applied sciences

MDPI

Article

A Comprehensive QR Code Protection and Recovery System Using Secure Encryption, Chromatic Multiplexing, and Wavelength-Based Decoding †

Paola Noemi San Agustin-Crescencio *, Leobardo Hernandez-Gonzalez *, Pedro Guevara-Lopez, Oswaldo Ulises Juarez-Sandoval, Jazmin Ramirez-Hernandez and Eduardo Salvador Estevez-Encarnacion

Escuela Superior de Ingeniería Mecánica y Eléctrica, Unidad Culhuacan, Instituto Politécnico Nacional, Av. Santa Ana No. 1000, Col. San Francisco Culhucan, Mexico City 04430, Mexico; pguevara@ipn.mx (P.G.-L.); ojuarezs@ipn.mx (O.U.J.-S.); jramirezhe@ipn.mx (J.R.-H.); eesteveze1400@alumno.ipn.mx (E.S.E.-E.)

* Correspondence: psanagustinc1300@alumno.ipn.mx (P.N.S.A.-C.); lhernandezg@ipn.mx (L.H.-G.)

† This article is a revised and expanded version of a paper published in San Agustín Crescencio, P.N.; Hernández González, L.; Guevara López, P.; Ramírez Hernández, J.; Estevez Encarnación, E.S. Information Encryption with Combined QR Codes with Two Security Levels: GPG Method and Chromatic Multiplexing. In Proceedings of the 23th International Conference on Intelligent Software Methodologies, Tools and Techniques IPN, Cancun, Mexico, 24–26 September 2024.

Featured Application

The proposed method can be applied in scenarios where secure and selective access to sensitive or confidential information is required. The approach of embedding data within chromatic QR codes using visible color multiplexing has been demonstrated to enhance protection against unauthorized decoding. The potential applications include information security for government institutions, financial services, and private companies that handle classified or exclusive data.

Abstract

QR codes (Quick Response) were originally developed by the automotive industry to enable rapid data exchange and have since evolved into versatile tools for commercial applications, such as linking to products or websites. However, the scope of their adoption has expanded into sensitive domains including financial, corporate, and governmental sectors. In order to address increasing security concerns, this work proposes a novel three-layer protection scheme. First, data confidentiality is ensured through encryption—in this study, symmetric AES (Advanced Encryption Standard) encryption is used as an example, though any encryption algorithm can be employed. Second, a multiplexing technique is employed to integrate two independent dichromatic QR codes into a single printed chromatic structure. Third, the recovery of each dichromatic code is achieved through the controlled incidence of specific wavelengths, not only providing improved channel separation but also functioning as a physical access control mechanism. This physical layer restricts unauthorized reading.

Keywords: data capacity enhancement; data encryption; dichromatic multiplexing; information security; quick response codes; wavelength

check for updates

Academic Editor: Paris Kitsos

Received: 20 July 2025
Revised: 26 August 2025
Accepted: 1 September 2025
Published: 3 September 2025

Citation: San Agustin-Crescencio, P.N.; Hernandez-Gonzalez, L.; Guevara-Lopez, P.; Juarez-Sandoval, O.U.; Ramirez-Hernandez, J.; Estevez-Encarnacion, E.S. A Comprehensive QR Code Protection and Recovery System Using Secure Encryption, Chromatic Multiplexing, and Wavelength-Based Decoding. *Appl. Sci.* **2025**, *15*, 9708. https://doi.org/10.3390/app15179708

Copyright: © 2025 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/).

1. Introduction

The Quick Response (QR) code [1], developed by the Japanese company Denso Wave in 1994, is characterized by its high data storage capacity, which depends on the physical

size of the code and the optical resolution of the scanner. It can encode up to 7089 numeric characters or 2953 bytes under optimal conditions [2]. Among its variants are Model 1, Model 2, and Micro QR. This work utilizes Model 2, as it incorporates an alignment pattern that improves positional accuracy and allows for greater data capacity compared to Model 1. Versions of Model 2 range from 1 to 40, registered under the AIMI standard [3], with version 40 offering the highest capacity [4].

Thanks to its versatility and ease of use, the QR code has gained significant popularity in recent years, expanding beyond commercial applications to be integrated into official and personal documents such as government-issued IDs, corporate credentials, and medical records. However, the adoption of QR codes in contexts that handle sensitive information has increased the attack surface, exposing them to threats such as spoofing through redirection to malicious sites [5], theft of personal data [6], alteration of the encoded content, and even physical counterfeiting in environments such as parking lots, digital menus, and payment points, where attackers replace or overlay legitimate codes with fraudulent versions [7]. These threats aim to exploit user trust and the absence of visible authentication mechanisms in traditional codes.

In response to this scenario, QR code security has evolved with the development of new techniques to safeguard the information they contain. This work proposes a solution for protecting printed QR codes that store sensitive data, based on the integration of two complementary security layers. First, data confidentiality is ensured through encryption, in this case, AES encryption [8], which ensures the integrity and confidentiality of information during storage and transmission. The second layer employs chromatic multiplexing, which enables the embedding of two independent dichromatic codes into a single chromatic QR code, assigning different encrypted information to each color component (excluding the white background). This design makes it more difficult to tamper with or falsify the content, as altering one of the chromatic channels compromises the complete readability of the entire message. Data can be retrieved more easily thanks to a visual representation in the anaglyph style [9,10], which improves code separation during photographic capture and reduces the risk of incorrect reading or unauthorized manipulation.

This work proposes the integration of two security layers into QR codes: plaintext information is encrypted using the AES algorithm, and a chromatic printed QR code is generated. The encoded information can be retrieved from a photograph through a visual technique based on the anaglyph style, which facilitates the separation of color-encoded data during the decoding process.

The remainder of this paper is organized as follows: Section 2 reviews related work in QR code security. Section 3 details the methodology employed in developing the proposed solution. Section 4 formalizes the mathematical foundations underlying the approach. Section 5 presents a case study illustrating the implementation. Section 6 discusses the obtained results, followed by Section 7, which provides a thorough analysis of the findings and their implications. Finally, Section 8 concludes the paper and outlines directions for future research.

2. Related Work

QR codes offer a fast and convenient way to access information; however, they also pose potential risks such as redirection to malicious websites, theft of personal data, and manipulation of the encoded content. Consequently, various protection measures have been proposed, including encryption, source verification, and the adoption of safe practices by users and organizations [2]. Among these measures, dual-layer QR codes are particularly useful for document authentication and secure information exchange, by superimposing a visible code and a hidden one, which is activated under specific conditions [2]. In

particular, secret sharing schemes take advantage of the error correction capability of QR codes to ensure that data can only be recovered if all authorized parties participate [11,12]. The integration of encryption algorithms and digital watermarking has also been key in the development of more secure QR codes. Several methods combining symmetric and asymmetric cryptography with complex mathematical transformations have been proposed, such as ADNA with Blowfish [4], Lightweight Cryptography (LWC) [13], and LU decomposition and PCA [14], as well as the use of the Fourier transform to generate encrypted diffraction patterns [15,16]. Other techniques that have been explored include QR decomposition in the wavelet domain to protect biometric data [17], and the use of the RSA algorithm to secure highly sensitive information [18].

