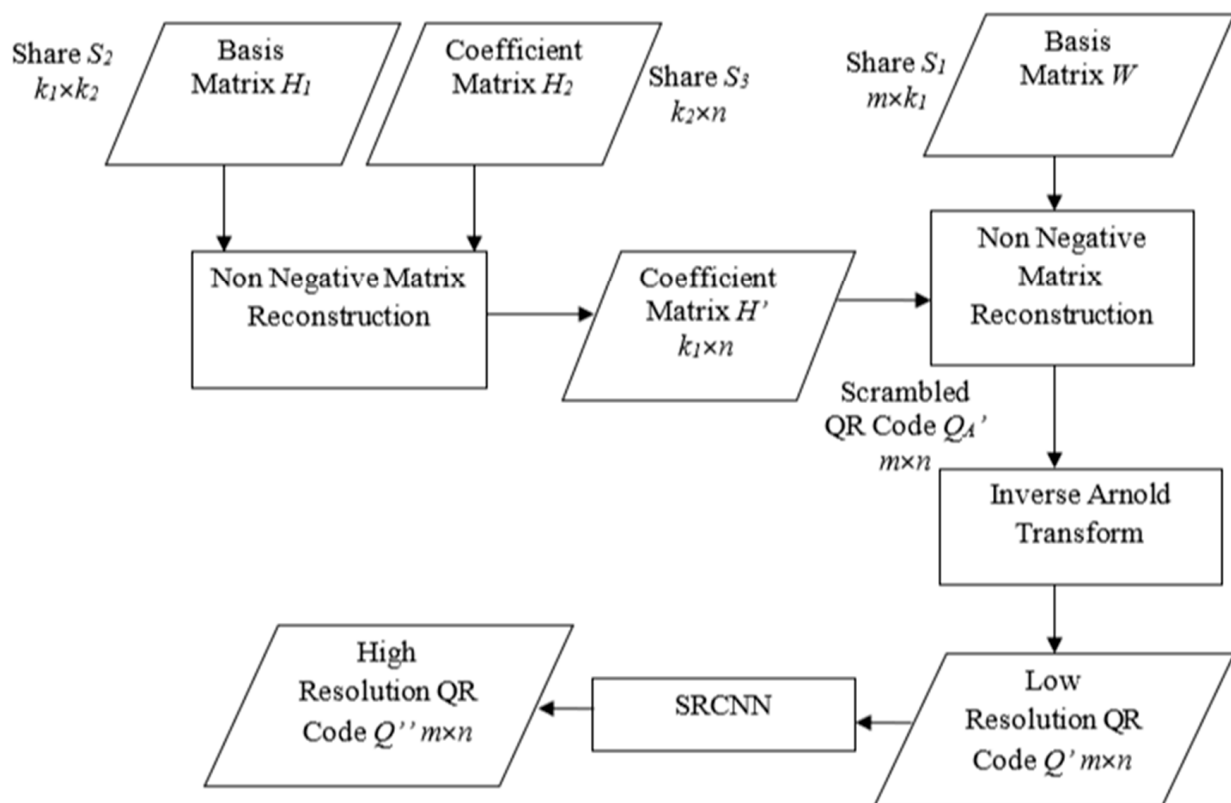
Extraction of the QR code from the secret shares is shown in Figure 6. Initially, the shares  $S_2$  and  $S_3$  are multiplied to generate  $H'$ , the approximation of  $H$ . The secret share  $S_1$  is multiplied with  $H'$  to get the approximation  $Q_A'$ , of the scrambled QR code  $Q$ . Inverse Arnold Transform is applied on  $Q_A'$  to retrieve the unscrambled QR code. The SRCNN is applied on the reconstructed QR code  $Q'$  to generate a high-resolution QR code  $Q''$ . Algorithm 2 lists the steps for implementing this process.

**Algorithm 2. Secret Reconstruction**

Input: Secret shares  $S_1, S_2$  &  $S_3$ , number of iterations  $i$   
 Output: Reconstructed secret  $Q''$

Method:

1. Reconstruct the coefficient matrix  $H'$   
 $H' \leftarrow S_2 * S_3$
2. Reconstruct the Arnold Transformed Secret  $Q'_A$   
 $Q'_A \leftarrow S_1 * H'$
3. Apply Inverse Arnold Transform on  $Q'_A$   
 $Q' \leftarrow \text{Arnold Transform}(Q'_A, i)$
4. Reconstruct the secret by Super Resolution
  - a.  $Q'' \leftarrow \text{SRCNN}(Q')$



**Figure 6.** Secret-image reconstruction.

Experimental results have shown that image reconstruction from the *NMF* component matrices provides an approximation of the original image. Since the image is subjected to two levels of decomposition in the proposed system, the reconstructed image cannot provide a best approximation of the original image. The SRCNN-based reconstruction algorithm is implemented in this system to improve the quality and in turn the readability of the reconstructed QR code.

#### 4.3. Image Super Resolution

The schematic of the SRCNN is shown in Figure 7 for reconstruction of an HR QR code from its LR version. In the proposed work, we employ the SRCNN constrained by structural regularization in recovering the readable QR code from the approximate version reconstructed by combining the secret shares constructed with *NMF*. Initially, the binary QR codes in the dataset are transformed to RGB to enhance the image resolution. The first stage of the SRCNN convolves the LR image with filters of size  $f_1 \times f_1$  for  $n_1$

times to represent each patch as an  $n_1$  dimensional vector. In the second stage, each  $n_1$  dimensional vector is transformed into an  $n_2$  dimensional vector by convolution with  $n_2$  filters of size  $f_2 \times f_2$ . Each  $n_2$  dimensional vector is the HR representation of a patch in the LR image. Finally, these vectors are convolved with filters of size  $f_3 \times f_3$  to construct the super-resolved image.

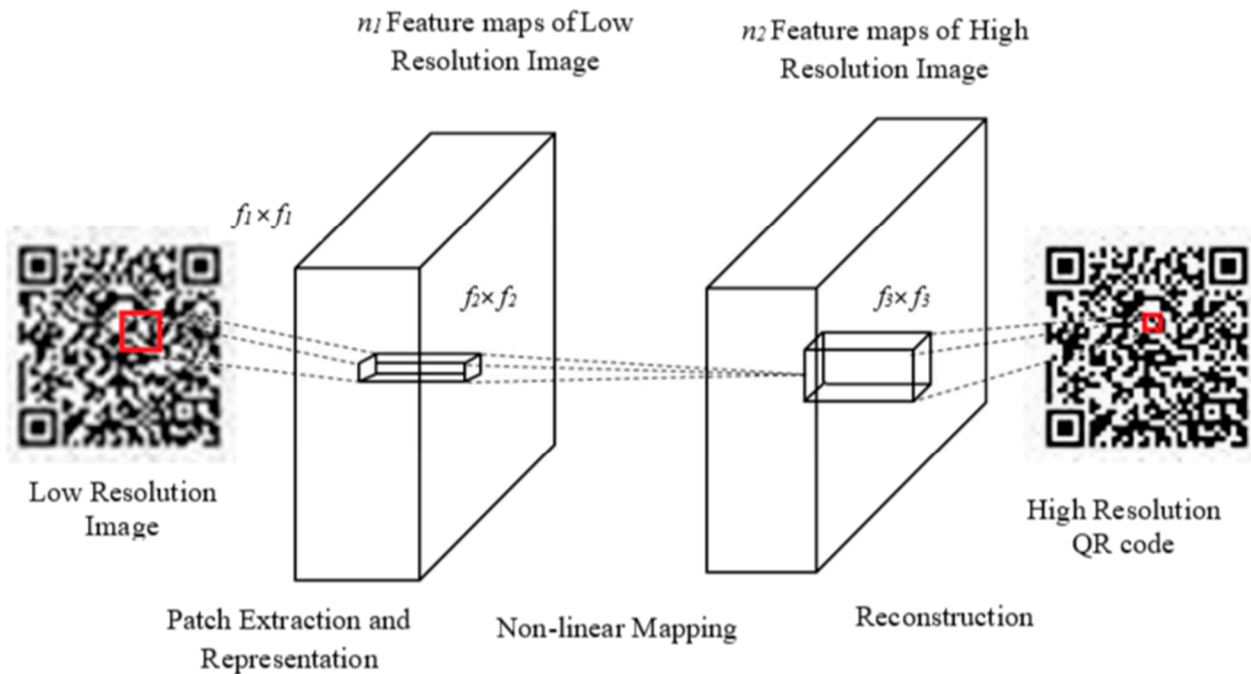


Figure 7. QR code super resolution.



















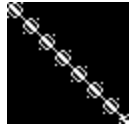

















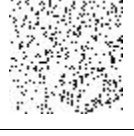
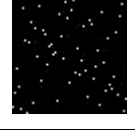
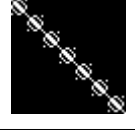



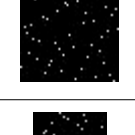
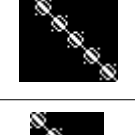






## 5. Experimental Results and Discussions

The proposed system was run in an Intel i5 processor with NVIDIA GeForce 920 MX GPU on the QR codes in the dataset described in Section 3.1. The number of iterations  $i$  for Arnold transform is assumed to be 4, while rank values  $k_1$  and  $k_2$  depend on the input matrix. The 9-5-5 SRCNN model with hyper parameters  $f_1 = 9, f_2 = 5, f_3 = 5, n_1 = 32$  and  $n_2 = 64$  is employed in the QR code reconstruction. For structural regularization,  $\lambda_s$  is initialized to 0.2 after empirical evaluations. In Table 2, the QR codes, secret shares, and reconstructed QR codes along with image quality metrics are shown for 10 best samples in terms of SSIM values in decreasing order.

From the results in Table 2, it is seen that the reconstructed QR codes possess reasonable visual quality from the PSNR values. The SSIM values also signify the similarity between the original and reconstructed QR codes. However, readability of the QR code is the prime requirement compared to the visual quality and similarity metrics. Secret sharing is accomplished in the proposed system only if the reconstructed secret is decodable. It has been verified that all the QR codes with different error-correction levels are decodable by the Zxing decoder. Finally, the decoded QR codes are transformed as binary images for performance evaluation of the system as the original dataset contains binary QR codes.

It is seen that the highest SSIM value of 0.9373 is achieved for a QR code of size  $29 \times 29$ , while the highest PSNR of 32.3889 dB is attained on recovering a QR code of  $53 \times 53$ . Further, analysis of the smallest values of the metrics show that least PSNR and SSIM values of 30.4143 dB and 0.8669 are attained on reconstruction of a  $61 \times 61$  QR code. This result shows that performance metrics are irrespective of the size of the code. However, ability of the system to reconstruct decodable QR codes for all the test samples demonstrates the reliability of the system.

Table 2. Experimental results for QR code sharing and reconstruction.

Original QR Code	Secret Share $S_1$	Secret Share $S_2$	Secret Share $S_3$	Reconstructed QR Code	PSNR in dB	SSIM	Readability
					32.3639	0.9373	Yes
					32.0880	0.9313	Yes
					32.2787	0.9310	Yes
					32.2555	0.9298	Yes
					32.3889	0.9297	Yes
					32.2646	0.9265	Yes
					31.5443	0.9201	Yes
					31.6609	0.9128	Yes
					32.1306	0.9110	Yes
					31.3103	0.9091	Yes

### 5.1. Performance Analysis

The experimental results clearly show that NMF is a suitable tool for secret sharing and recovery. Compared to the conventional secret-sharing schemes, which involve complex mathematical operations for secret sharing and reconstruction, the proposed system is comparatively simpler as it involves only factorization and multiplication operations. Further, the proposed system is devoid of the pixel expansion, a major limitation of the conventional secret-sharing schemes. Detailed comparisons of the proposed system with

the existing secret-sharing systems with respect to different attributes are summarized in Table 2. This comparison is an extension of the comparisons presented in [22], which is a similar work in this context.

It has been shown that the complexity of NMF is  $O(kmn)$  in [53] and earlier literature, where  $k$  is the rank of the matrix. It is seen from Table 3 that the proposed system exhibits lossless recovery similar to few existing methods. Here, the shadow size depends on rank of the matrix  $k$ , which is less than  $\min(m,n)$  for an  $m \times n$  matrix. Hence the share size is either the same as or less than that of the secret. Similar to [21], the complexity of the proposed system is proportional to the number of shares or participants. Hence the complexity of the system is  $O(n)$ .

**Table 3.** Comparisons of significant attributes.

Methods	Recovery of Secret Image	Shadow Size with Respect to Secret Image Size	Pixel Expansion	Pre-Encryption & Decryption	Complexity
Naor & Shamir [18]	Lossy	1	No	No	$O(k \log_2 k)$
Thien and Lin [19] (lossy)	Lossy	$1/k$	No	Yes	$O(k^3)$
Thien and Lin [19] (lossless)	Lossless	$1/k$	Yes	Yes	$O(k^3)$
Yang et al. [20]	Lossless	1	No	No	High
Ding et al. [21]	Lossless	1	No	No	$O(k^3)$
Zhou et al. [22]	Lossless	$1/1 - k$	No	Yes	$O(k^3)$
Zhou et al. [22] (without permutation)	Lossless	$1/1 - k$	No	No	$O(k^3)$
Singh et al. [23]	Lossless	1	No	No	$O(n)$
Huang et al. [33]	Lossless	1	No	No	$O(n)$
Chen et al. [34]	Lossless	1	No	No	$O(n)$
<b>Proposed Method</b>	<b>Lossless</b>	<b><math>\leq 1</math></b>	<b>No</b>	<b>No</b>	<b><math>O(n)</math></b>

The summary of the running times of the existing and proposed methods is presented in Table 4. For the proposed system, the time for secret-share creation and reconstruction is the average values of the time taken for these operations on the 34 sample QR codes.