Another line of research involves nested QR codes, in which one code contains another inside it, allowing the transmission of multiple messages depending on the scanning angle or distance [19,20]. Additionally, steganographic techniques have also been developed to conceal information alongside the main message [21,22], including methods such as subbyte encryption [23] and the insertion of false data to mislead unauthorized users [24]. Some approaches even integrate homomorphic encryption or NTRU with steganography to hide information within a cover image embedded in the QR code [25].

Multiplexing and Capacity Enhancement

The use of colors and multiplexing techniques has significantly improved both the security and storage capacity of QR codes [26]. Methods such as the Prism algorithm for ultra-color encoding [27], the Rubik's cube principle for separating RGB channels [28], and the simultaneous use of multiple colors (red, green, and blue) within the code's structure [29,30] open up new possibilities for advanced encoding. In [31,32], the importance of multiplexing is also highlighted as an effective technique to increase the amount of information that can be stored without altering the visual appearance of the QR code. Furthermore, recent studies have explored less complex but highly functional multiplexing approaches, which enable greater encoding capacity while maintaining the structural simplicity of a chromatic QR code [32,33]. All of the development methodology presented in the following sections is inspired by the initial basic concepts published in [33,34].

3. Methodological Approach

The methodological approach is structured in three main phases: encryption of the information (EA and EB) using dichromatic QR codes (A and B), generation of a chromatic QR code (C) by superimposing the two dichromatic QR codes, and recovery of each dichromatic code through color-based identification techniques using a photograph, as illustrated in Figure 1.

The process begins with two distinct sets of information (IA and IB), which are encrypted and encoded into two dichromatic QR codes labeled A and B. These are then integrated through a multiplexing approach to produce a single chromatic QR code labeled C. To retrieve the original codes A and B from the chromatic QR code C, a visual technique known as the anaglyph is employed.

In this process, the physical control of illumination through the modulation of the duty cycle and frequency of each light beam is essential. The duty cycle ensures chromatic stability, preventing unwanted color mixing, while the frequency regulates luminous intensity, guaranteeing adequate contrast and reducing the impact of undesirable noise during photographic capture.

This physical control of lighting eliminates the need for specialized image sensors or complex software filtering, and it ensures reliable channel separation, independent of ambient lighting conditions or camera characteristics. The system is intended for spe-

cific applications in sectors such as banking and government, where a dedicated device including both specialized illumination hardware and decoding software is deployed to guarantee data security and controlled access.

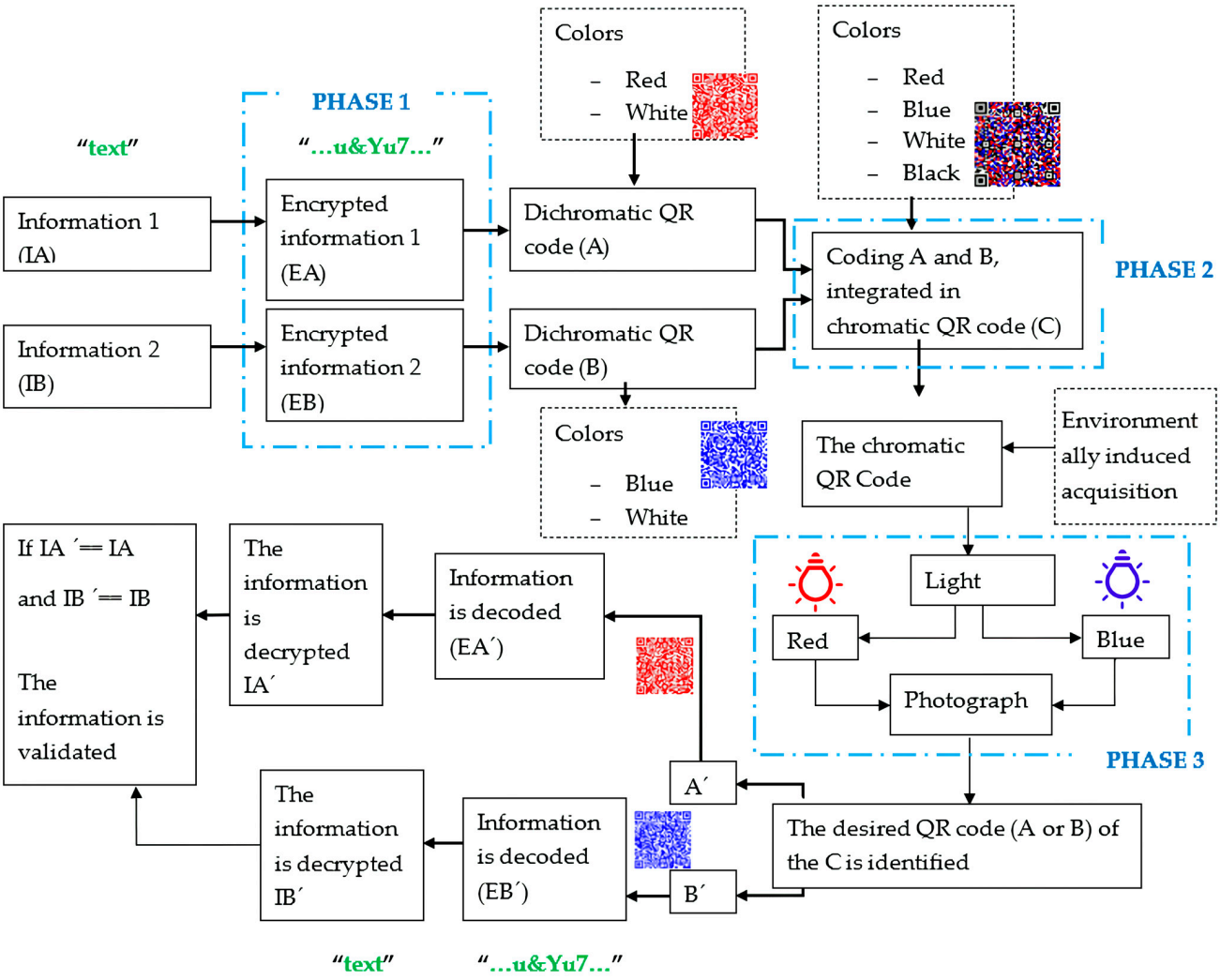


Figure 1. Encryption, multiplexing, and retrieval scheme for dichromatic QR codes.