**Table 4.** Comparison of execution times.

Method	Sharing Time (s)	Recovery Time (s)
Naor & Shamir [18]	7.721	7.831
Thien and Lin [19] (lossy)	1.792	2.764
Ding et al. [21]	138.219	10.585
Zhou et al. [22]	1.732	2.424
Zhou et al. [22] (mod 257)	2.714	3.205
Singh et al. [23]	1.3219	0.0615
<b>Proposed Method</b>	<b>0.2436</b>	<b>0.0910</b>

From Table 4, it is seen that the time taken by the proposed method is comparatively very low. The comparisons presented in Tables 3 and 4 are meant to provide a summary of the performance metrics only, as the proposed scheme is completely distinct from others. The methods proposed in [17,18,20,21] were based on evaluation of polynomials during secret-share construction and solving linear equations to reconstruct each pixel. The

proposed scheme involves factorization for secret sharing, and reconstruction of secret is based on multiplications of shares and convolution in the SRCNN. Hence, the proposed method exhibits lower computational times with respect to [17,18,20,21] for both secret-share creation and secret reconstruction.

The  $(n,n)$  method in [23] involved generation of basis matrices and random shares, and conversion of random shares to meaningful shares for construction of secret shares. Hence, the proposed system has lower computational time for secret creation. The decryption involves only XOR operations between shares in [23] and therefore it is lower than the proposed system. Further,  $C_{SRCNN}$  the complexity of the SRCNN is given in Equation (10).

$$c_{SRCNN} = O((f_1^2 n_1 + n_1 f_2^2 n_2 + n_3 f_3^2) S_{HR}) \quad (10)$$

where

$f_i$  is the filter size

$n_i$  is the number of filters

$S_{HR}$  is the size of the HR image

In the proposed system, the complexity of the construction of the HR QR code from its LR representation is analogous to Equation (10). This complexity can be considerably reduced by modifying the values of hyper parameters. Further, there are no security constraints with the SRCNN.

As stated earlier, there are not many works reported on the sharing of QR codes, and for one such method presented in [41] explicit results are not available. Unlike the conventional secret-sharing methods that focus on the visual quality of the secret, the proposed system has the rigorous requirement of the readability of the secret that is achieved with the proposed system.

## 5.2. Security Analysis

The security of the proposed system relies on the imperceptibility of secret shares, attributed to the NMF factorization. From the experimental results, it is seen that the secret shares do not contain any trace of the secret. Further, the size of the shares depends on the ranks  $k_1$  and  $k_2$  of the candidate matrices  $Q_A$  and  $H$ , respectively. It has been highlighted in literature that NMF is not unique for a given matrix  $V$ , and determination of the rank  $k$  is an NP hard problem. To recover the QR code from the shares, an attacker needs the following:

- Secret Shares  $S_1$ ,  $S_2$  and  $S_3$ .
- Sequence of combinations of shares.
- Number of iterations for inverse Arnold Transform  $i$ .

The QR code can be recovered only on combination of the shares in a particular sequence, i.e.,  $S_2$  and  $S_3$  must be combined to recover  $H'$ , which must be combined with  $S_1$ . In addition, the number of iterations  $i$  for scrambling the QR code and applying Arnold Transform also governs the security of the QR code. Inverse Arnold Transform with an erroneous number of iterations cannot recover the QR code. The degree of freedom for choosing the number of iterations is very large, which makes the retrieval of QR code difficult. In the proposed system, the ranks  $k_1$  and  $k_2$  are evaluated from the candidate matrices, by determining the number of linearly independent rows or columns larger than a tolerance, using the  $rank()$  function of MATLAB.

The information theoretical and computational security analysis of the proposed system is as below.

### Information Theoretic Security

*Any  $(n,n)$  secret-sharing scheme is information theoretic secure, if the secret cannot be revealed by any  $(n - 1)$  number of shares.*

In the proposed system, the shares have no visible components of the secret. According to the principle of NMF, the original matrix can be reconstructed only from the basis and



coefficient matrices. In the proposed system, the secret shares are derived from the basis and coefficient matrices of a QR code, without which the QR code cannot be constructed. Hence, the proposed system is information theoretic secure.

### Computational Security

*Any  $(n,n)$  secret-sharing scheme is computationally secure, if it is infeasible to invert the scheme from  $(n - 1)$  number of shares.*

It is very much evident that all the shares  $S_1$ ,  $S_2$  and  $S_3$  must be combined for the reconstruction of  $Q'$ . Hence, it is infeasible to recover the secret unless all the shares are available. Generally, inversion of the secret-sharing scheme is associated with hardness assumptions of the computational procedures involved, such as use of encryption algorithms such as Advanced Encryption Standard (AES) and Cipher Block Chaining (CBC).

In the proposed system, the reconstruction involves only multiplication operations and inverse Arnold Transform. With either one or two shares available out of the three shares, it is not possible to construct the other shares and construct the secret, as each share is incrementally constructed starting from the factorization of the secret. Further, the security of the proposed system is demonstrated in this section with a quantitative analysis on the difficulty of brute force attacks and construction of imperceptible secrets from tampered shares.

#### 5.2.1. Brute Force Attack

Here, for a given  $m \times m$  secret, we evaluate the number of computations required to generate the shares and reconstruct the secret. We arrive at the mathematical expressions for various computations and evaluate them with respect to the dataset used in our experiments. Similarly, we calculate the number of combinations required for brute-force attack on the dataset by the approach proposed in [23] and present a comparison.

In the proposed system, the secret shares  $S_1$ ,  $S_2$  and  $S_3$  are of the dimensions  $m \times k_1$ ,  $k_1 \times k_2$  and  $k_2 \times n$ , respectively. For the entire data set  $m=n$  and hence the share dimensions are  $m \times k_1$ ,  $k_1 \times k_2$  and  $k_2 \times m$ , respectively for  $S_1$ ,  $S_2$  and  $S_3$ .

The attacker needs to construct the individual shares by brute-force approach to recover the secret. Representing each pixel by either 0 or 1, the number of combinations for recovering the shares  $S_1$ ,  $S_2$  and  $S_3$  is given in Equation (11). Further,  $k_1$  and  $k_2$  can assume any value from 1 to  $m$  according to Equation (2). This increases the number of combinations, and  $C$  can be expressed as in Equation (12).

$$C = 2^{mk_1+k_1k_2+k_2m} \quad (11)$$

$$C = 2^{mk_1+k_1k_2+k_2m} 2^m 2^m \quad (12)$$

Substituting  $k_1$  and  $k_2$  by the minimum value 1 in Equation (12), the minimum number of combinations is expressed as  $C_{min}$  in Equation (13).

$$C_{min} = 2^{m+1+m} 2^1 2^1 = 2^{2m+3} \quad (13)$$

Similarly, substituting  $k_1$  and  $k_2$  by the maximum value  $m$  in Equation (12), the maximum number of combinations is expressed as  $C_{max}$  as in Equation (14).

$$C_{max} = 2^{m^2+m^2+m^2} 2^m 2^m = 2^{3m^2+2m} \quad (14)$$

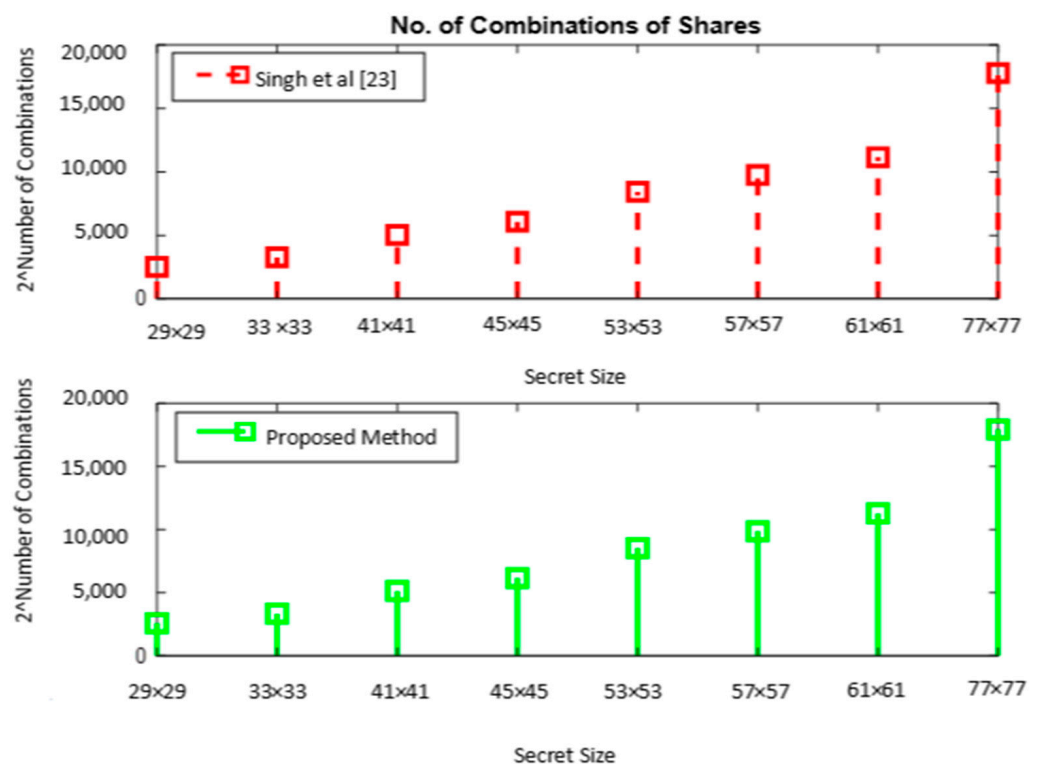
In the  $(n,n)$  secret-sharing scheme proposed in [23],  $2^m \times m \times n$  combinations are required to construct  $n$  shares, each of size  $m \times m$ . A comparison of the number of combinations for constructing the shares in [23] and the proposed system is given in Table 4, for the secrets of varying sizes in our dataset.

It is seen from Table 5 that the number of combinations for constructing 3 shares is very high for the proposed system compared to that of [23]. A graphical illustration of the above table in Figure 8 shows an identical pattern of the plots, which reveals that the number

of combinations of shares linearly increases with the size of the secret. For a secret of size  $29 \times 29$ , the proposed method requires  $2^{58}$  additional combinations to be tried compared to [23], which affirms the security of the proposed approach.

**Table 5.** No. of combinations for construction of shares.

Size of Secret	$m$	No. of Combinations		
		Singh et al. [23]	Proposed Method	
			Minimum	Maximum
		$2^{3m^2}$	$2^{2m+3}$	$2^{3m^2+2m}$
$29 \times 29$	29	$2^{2523}$	$2^{61}$	$2^{2581}$
$33 \times 33$	33	$2^{3267}$	$2^{69}$	$2^{3333}$
$41 \times 41$	41	$2^{5043}$	$2^{85}$	$2^{5125}$
$45 \times 45$	45	$2^{6075}$	$2^{93}$	$2^{6165}$
$53 \times 53$	53	$2^{8427}$	$2^{109}$	$2^{8533}$
$57 \times 57$	57	$2^{9747}$	$2^{117}$	$2^{9861}$
$61 \times 61$	61	$2^{11,163}$	$2^{125}$	$2^{11,285}$
$77 \times 77$	77	$2^{17,787}$	$2^{157}$	$2^{17,941}$



**Figure 8.** Brute-force attack—number of combinations of shares.

Further, the secret image is reconstructed by multiplying  $S_2$  and  $S_3$  first and the resultant with  $S_1$  in the proposed system. As the attacker is unaware of the share labels, all the possible combinations must be tried. For 3 shares, the number of combinations is  $2^3$ . Two multiplication operations are required between the shares to recover the secret. From

the above, the minimum and maximum number of total computations  $T_{min}$  and  $T_{max}$  can be expressed as in Equations (15) and (16).

$$T_{min} = 2^{m+1+m}2^12^12^32 = 2^{2m+7} \quad (15)$$

$$T_{max} = 2^{m^2+m^2+m^2}2^m2^m2^32 = 2^{3m^2+2m+4} \quad (16)$$

Further, inverse Arnold Transform must be applied on the scrambled secret reconstructed from the shares. Generally, an image of  $2^d$  pixels requires  $3(2^{d-2})$  transformations to return to its original position. The number of transformations required for the test data set is given in Table 6. This further increases the number of computations to a greater extent.

**Table 6.** Number of iterations of Arnold Transform to unscramble the secret.

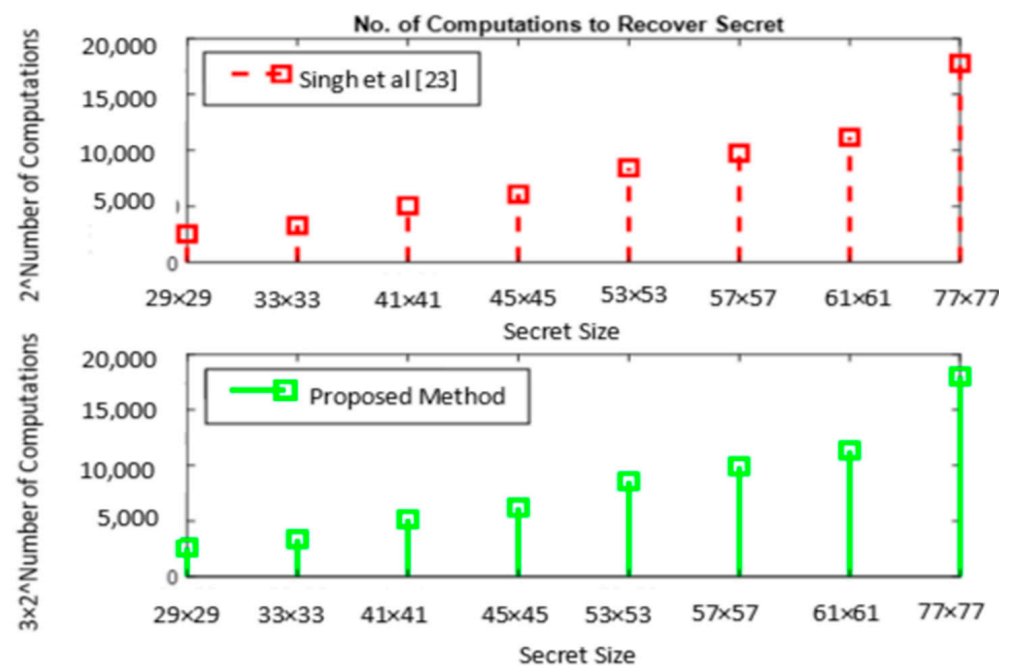
Size of Secret	$d$	No. of Iterations of Arnold Transform $3(2^{d-2})$
$29 \times 29$	29	$3 \times 2^{27}$
$33 \times 33$	33	$3 \times 2^{31}$
$41 \times 41$	41	$3 \times 2^{39}$
$45 \times 45$	45	$3 \times 2^{43}$
$53 \times 53$	53	$3 \times 2^{51}$
$57 \times 57$	57	$3 \times 2^{55}$
$61 \times 61$	61	$3 \times 2^{59}$
$77 \times 77$	77	$3 \times 2^{75}$