All simulations and data processing were conducted using Python 3.9.4 (Python Software Foundation).

4. Mathematical Formalization

This study is based on two QR codes (A) (B) that represent two different sets of information. Both codes are represented as input values, which are defined as matrices A and B; each of these matrices, in turn, is defined as a collection of elements, $\{a_{i,j}\}$ and $\{b_{i,j}\}$, respectively.

Definition 1 (Dichromatic QR Code). *A dichromatic QR code is a two-dimensional matrix* $A_{m\times n}$ *with* $m,n \in Nm,n \in N$ *such that each element* $a_{i,j} = \{x,y \mid x \neq y\}$ *with* $0 < i \leq m$ *and* $0 < j \leq n$*, with x and y being colors.*

With two dichromatic QR codes, these being matrix $A_{m\times n}$ and matrix $B_{m\times n}$, it is possible to obtain a chromatic code by a multiplexing relation; this is expressed in Definition 2 and Definition 3.

Definition 2 (Chromatic QR Code). *A chromatic QR code is a two-dimensional matrix* $C_{m\times n}$ *with* $m, n \in N$ *such that each element* $c_{i,j} = \{x, w, y, z \mid x \neq y, w \neq y, z \neq y, x \neq w, z \neq w, x \neq z, y \neq z\}$ *with* $0 < i \leq m$ *and* $0 < j \leq n$, *with* x, y, w, *and* z *being colors.*

Definition 3 (Multiplexing (r)). *Every r multiplexing is a binary relation that, given two dichromatic QR codes* $A_{m\times n}$ *and* $B_{m\times n}$, *produces a chromatic QR code* $C_{m\times n}$, *such that* $A_{m\times n}$ r $B_{m\times n} \rightarrow C_{m\times n}$.

Definition 4 (Spectral Transformation (T)). *Every spectral transformation T is a binary relation that maps an image* $C_{m\times n}$ *to a dichromatic code image* Φ_λ, *that is,* $C_{m\times n}$ T $\lambda \rightarrow \Phi_\lambda$, *with* $\lambda = \{\lambda_B, \lambda_R \mid \lambda_B \neq \lambda_R\}$.

Definition 5 (Extraction). *For every extraction of dichromatic codes* $A_{m\times n}$ *and* $B_{m\times n}$, *a spectral transformation T is applied to a chromatic image* $C_{m\times n}$, *where* λ_B *is the wavelength to extract* $A_{m\times n}$ *and* λ_R *is the wavelength to extract* $B_{m\times n}$, *that is,* $C_{m\times n}$ T $\lambda_B \rightarrow A_{m\times n}$ *and* $C_{m\times n}$ T $\lambda_R \rightarrow B_{m\times n}$.

Definition 6 (Absorption or Reflection). *For every absorption or reflection, the result is obtained from a spectral transformation T of an image* $C_{m\times n}$, *such that each element* $c_{i,j} = \{y, z \mid y \neq z\}$, *with* y, $z \in \{0, 1\}$, *where* **1** *denotes reflection and* **0** *denotes absorption.*

According to Definition 3, creating a chromatic QR code involves constructing a matrix of ordered pairs C, where each pair consists of two elements taken from the two-dimensional matrices A and B. This matrix is referred to as Multiplexing (r). In accordance with Definition 5, the dichromatic QR codes are recovered through a spectral transformation involving two distinct wavelengths Φ_λ. Figure 2 illustrates this process as a general mathematical diagram, designed to allow users to select any colors they wish. The identification of each QR code can be performed using visible or non-visible wavelengths, such as UV or infrared, depending on the type of printing ink used.

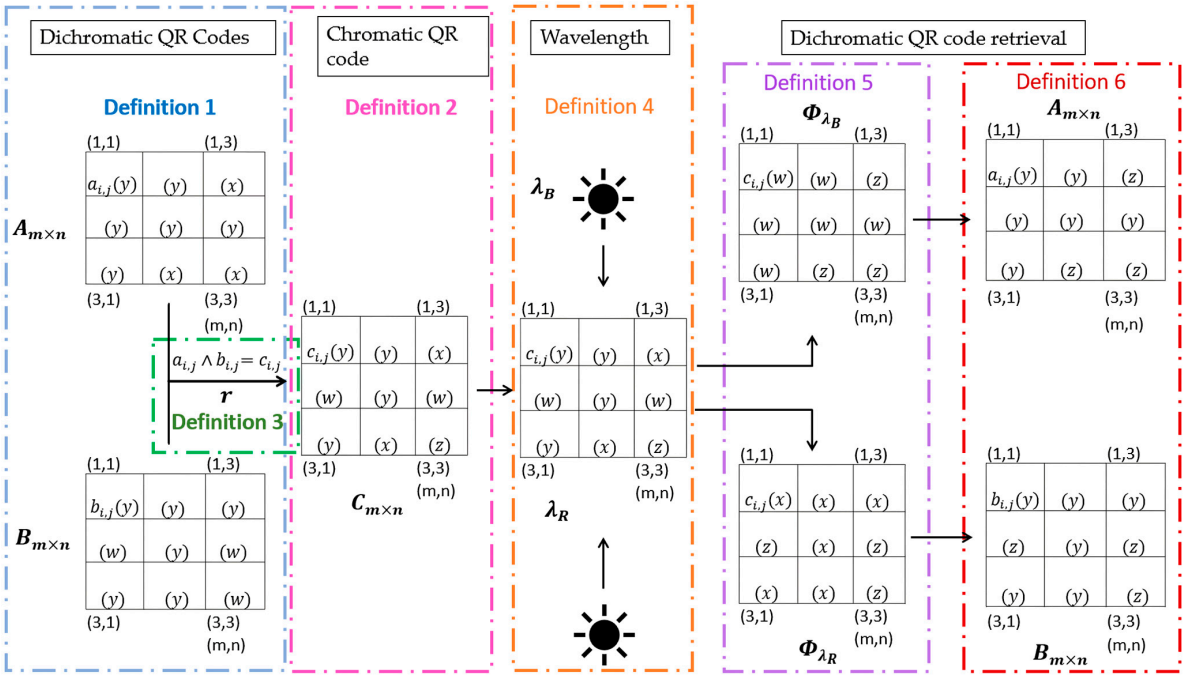


Figure 2. Multiplexing of dichromatic QR codes and their retrieval by wavelengths.

5. Case Study Based on the RGB Format

5.1. Obtaining the Tetrachromatic QR Code

For the creation of the chromatic QR code, a binary relation r is used to construct a matrix of ordered pairs, C, where each ordered pair consists of two elements taken from the two-dimensional matrices A and B. This binary relation is called Multiplexed (r), as shown in Figure 3.