Based on Equations (15) and (16) and column 3 of Table 6, the number of computations to be performed to recover the unscrambled secret is evaluated and given in Table 7. For a comparative analysis, this value is presented for [23], considering the XOR operations between  $n$  shares. For 3 shares, 2 XOR operations are to be performed which results in  $2^{3m^2+1}$  computations.

**Table 7.** Total number of computations to recover the secret.

Secret Size	Singh et al. [23]	No. of Computations to Recover the Secret [Proposed System]	
		Minimum	Maximum
$29 \times 29$	$2^{2524}$	$3 \times 2^{92}$	$3 \times 2^{2612}$
$33 \times 33$	$2^{3268}$	$3 \times 2^{104}$	$3 \times 2^{3368}$
$41 \times 41$	$2^{5044}$	$3 \times 2^{128}$	$3 \times 2^{5168}$
$45 \times 45$	$2^{6076}$	$3 \times 2^{140}$	$3 \times 2^{6212}$
$53 \times 53$	$2^{8428}$	$3 \times 2^{164}$	$3 \times 2^{8588}$
$57 \times 57$	$2^{9748}$	$3 \times 2^{176}$	$3 \times 2^{9920}$
$61 \times 61$	$2^{11,164}$	$3 \times 2^{188}$	$3 \times 2^{11,348}$
$77 \times 77$	$2^{17,788}$	$3 \times 2^{236}$	$3 \times 2^{18,020}$

A graphical representation of Table 7 shown in Figure 9 matches that of Figure 8, signifying the consistent behavior of the proposed model compared to [23] with respect to the number of combination of shares to be considered and the number of computations to recover the secret by bruteforce attack. Observation of the number of computations for a  $29 \times 29$  QR code shows that  $3 \times 288$  additional computations are required to recover the secret compared to [23]. However, it is seen that the number of computations required by the proposed system is very high compared to [23] as the secret size increases.



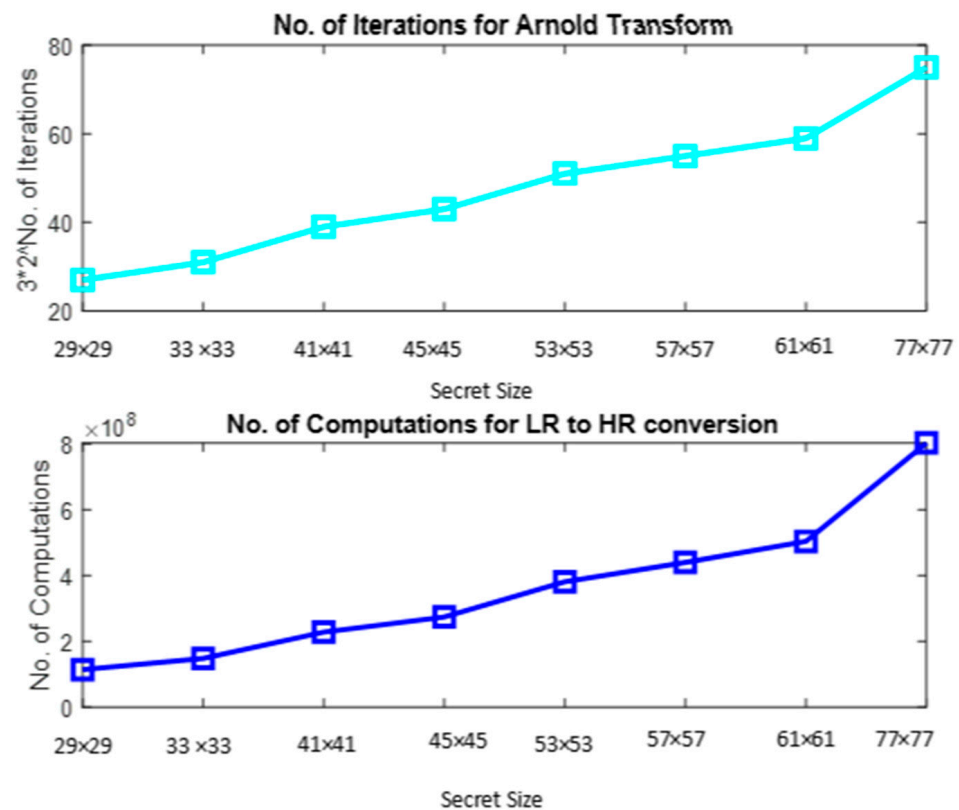
**Figure 9.** Brute-force attack—number of computations to recover secret.

Finally, we present the number of computations evaluated with Equation (10) for the generation of HR secret from the LR secret in Table 8.

**Table 8.** No. of computations for LR to HR conversion.

Secret Size	No. of Computations
$29 \times 29$	$1.14 \times 10^8$
$33 \times 33$	$1.48 \times 10^8$
$41 \times 41$	$2.28 \times 10^8$
$45 \times 45$	$2.74 \times 10^8$
$53 \times 53$	$3.81 \times 10^8$
$57 \times 57$	$4.40 \times 10^8$
$61 \times 61$	$5.04 \times 10^8$
$77 \times 77$	$8.03 \times 10^8$

Graphical illustrations of Tables 6 and 8 are given in Figure 10, which summarizes the number of iterations of Arnold Transform and the number of computations required for super resolution of the secret obtained by brute-force attack. It is seen that the plots are identical, reinstating a linear increase in computational complexities with respect to the size of the secret.



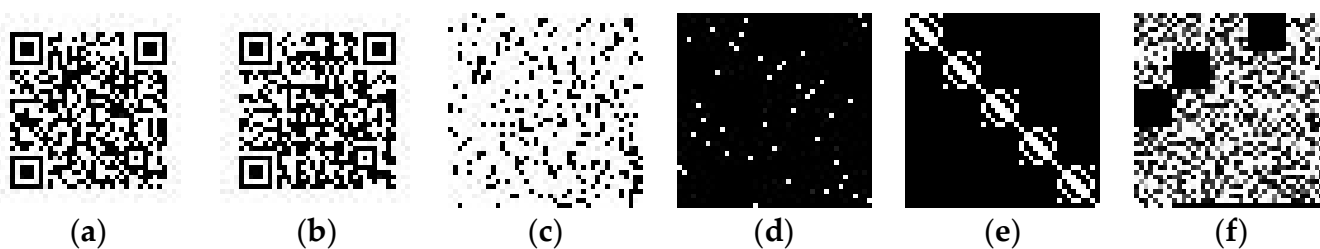
**Figure 10.** Brute-force attack—number of iterations for Arnold Transform and number of computations of Image Super Resolution.

It is seen that the number of computations increases with the size of the secret. From the number of computations required to construct a secret, it is seen that it is difficult for an attacker to construct a secret even with extreme computational resources.

### 5.2.2. Attack on Shares

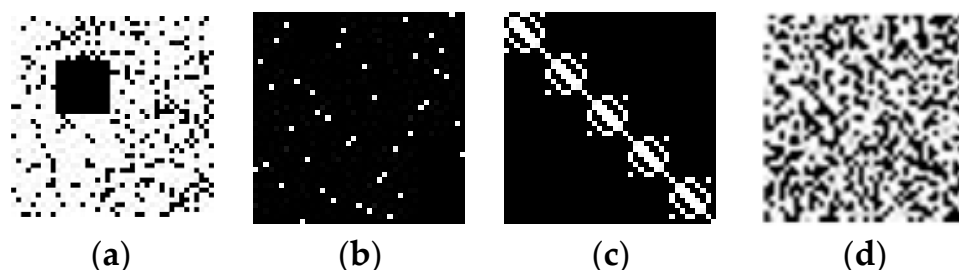
In secret-sharing schemes, the secrets are susceptible to intentional or accidental attacks. These shares may be tampered with by noise addition to the entire secret or selective modification of content. We show that the proposed system is resistant to these attacks with three experiments.

The first attack is posed by completely replacing a secret share by other. It is seen from Table 2 that the secret share  $S_3$  exhibits a similar geometric pattern with significant values along the diagonals. This leads to an implication that  $S_3$  can be guessed and constructed with arbitrary significant values, challenging the security of the system. We experimented with this with the 5th and the 6th QR codes in [50], named *cite\_09\_Q\_small* and *cite\_10\_Q\_small*, respectively, each with dimension  $41 \times 41$ . All the shares generated from these QR codes have the same dimension. We have applied the reconstruction procedure on  $S_2$  of the 5th QR code and  $S_3$  of the 6th QR code to generate  $H'$ . The QR code  $Q'$  is reconstructed by combining this  $H'$  and  $S_1$  of the 5th QR code. The results of this experiment are shown in Figure 11. It is seen that the reconstructed QR code is completely indiscernible, testifying to the security of the proposed system.



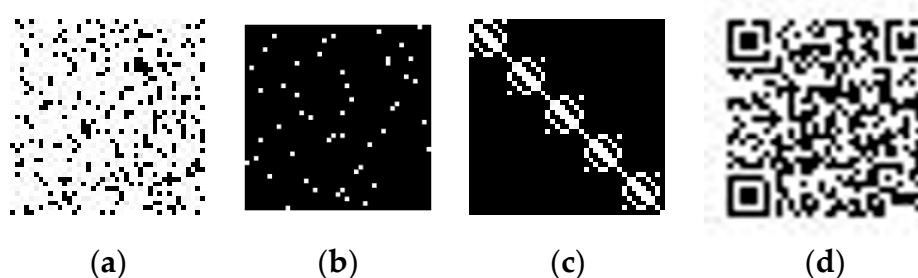
**Figure 11.** QR code reconstruction from tampered share (a) 5th QR code, (b) 6th QR code, (c)  $S_1$  (5th QR code), (d)  $S_2$  (5th QR code), (e)  $S_3$  (6th QR code), (f) reconstructed QR code.

The second attack is launched by selective tampering of pixels in  $S_1$ . The impact of this attack is tested by flipping some of the pixels in  $S_1$  of the 6th QR code and assigning 0 a block of  $10 \times 10$  pixels. The shares corresponding to this QR code and the reconstructed secret are shown in Figure 12. It is seen that the reconstructed QR code is completely distorted.



**Figure 12.** QR code reconstruction from selectively tampered share (a)  $S_1$  (6th QR code), (b)  $S_2$  (6th QR code), (c)  $S_3$  (6th QR code), (d) reconstructed QR code.

The third attack is performed by addition of noise to  $S_2$ . Salt-and-pepper noise of density 0.02 is added to the share  $S_2$  of the 6th QR code to study the effect of accidental noise addition. The shares and the reconstructed secret are shown in Figure 13. In spite of the secret being distorted, the structure of the secret is not completely lost. However, this secret is not decodable by the QR code reader. A noise density of 0.02 affects 2% of pixels in an image. We see that modification of a share by 2% introduces obvious distortions in the secret, rendering it unreadable.



**Figure 13.** QR code reconstruction from share added with noise (a)  $S_1$  (6th QR code), (b)  $S_2$  (6th QR code), (c)  $S_3$  (6th QR code), (d) Reconstructed QR code.

### 5.3. Limitations and Future Works

Initially, we present the limitation of this research. This paper reports complete reconstruction and successful decoding of the QR codes in the dataset and also presents image-quality measures. However, most recent representative works do not contain such explicit results for comparison. The authors report complete recovery and decoding of a  $41 \times 41$  QR code in [31] without obvious performance analysis of the (3,3) secret-sharing approach on a complete dataset. Similarly, in [32] only subjective results are presented

for a small set of QR codes without objective results. Lack of comparative analysis with a standard dataset and quantitative measures restricts further explorations regarding the enhancement of the approaches. Further, due to lack of relevant works, security of the proposed system is compared only with that of [23], which is an  $(n,n)$  secret-sharing scheme. However, it shares the secret as meaningful shares.

From statistical evaluations and experiments by intentional modification of shares, it is seen that the proposed system is secure against brute-force and tampering attacks. However, appearance of uniform geometric patterns in all  $S_3$  is a vital security concern, which requires further investigation. The security of the system can be further improved by scrambling the shares and constructing meaningful shares, which do not raise suspicion. The *rank()* function employed in secret creation evaluates the rank of the matrix as the number of singular values of a matrix, greater than a default tolerance. Since NMF is applied in two stages in this work, the tolerance values can also be used to enforce the security by assuming suitable values. Further, the number of NMF stages can be increased to improve the security of the system.

Of late, color QR codes that have high data capacity and flexibility of encoding are widely used in product and service marketing. However, decoding them is a challenging task due to variations in color maps, channel interferences and the resolution of the camera. Further, applying VSS on color QR codes incurs additional costs, which increases the complexity of the system. The proposed VSS scheme can be extended to color QR codes with the same framework, using Nonnegative Tensor Factorization (NTF) in place of NMF.