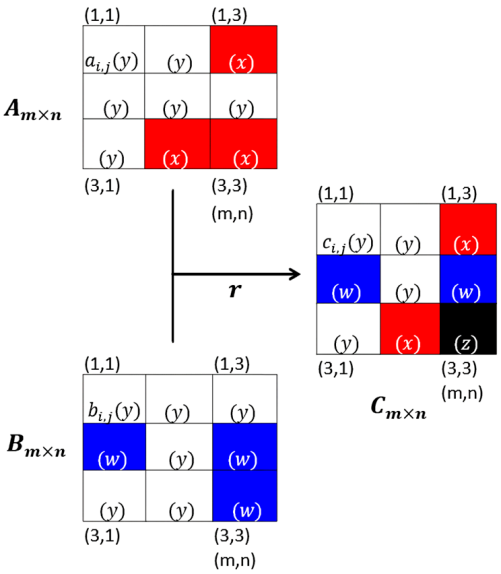


Figure 3. Multiplexing of QR-A and QR-B dichromatic codes.

As described in [28], the colors used in matrices A and B are red, blue, and white. It is essential to work with colors in the (R, G, B) channel format, where each channel takes a binary value of 0 or 1. Red and blue were selected because they represent fundamental and contrasting chromatic components within the RGB color space, which facilitates their manipulation and reliable separation through optical and image processing techniques. This choice also enables clear detection thresholds and scalability to other color formats. The specific RGB values of these colors are shown in Table 1.

Table 1. Matrix colors A (red and white) and B (blue and white).

	x	w	y	z
Channel	**Red**	**Blue**	**White**	**Black**
R	1	0	1	0
G	0	0	1	0
B	0	1	1	0
Format (R, G, B)	(1,0,0)	(0,0,1)	(1,1,1)	(0,0,0)

5.2. Recovery of the Original QR Codes

For the recovery of each dichromatic QR code, the printed image undergoes a spectral transformation process Φ_λ, with only two visible wavelengths considered: the red wavelength λ_R, ranging from 620 nm to 750 nm, and the blue wavelength λ_B, spanning from 450 nm to 495 nm. These spectral ranges are essential as they provide the precise parameters needed to manage the variation in ambient lighting during image capture.

Once the photograph resulting from the spectral transformation Φ_{λ_B} or Φ_{λ_R} has been obtained, the captured image is processed through a binarization algorithm defined by the following threshold: $0 \leftarrow 0.32 \geq pixel\ (p) \geq 0.33 \rightarrow 1$. This procedure corrects tonal

variations caused by ambient illumination fluctuations, ensuring precise dichromatic QR code segmentation. The entire process is visualized in Figure 4.

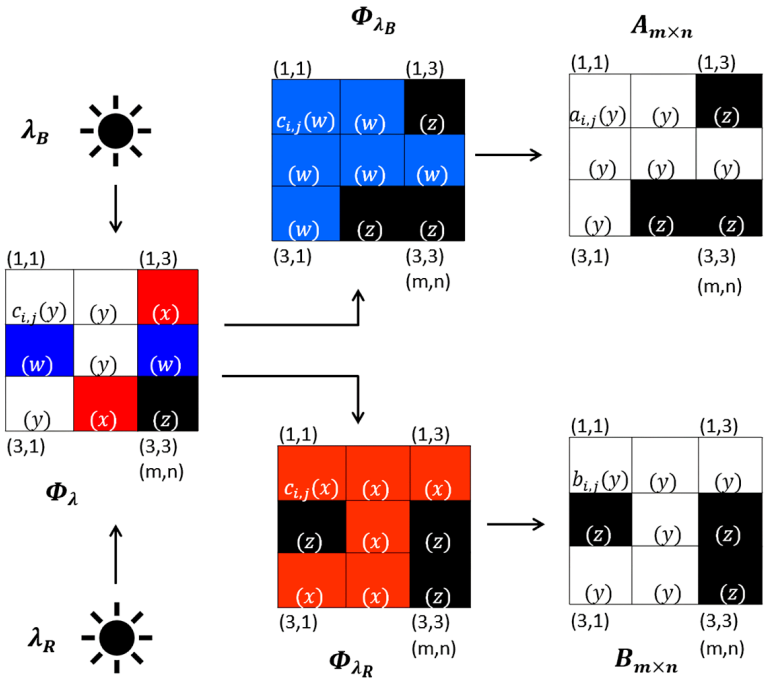


Figure 4. Recovery of dichromatic QR codes via spectral wavelengths.

6. Results

An evaluation scenario was conducted in which a chromatic QR code was generated as an access ticket to a security conference. Through dichromatic QR code A, a personalized access link is provided to each participant, consisting of the event's website with the unique ID extension assigned to the guest. QR code B, on the other hand, contains the private access token required for authentication. The AES algorithm was used to encrypt the information, offering a reliable, widely accepted, and secure method. For this implementation, the following configuration was applied, ensuring both high security and modularity of the system: AES-256, CBC (Cipher Block Chaining) mode, with PKCS7 padding. It is worth noting that, in scenarios where the tokens or information contained in the dichromatic codes is particularly sensitive, it is possible to combine both codes into an additional encrypted block and apply integrity techniques such as hash or HMAC. This implementation does not affect the main methodology of decoding via wavelengths and provides an extra layer of security according to the requirements of the use case.

6.1. Encrypted Information

1. Information 1 (IA)

   https://secure-login.com/session?id=87213

2. Encrypted information 1 (EA)

   gAAAAABocEI3WPfOFvyJ_g9OZoAKCZGJdHUwIsVw7WSf-Ia1V6iw0FylngCv3GIHPjtnaAauMSiaLklca5WFAEX5aLL-fXGhFRzsiQ8VN3chcxxEiTP6J4-Hm0LDbiVpBxPQVMDsVOUAq

3. Information 2 (IB)

   Token: 39428, Exp. 2025-11-10 T 14:00:00Z

4. Encrypted information 2 (EB)

gAAAAABocEZOjQRkg3b9NdrE25_X2bBYPgDcJYkKsH4jiu-
zoM4RF4xdz3Wh4GIiwX_vmRNIjnMBh7w4fyR6Gi7rdbxF1fS3p1fWtQppcldoUD-
PvpHiwtvWrTpCac9WGum3cDzvZUUGMs

6.2. Creation of the Chromatic QR Code

Once the corresponding encrypted information strings, identified as EA and EB, have been obtained, the process of generating the dichromatic QR codes A and B begins, as shown in Figure 5. This process consists of the encoding of EA and EB, using specific color schemes that allow each code to be distinguished and linked with its respective protected information.



(**a**) (**b**) (**c**)

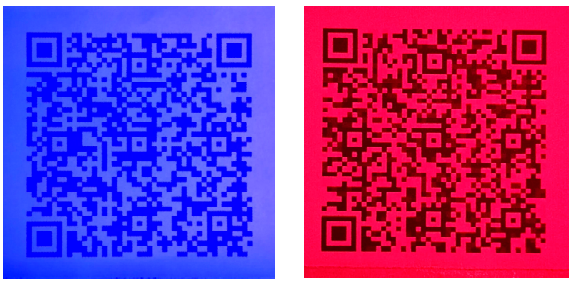
Figure 5. Creation of dichromatic codes and chromatic QR; (**a**) dichromatic QR code A of dimensions m × n; (**b**) dichromatic QR code B of dimensions m × n; (**c**) chromatic QR code $C_{m\times n}$.

A single composite chromatic code was constructed from the previously generated dichromatic QR codes A and B, as shown in Figure 5. This code visually integrates both patterns into a single graphic representation, preserving the distinctive chromatic characteristics of each one. The controlled merging of codes A and B allows multiple layers of information to be stored in a single visual support.

6.3. Identification of Dichromatic QR Codes A and B

Once QR code C has been printed, the recovery phase is divided into two stages, corresponding to the incidence of blue λ_B and red λ_R wavelengths. To minimize variations in ambient lighting and ensure greater accuracy in color recovery, a custom-designed lightbox was used for photographic capture of the QR codes. Noise variations naturally occur during photographic capture of chromatic QR codes due to environmental factors such as unwanted glare. Returning to the illumination stage described in the methodology, it is important to highlight that the duty cycle and frequency of the light beams used vary depending on the color. For example, red, being brighter than blue, requires a relatively higher duty cycle, while blue, being less bright, is used with a relatively lower duty cycle. This precise optical control not only ensures the correct recovery of the dichromatic codes but also strengthens the system's security against the threats described in Section 2. Furthermore, during photographic capture, brightness variations may occur, generating slightly different shades of the same color (e.g., wine red versus carmine red, or sky blue versus cobalt blue). These variations represent system noise, which can affect the correct identification of the codes. To mitigate this effect, precise control of the incident wavelength is employed, carefully adjusting the duty cycle and frequency of each light beam, ensuring that each dichromatic code is reliably identified and that the information is accessible only to authorized individuals.

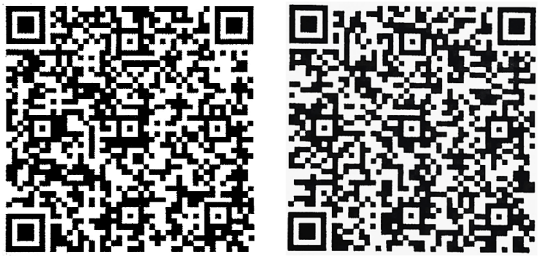
According to Definition 4, when blue-wavelength light is projected onto code Φ_{λ_B}, code $A_{m\times n}$ becomes visible, whereas projecting red-wavelength light onto the same code Φ_{λ_R} reveals code $B_{m\times n}$. Photographs of each code were taken during the process, as illustrated in Figure 6.



(**a**) (**b**)

Figure 6. Visualization of the dichromatic codes derived from QR code $C_{m\times n}$: (**a**) QR code A under blue-light illumination (Φ_{λ_B}); (**b**) QR code B under red-light illumination Φ_{λ_R}.

A binarization algorithm is used to classify the image modules into two categories, corresponding to the colors black and white. The modules assigned to the black color represent those regions with lower tonalities in the grayscale, while the modules classified as white correspond to higher tonalities. This classification is performed based on a luminance threshold defined in the interval $0 \leq p \leq 1$, where a pixel p is considered black if $0 \leq p \leq 0.32$, and white if $0.33 \leq p \leq 1$, as illustrated in Figure 7.



(**a**) (**b**)

Figure 7. Recovery of the dichromatic codes: (**a**) QR code A ($A_{m\times n}$); (**b**) QR code B ($B_{m\times n}$).

6.4. Validation of the Original QR Code Information

To validate the integrity of the recovered information, the original IA and IB strings are compared with their respective reconstructed versions, IA' and IB'. As shown in Figure 8, both matches confirm that the encoding and decoding process was performed accurately and that the data was not altered.

```
Encrypted: b'gAAAAABocEI3WPfOFvyJ_g9OZoAKCZGJdHUwIsVw7WSf-Ia1V6iw0FylngCv3GIHPjtnaAauMSiaLklca5WFAEX5aLLfXGhFRzsiQ8VN3chcxxEiTP6J4-Hw0LDbiVpBxPQVMDsVOUAq'
Decrypted: https://secure-login.com/session?id=87213
```

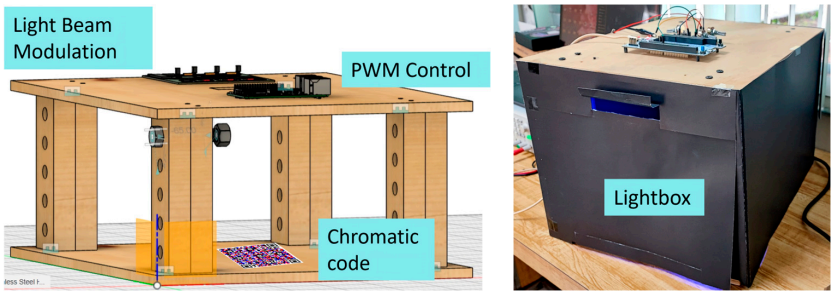
(**a**)

```
Encrypted: b'gAAAAABocEZOjQRkg3b9NdrE25_X2bBYPgDcJYkKsH4jiuzoM4RF4xdz3Wh4GIiwX_vmRNIjnMBh7w4fyR6Gi7rdbxF1fS3p1fWtQppcldoUDPvpHiwtvWrTpCac9WGum3cDzvZUUGMs'
Decrypted: Token: 39428, Exp. 2025-11-10 T 14:00:00Z
```

(**b**)

Figure 8. Validation of information integrity: (**a**) it is confirmed that IA and IA' represent the same information; (**b**) it is confirmed that IB and IB' represent the same information.

For this case study, an experimental system was employed, consisting of a lightbox that integrates an STM32 board for precise control of the wavelengths, along with a modulation circuit responsible for regulating the duty cycle and frequency of each light beam. This setup ensures reliable identification of the dichromatic QR codes, allowing each color to be detected and recovered independently. Figure 9 provides a detailed view of the system: in (a), the schematic design of the lightbox is shown, highlighting the internal arrangement of the components, while in (b), the constructed prototype is displayed, illustrating its external appearance and the complete integration of the control hardware.