## 6. Conclusions

While the existing secret-sharing systems employ QR codes as cover images to carry secret data, we envision the need for sharing QR codes as secrets. Recent medical IoT applications that transform real-time clinical data into QR codes require the protection of QR codes from unauthorized access and tampering. This security requirement can be realized with the proposed system, as demonstrated by our experimental works. This paper presents a novel QR code-sharing scheme exploiting the potential of NMF in part-based representation of images. It also harnesses the potential of SRCNN in the reconstruction of QR codes, which has not been attempted so far. With a standard dataset containing QR codes of varying error-correction levels, we have clearly demonstrated the efficacy of our system with experimental results, theoretic analyses and empirical evaluations of the security attacks. Though the first of its kind, this system imbibes the desirable features of a cryptographic system for secured exchange of sensitive data among participants. This research can be extended by customizing the proposed approach to diverse image classes such as micro QR codes, finger-prints and multi-modal digital images. Recently, color QR codes were introduced that can carry a relatively large amount of information. Though these QR codes feature high data density, they are prone to several problems such as color coding, detection, deblurring, etc., in reconstruction and decoding. The proposed system can be extended to share color QR codes enforcing additional constraints with the NMF and the SRCNN.

**Author Contributions:** Conceptualization, R.V., H.S., G.C., S.B. and M.V.J.; methodology, R.V., H.S., G.C., S.B. and M.V.J.; software, R.V., H.S., G.C., S.B. and M.V.J.; validation, N.D. and G.C.; analysis, R.V., H.S., S.B. and M.V.J.; investigation, G.C. and N.D.; resources, N.D.; data curation, R.V., H.S., G.C., S.B. and M.V.J.; writing—original draft preparation, R.V., H.S., G.C., S.B. and M.V.J.; writing—review and editing, R.V., H.S., G.C., S.B., M.V.J. and N.D.; visualization, R.V., H.S., G.C., S.B. and M.V.J.; supervision, N.D.; project administration, N.D.; funding acquisition, G.C. and N.D. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research has partially been funded by Danish Industry Foundation through project “CIDI—Cybersecure IoT in Danish Industry” (project number 2018-0197).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Pena-Pena, K.; Lau, D.L.; Arce, A.J.; Arce, G.R. QRnet: Fast learning-based QR code image embedding. *Multimed. Tools Appl.* **2022**, *81*, 10653–10672. [[CrossRef](#)]
2. Lu, Y.; Li, P.; Xu, H. A Food anti-counterfeiting traceability system based on Blockchain and Internet of Things. *Procedia Comput. Sci.* **2022**, *199*, 629–636. [[CrossRef](#)]
3. Huang, H.-C.; Chang, F.-C.; Fang, W.-C. Reversible data hiding with histogram-based difference expansion for QR code applications. *IEEE Trans. Consum. Electron.* **2011**, *57*, 779–787. [[CrossRef](#)]
4. Dey, S.; Mondal, K.; Nath, J.; Nath, A. Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA\_QR Algorithm. *Int. J. Mod. Educ. Comput. Sci.* **2012**, *4*, 59–67. [[CrossRef](#)]
5. Li, L.; Wang, R.L.; Chang, C.C. A Digital Watermark Algorithm for QR Code. *Int. J. Intell. Inf. Process.* **2011**, *2*, 29–36. [[CrossRef](#)]
6. Rungrangsilp, S.; Ketcham, M.; Kosolvijak, V.; Vongpradhip, S. Data hiding method for QR code based on watermark by compare DCT with DFT domain. In Proceedings of the 3rd International Conference on Computer and Communication Technologies, Allahabad, India, 23–25 November 2012; pp. 144–148.
7. Gao, M.; Sun, B. Blind Watermark Algorithm Based on QR Barcode. In *Foundations of Intelligent Systems*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 457–462. [[CrossRef](#)]
8. Chiang, Y.J.; Lin, P.Y.; Wang, R.Z.; Chen, Y.H. Blind QR Code Steganographic Approach Based upon Error Correction Capability. *KSII Trans. Internet Inf. Syst.* **2013**, *7*, 2527–2543. [[CrossRef](#)]
9. Chen, C. QR Code Authentication with Embedded Message Authentication Code. *Mob. Netw. Appl.* **2017**, *22*, 383–394. [[CrossRef](#)]
10. Siribunyaphat, N.; Punsawad, Y. Steady-State Visual Evoked Potential-Based Brain–Computer Interface Using a Novel Visual Stimulus with Quick Response (QR) Code Pattern. *Sensors* **2022**, *22*, 1439. [[CrossRef](#)]
11. Colvenkar, S.; Sv, R. Denture Marking for Forensic Identification Using Laser-Marked Stainless Steel Quick Response (QR) Code. *Cureus* **2022**, *14*, e22431. [[CrossRef](#)]
12. Feng, S.; Caire, R.; Cortazar, B.; Turan, M.; Wong, A.; Ozcan, A. Immunochromatographic Diagnostic Test Analysis Using Google Glass. *ACS Nano* **2014**, *8*, 3069–3079. [[CrossRef](#)]
13. Jamu, J.T.; Lowi-Jones, H.; Mitchell, C. Just in time? Using QR codes for multi-professional learning in clinical practice. *Nurse Educ. Pract.* **2016**, *19*, 107–112. [[CrossRef](#)]
14. Mthembu, C.L.; Sabela, M.I.; Mlambo, M.; Madikizela, L.M.; Kanchi, S.; Gumede, H.; Mdluli, P.S. Google Analytics and quick response for advancement of gold nanoparticle-based dual lateral flow immunoassay for malaria–Plasmodium lactate dehydrogenase (pLDH). *Anal. Methods* **2017**, *9*, 5943–5951. [[CrossRef](#)]
15. Paatero, P.; Tapper, U. Positive matrix factorization: A non-negative factor model with optimal utilization of error estimates of data values. *Environmetrics* **1994**, *5*, 111–126. [[CrossRef](#)]
16. Dong, C.; Loy, C.C.; He, K.; Tang, X. Image Super-Resolution Using Deep Convolutional Networks. *IEEE Trans. Pattern Anal. Mach. Intell.* **2016**, *38*, 295–307. [[CrossRef](#)] [[PubMed](#)]
17. Tsai, C.-S.; Chen, H.-L.; Wu, H.-C.; Ying, J.J.-C. A Puzzle-Based Data Sharing Approach with Cheating Prevention Using QR Code. *Symmetry* **2021**, *13*, 1896. [[CrossRef](#)]
18. Naor, M.; Shamir, A. Visual cryptography. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May 1994; Springer: Berlin/Heidelberg, Germany, 1994; pp. 1–12.
19. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [[CrossRef](#)]
20. Yang, C.N.; Chen, T.S.; Yu, K.H.; Wang, C.C. Improvements of image sharing with steganography and authentication. *J. Syst. Softw.* **2007**, *80*, 1070–1076. [[CrossRef](#)]
21. Ding, W.; Liu, K.; Yan, X.; Liu, L. Polynomial-Based Secret Image Sharing Scheme with Fully Lossless Recovery. *Int. J. Digit. Crime Forensics* **2018**, *10*, 120–136. [[CrossRef](#)]
22. Zhou, X.; Lu, Y.; Yan, X.; Wang, Y.; Liu, L. Lossless and Efficient Polynomial-Based Secret Image Sharing with Reduced Shadow Size. *Symmetry* **2018**, *10*, 249. [[CrossRef](#)]
23. Singh, P.; Raman, B.; Misra, M. A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares. *Signal Process.* **2018**, *142*, 301–319. [[CrossRef](#)]
24. OWASP. Cross-Site Request Forgery (CSRF). 2013. Available online: [https://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery\\_\(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)) (accessed on 29 September 2020).
25. OWASP. Cross-Site Scripting (XSS). 2013. Available online: [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) (accessed on 29 September 2020).
26. Krombholz, K.; Frühwirt, P.; Kieseberg, P.; Kapsalis, I.; Huber, M.; Weippl, E. QR Code Security: A Survey of Attacks and Challenges for Usable Security. In Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust, Heraklion, Greece, 22–27 June 2014; Springer: Cham, Switzerland, 2014; pp. 79–90.
27. Lin, P.-Y. Distributed Secret Sharing Approach with Cheater Prevention based on QR Code. *IEEE Trans. Ind. Inform.* **2016**, *12*, 384–392. [[CrossRef](#)]