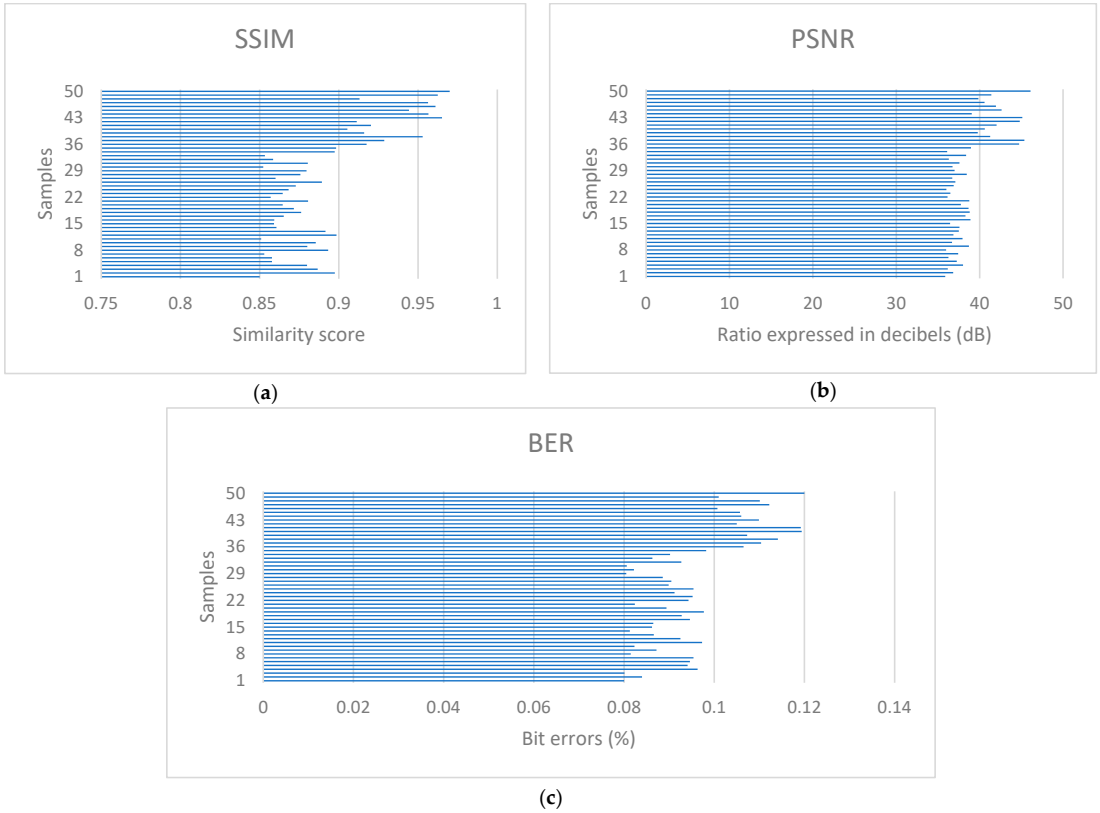
(**a**) (**b**)

Figure 9. Experimental setup: (**a**) schematic design of the lightbox; (**b**) constructed prototype.

6.5. Quantitative Evaluation of the Proposed Method Using PSNR and BER Metrics

To validate the proposed method quantitatively, a total of 50 samples were evaluated under controlled capture and processing conditions. The metrics employed were the Structural Similarity Index Measure (SSIM), the Peak Signal-to-Noise Ratio (PSNR), and the Bit Error Rate (BER).

According to the literature, SSIM values above 0.90 are indicative of high structural similarity between images, and PSNR values greater than 30 dB suggest good visual reconstruction quality. Similarly, a BER close to 0% reflects precise information recovery with minimal errors [35]. The results in this study demonstrate SSIM values between 0.85 and 0.97, SNRs ranging from 35.87 dB to 46.10 dB, and BERs between 0.08% and 0.12%, with these values presented in Figure 10. It is observed that the slight variation in errors in the last quarter of the samples is due to some encrypted strings being longer, which consequently generate a higher number of cells in the dichromatic QR codes. Although the system successfully illuminates all the cells, the increased number of cells makes small variations unavoidable during the recovery process, explaining the slight relative increase in the error rate in this section. These results reflect high fidelity in code recovery, as detailed in Table 2.



(**a**) (**b**)

(**c**)

Figure 10. Quantitative evaluation of the method using (**a**) SSIM; (**b**) PSNR; (**c**) BER metrics.

Table 2. Quantitative performance indicators of the proposed method.

Metric	Mean	Standard Deviation (σ)	Minimum	Maximum
SSIM	0.8922	0.0356	0.85	0.97
PSNR (dB)	38.8162	2.7690	35.87	46.10
BER (%)	0.0953	0.0113	0.08	0.12

7. Discussion

7.1. Proposed Method

The proposed method is based on a data multiplexing scheme that utilizes a single printed chromatic QR code, composed of red, blue, white, and black modules. By controlling the incidence of specific wavelengths (red and blue), it is possible to selectively recover two independent dichromatic QR codes, allowing the separation and decoding of distinct data sets.

Additionally, data encryption using the AES algorithm was incorporated as the first layer of security, enhancing the confidentiality of the information contained within each chromatic channel. Quantitative evaluation using SSIM, PSNR, and BER metrics showed high fidelity in recovering the modular patterns, with average values of 0.89 for the SSIM, 38.8 dB for the PSNR, and 0.095% for the BER, all within acceptable ranges reported in the literature.

7.2. Limitations and Scalability

The recovery process depends on controlled illumination conditions, which are typically achieved using a black box or dark camera enclosure to ensure precise wavelength incidence. So far, experiments have successfully multiplexed up to four dichromatic QR codes into a single chromatic QR code. However, increasing the number of input elements affects the tonal distinction between colors, complicating recovery by wavelength discrimination.

Moreover, although the resolution of the resulting chromatic QR code image remains constant, as all input matrices must have the same dimensions ($m \times n$) to create the combined code, practical scalability is limited by the perceptual and spectral distinguishability of the multiplexed colors.

7.3. Practical Application

The feasibility of transferring this study's methods from controlled laboratory conditions to real-world scenarios is promising, given that preliminary printed samples have already been produced and tested. The stability of the output image size and resolution means that it can be implemented without the need for specialized image sensors, relying instead on controlled illumination and standard photographic equipment.

Future work will focus on improving robustness against variability in ambient lighting and exploring multiplexing schemes with more than four input codes. The aim is to enhance scalability without compromising decoding accuracy.

Table 3 presents a detailed comparison of the proposed method with related works, considering factors such as capacity, encryption use, average encoding and decoding times, photographic recovery, and code multiplexing. This comparison helps to contextualize the strengths and limitations of the developed method within the state of the art.

Table 3. Comparative analysis of the proposed method and related works.

Method	Max Capacity (bytes)	Encryption Type	Encoding Time (s)	Decoding Time (s)	Use of Chromatic Codes	Photographic Recovery	Recovery by Wavelengths	Multiplexed Codes	Recovery Conditions
Proposed	5906	AES	26.14	31.58	Yes	Yes	Yes	2	Black box/controlled illumination
Toh et al. [13]	5906	—	Not reported	Not reported	No	No	No	2	Not specified

Table 3. *Cont.*

Method	Max Capacity (bytes)	Encryption Type	Encoding Time (s)	Decoding Time (s)	Use of Chromatic Codes	Photographic Recovery	Recovery by Wavelengths	Multiplexed Codes	Recovery Conditions
Wang et al. [2]	2953	—	Not reported	79.8	Yes	Yes	Yes	3	Not specified
G.-J. et al. [7]	5906	—	Not reported	Not reported	No	No	No	2	—
T. Yuan et al. [9]	5906	—	Not reported	Not reported	No	Yes	No	2	—
H. J. Galiyawala et al. [14]	41,342	—	53.157	1236.105	Yes	No	No	14	—

8. Conclusions

This work presents a methodology for encoding and retrieving information using printed chromatic QR codes with a structured chromatic configuration. The proposed approach combines optical multiplexing with controlled illumination based on specific wavelengths, enabling the selective recovery of multiple data streams from a single chromatic QR code.

The system incorporates two layers of protection: data encryption using the AES algorithm and physical separation of information through chromatic channels differentiated by their spectral response. This dual-layer security guarantees confidentiality and robustness against unauthorized access or image degradation.

The recovery process relies on controlled illumination conditions, which are typically achieved using a black box or dark camera enclosure to ensure precise wavelength incidence. Experimental results have demonstrated successful multiplexing of up to four dichromatic QR codes within a single chromatic QR code. However, increasing the number of input codes introduces challenges related to color tone distinction, which may affect recovery accuracy.

While the resolution of the output chromatic QR code image remains consistent, as the input matrices must have identical dimensions, practical scalability is limited by the perceptual and spectral distinguishability of the multiplexed colors.

Preliminary printed samples confirm the feasibility of transferring this technology from controlled laboratory settings to practical real-world applications, particularly in fields such as document verification, product authentication, and secure information transmission. The stability of image size and resolution means that implementation with standard photographic equipment and controlled illumination is possible, without the need for specialized sensors.

Future research will focus on three areas: enhancing robustness against ambient lighting variability, designing chromatic codes that are invisible to the human eye and are activated only by specific optical stimuli, and extending the multiplexing scheme to include more than two dichromatic channels without compromising readability or security.

Additionally, a comparative analysis will situate this methodology within the current state of the art, highlighting its strengths and limitations in relation to related works in this field.

Author Contributions: Conceptualization, P.N.S.A.-C., L.H.-G. and P.G.-L.; methodology, L.H.-G. and P.G.-L.; software, P.N.S.A.-C. and L.H.-G.; validation, L.H.-G. and P.G.-L.; formal analysis, P.N.S.A.-C., L.H.-G. and P.G.-L.; investigation, P.N.S.A.-C., O.U.J.-S., J.R.-H. and E.S.E.-E.; writing—original draft preparation, P.N.S.A.-C., L.H.-G. and P.G.-L.; writing—review and editing, O.U.J.-S., J.R.-H. and E.S.E.-E.; visualization, L.H.-G., P.G.-L., J.R.-H. and E.S.E.-E.; supervision, L.H.-G. and P.G.-L.; project

administration, L.H.-G., P.G.-L. and O.U.J.-S.; funding acquisition, L.H.-G. and P.G.-L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Instituto Politécnico Nacional (IPN), through the research project: SIP 20230334.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All the necessary information to reproduce the results of this paper is contained within it. In case further information is required, please contact the first author.

Acknowledgments: The authors would like to thank the Instituto Politécnico Nacional (IPN) of Mexico and the Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI) for the financial support and resources provided for this research.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

A	Dichromatic QR code A
B	Dichromatic QR code B
C	Chromatic QR code
IA	Information 1
IB	Information 2
EA	Encrypted information 1
EB	Encrypted information 2
EA′	Recovery of encrypted information 1
EB′	Recovery of encrypted information 2
IA′	Information retrieval 1
IB′	Information retrieval 2

References

1. Rouillard, J. Contextual QR Codes. In Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology (ICCGI 2008), Athens, Greece, 27 July–1 August 2008; pp. 50–55.
2. Wang, Y.-M.; Sun, C.-T.; Kuan, P.-C.; Lu, C.-S.; Wang, H.-C. Secured graphic QR code with infrared watermark. In Proceedings of the 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 13–17 April 2018; pp. 690–693. [CrossRef]
3. *AIMI 97-001*; QR Code Model 2. Automatic Identification Manufacturers International (AIMI): Warrendale, PA, USA, 1997.
4. Palaniappan, A.; Veilumuthu, L.P.; Louis, R.P.S. Enhancing Security Through QR Code and Enriched Blowfish Cryptography for Sensitive Data. In *Advancements in Smart Computing and Information Security. ASCIS 2023. Communications in Computer and Information Science*; Rajagopal, S., Popat, K., Meva, D., Bajeja, S., Eds.; Springer: Cham, Switzerland, 2024; Volume 2039. [CrossRef]
5. Amoah, G.A. QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing). *Int. J. Comput. Appl.* **2022**, *184*, 39–44. [CrossRef]
6. Trivedi, A.; Jangal, K.; Gupta, R. Phishing Detection in Advanced QR Code Attacks: Challenges and AI-Driven Solutions. *IJRASET* **2025**, *13*, 66306–66312. [CrossRef]
7. Zhang, Y.; Liu, X. Anti-counterfeiting Textured Pattern for QR Codes. *Sensors* **2023**, *23*, 795. [CrossRef]
8. *FIPS PUB 197*; Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2001.
9. Pareja, D.; Hernandez Mendez, A.; Toledo, R. Estereoscopia de dos colores, anaglifos. *Rev. Estud. Nac. Ing. Arquit.* **2011**, *2*, 2011. Available online: https://www.researchgate.net/profile/Rolando-Toledo/publication/261985555_Estereoscopia_de_dos_colores_anaglifos/links/0a85e53611c9e5cfd5000000/Estereoscopia-de-dos-colores-anaglifos.pdf (accessed on 17 July 2024).
10. Lv, Z.; Rehman, S.U.; Khan, M.S.L.; Li, H. An anaglyph 2D-3D stereoscopic video visualization approach. *Multimed. Tools Appl.* **2020**, *79*, 825–838. [CrossRef]
11. 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]