28. Wan, S.; Lu, Y.; Yan, X.; Wang, Y.; Chang, C. Visual secret sharing scheme for  $(k, n)$  threshold based on QR code with multiple decryptions. *J. Real-Time Image Process.* **2018**, *14*, 25–40. [[CrossRef](#)]
29. Chow, Y.W.; Susilo, W.; Yang, G.; Phillips, J.G.; Pranata, I.; Barmawi, A.M. Exploiting the error correction mechanism in QR codes for secret sharing. In Proceedings of the Australasian Conference on Information Security and Privacy, Melbourne, Australia, 4–6 July 2016; Springer: Cham, Switzerland, 2016; pp. 409–425.
30. Chow, Y.-W.; Susilo, W.; Tonien, J.; Vlahu-Gjorgievska, E.; Yang, G. Cooperative Secret Sharing Using QR Codes and Symmetric Keys. *Symmetry* **2018**, *10*, 95. [[CrossRef](#)]
31. Liu, T.; Yan, B.; Pan, J.-S. Color Visual Secret Sharing for QR Code with Perfect Module Reconstruction. *Appl. Sci.* **2019**, *9*, 4670. [[CrossRef](#)]
32. Yu, B.; Fu, Z.; Liu, S. A Novel Three-Layer QR Code Based on Secret Sharing Scheme and Liner Code. *Secur. Commun. Netw.* **2019**, *2019*, 7937816. [[CrossRef](#)]
33. Huang, P.-C.; Chang, C.-C.; Li, Y.-H.; Liu, Y. Enhanced  $(n, n)$ -threshold QR code secret sharing scheme based on error correction mechanism. *J. Inf. Secur. Appl.* **2021**, *58*, 102719. [[CrossRef](#)]
34. Chen, J.; Wang, Y.; Yan, X.; Wang, J.; Li, L. Visual secret sharing scheme with  $(n, n)$  threshold based on WeChat Mini Program codes. *J. Vis. Commun. Image Represent.* **2022**, *82*, 103409. [[CrossRef](#)]
35. Du, R.; Kuang, D.; Drake, B.; Park, H. DC-NMF: Nonnegative matrix factorization based on di-vid-and-conquer for fast clustering and topic modeling. *J. Glob. Optim.* **2017**, *68*, 777–798. [[CrossRef](#)]
36. Lee, D.D.; Seung, H.S. Learning the parts of objects by non-negative matrix factorization. *Nature* **1999**, *401*, 788–791. [[CrossRef](#)]
37. Cai, X.; Sun, F. Supervised and Constrained Nonnegative Matrix Factorization with Sparseness for Image Representation. *Wirel. Pers. Commun.* **2018**, *102*, 3055–3066. [[CrossRef](#)]
38. Shan, D.; Xu, X.; Liang, T.; Ding, S. Rank-Adaptive Non-Negative Matrix Factorization. *Cogn. Comput.* **2018**, *10*, 506–515. [[CrossRef](#)]
39. Li, X.; Gan, J.Q.; Wang, H. Collective sparse symmetric non-negative matrix factorization for identifying overlapping communities in resting-state brain functional networks. *NeuroImage* **2018**, *166*, 259–275. [[CrossRef](#)] [[PubMed](#)]
40. Wang, H.Y. A Secure Image Watermarking Using Visual Cryptography and Discrete Fractional Fourier Transform. *Appl. Mech. Mater.* **2014**, *577*, 754–757. [[CrossRef](#)]
41. Huang, T.-Y.; Lin, C.-Y.; Chang, M.-K.; Kuo, C.-C. Secret sharing based on part-based factorization for Chinese characters. In Proceedings of the 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Taipei, Taiwan, 12–14 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 209–210.
42. Karsh, R.K.; Laskar, R.H.; Richhariya, B.B. Robust image hashing using ring partition-PGNMF and local features. *SpringerPlus* **2016**, *5*, 1995. [[CrossRef](#)] [[PubMed](#)]
43. Chang, H.T.; Shui, J.W.; Lin, K.P. Image multiplexing and encryption using the nonnegative matrix factorization method adopting digital holography. *Appl. Opt.* **2017**, *56*, 958–966. [[CrossRef](#)] [[PubMed](#)]
44. Chen, Z.; Li, L.; Peng, H.; Liu, Y.; Yang, Y.-X. A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization. *IEEE Trans. Multimed.* **2018**, *20*, 1973–1986. [[CrossRef](#)]
45. Weir, J.; Yan, W. Resolution variant visual cryptography for street view of Google Maps. In Proceedings of the 2010 IEEE International Symposium on Circuits and Systems, Paris, France, 30 May–2 June 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1695–1698.
46. Wu, X.; Wong, D.S.; Li, Q. Extended Visual Cryptography Scheme for color images with no pixel expansion. In Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT), Athens, Greece, 26–28 July 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–4.
47. Yang, J.; Wright, J.; Huang, T.S.; Ma, Y. Image Super-Resolution Via Sparse Representation. *IEEE Trans. Image Process.* **2010**, *19*, 2861–2873. [[CrossRef](#)]
48. Kim, K.I.; Kwon, Y. Single-Image Super-Resolution Using Sparse Regression and Natural Image Prior. *IEEE Trans. Pattern Anal. Mach. Intell.* **2010**, *32*, 1127–1133. [[CrossRef](#)]
49. Yang, J.; Wright, J.; Huang, T.; Ma, Y. Image super-resolution as sparse representation of raw image patches. In Proceedings of the 2008 IEEE Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 14–19 June 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 1–8.
50. Szentandrás, I.; Herout, A.; Dubská, M. Fast detection and recognition of QR codes in high-resolution images. In Proceedings of the 28th spring conference on computer graphics, Smolenice, Slovakia, 2–4 May 2012; pp. 129–136.
51. 2013. Available online: <https://github.com/zxing/zxing> (accessed on 29 September 2020).
52. Cichocki, A.; Zdunek, R.; Phan, A.H.; Amari, S.I. *Nonnegative Matrix and Tensor Factorizations: Applications to Exploratory Multi-Way Data Analysis and Blind Source Separation*; John Wiley & Sons: Hoboken, NJ, USA, 2009.
53. Dang, S.; Cui, Z.; Cao, Z.; Liu, Y.; Min, R. SAR target recognition via incremental nonnegative matrix factorization with  $L_p$  sparse constraint. In Proceedings of the 2017 IEEE Radar Conference (RadarConf), Seattle, WA, USA, 8–12 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 530–534.