12. Xiong, L.; Zhong, X.; Xiong, N.N.; Liu, R.W. QR-3S: A High Payload QR Code Secret Sharing System for Industrial Internet of Things in 6G Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7213–7222. [CrossRef]
13. Wahsheh, H.A.M.; Al-Zahrani, M.S. QR Codes Cryptography: A Lightweight Paradigm. In *International Conference on Information Systems and Intelligent Applications*; ICISIA 2022. Lecture Notes in Networks and Systems; Al-Emran, M., Al-Sharafi, M.A., Shaalan, K., Eds.; Springer: Cham, Switzerland, 2023; Volume 550. [CrossRef]
14. Chowdary, S.; Sanjjey, A.; Subhash, R.; Rohit Mugalya, A.R.; Reddy, L.J.; Rao, R.; Ishwariya, R. QR Code Encryption Using LU Decomposition and PCA. In Proceedings of the 2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT), Karaikal, India, 4–5 July 2024; pp. 1–6. [CrossRef]
15. Godínez, A.P.; Meléndez, R.P.; Treviño-Palacios, C.G. Códigos QR cifrados como Marcas de Agua en Patrones de Difracción. In Proceedings of the SOMI XXXII, Congreso de Instrumentación, Ciudad de Mexico, Mexico, 25–27 October 2017.
16. Lin, P.-Y. Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code. *IEEE Trans. Ind. Inform.* **2016**, *12*, 384–392. [CrossRef]
17. Mehra, S.; Nishchal, N.K. Fingerprint Image Encryption Using Phase Retrieval Algorithm in Gyrator Wavelet Transform Domain Using QR Decomposition. *Opt. Commun.* **2023**, *533*, 129265. [CrossRef]
18. Rani, E.; Sakthimohan, M.; Amuthaguka, D.; Gnanapriya, P.; Naveena, G.; Ashok, A.S. QR Code-Based Login with Robust RSA Algorithm Encryption. In Proceedings of the 2023 International Conference on Intelligent Technologies for Sustainable Electric and Communications Systems (iTech SECOM), Coimbatore, India, 18–19 December 2023; pp. 474–479. [CrossRef]
19. Chou, G.-J.; Wang, R.-Z. The Nested QR Code. *IEEE Signal Process. Lett.* **2020**, *27*, 1230–1234. [CrossRef]
20. Yuan, T.; Wang, Y.; Xu, K.; Martin, R.R.; Hu, S.-M. Two-Layer QR Codes. *IEEE Trans. Image Process.* **2019**, *28*, 4413–4428. [CrossRef] [PubMed]
21. Lin, P.-Y.; Chen, Y.-H. High Payload Secret Hiding Technology for QR Codes. *EURASIP J. Image Video Process.* **2017**, *78*, 22331–22350. [CrossRef]
22. Tkachenko, W.; Puech, W.; Destruel, C.; Strauss, O.; Gaudin, J.-M.; Guichard, C. Two-Level QR Code for Private Message Sharing and Document Authentication. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 571–583. [CrossRef]
23. Gupta, M.D.; Chauhan, R.K.; Pandey, P. Security Enhancement of QR Code Using S-Boxes and Hyper-Chaotic System. In Proceedings of the 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 23–24 June 2023; pp. 1–5. [CrossRef]
24. Alajmi, M.; Elashry, I.; El-Sayed, H.S.; Farag Allah, O.S. Steganography of Encrypted Messages Inside Valid QR Codes. *IEEE Access* **2020**, *8*, 27861–27873. [CrossRef]
25. Mittal, S.; Kaur, P.; Ramkumar, K.R. Achieving Privacy and Security Using QR-Code through Homomorphic Encryption and Steganography. In Proceedings of the 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), Noida, India, 3–4 September 2021; pp. 1–6. [CrossRef]
26. Aravindh, G.; Piraisudan, R.; Murali, L.; Silwin, B.R.; Nithish, T. A Visual Cryptographic Scheme for Colour QR Codes in Defence. In Proceedings of the 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 26–27 April 2024; pp. 1–6. [CrossRef]
27. Ignacio-Cerrato, S.; Pacios, D.; Ezquerro Rodríguez, J.M.; Vázquez-Poletti, J.L.; Avilés Mariño, M.E.; Stravakakis, K.; Di Iorio, A.; Cesarano, C.; Schetakis, N. Ultracolor Multiplexing in QR Codes for Data Encryption and Transmission. In Proceedings of the Frontiers in Optics + Laser Science 2024 (FiO, LS), Denver, CO, USA, 23–26 September 2024; p. JD4A.3. [CrossRef]
28. Narayanan, S.D.; Prabhu, S.; Padma, E. Improving QR Code Security Using Multiple Encryption Layers. In Proceedings of the 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS), Coimbatore, India, 17–19 April 2024; pp. 845–848. [CrossRef]
29. Toh, S.R.; Goh, W.; Yeo, C.K. Data Exchange via Multiplexed Color QR Codes on Mobile Devices. In Proceedings of the 2016 Wireless Telecommunications Symposium (WTS), London, UK, 18–20 April 2016; pp. 1–6. [CrossRef]
30. Galiyawala, H.J.; Pandya, K.H. To Increase Data Capacity of QR Code Using Multiplexing with Color Coding: An Example of Embedding Speech Signal in QR Code. In Proceedings of the Annual IEEE India Conference (INDICON), Pune, India, 11–13 December 2014; pp. 1–6. [CrossRef]
31. Abas, A.; Azzali, F. Boosting QR Code Storage Data Text Capacity with Advanced Multiplexing Model Techniques. In *Digital Innovation in Knowledge Management. KMICe 2024. Information Systems Engineering and Management*; Mat Aji, Z., Romli, R., Packeer Mohamed, S.F., Saip, M.A., Herawan, T., Eds.; Springer: Cham, Switzerland, 2025; Volume 49. [CrossRef]
32. Abas, A.; Azzali, F.; Raduan, R.; Zainal, M. Increasing Data Storage of Coloured QR Code Using Compress, Multiplexing and Multilayered Technique. *Bull. Electr. Eng. Inform.* **2020**, *9*, 2555–2561. [CrossRef]
33. San Agustín Crescencio, P.N.; Hernández González, L.; Guevara López, P.; Ramírez Hernández, J.; Estevez Encarnación, E.S. Information Encryption with Combined QR Codes with Two Security Levels: GPG Method and Chromatic Multiplexing. In *Frontiers in Artificial Intelligence and Applications, New Trends in Intelligent Software Methodologies, Tools and Techniques, Cancún, Quintana Roo, Mexico, 23–26 September 2024*; IOS Press: Amsterdam, The Netherlands, 2024; Volume 389, pp. 85–98. [CrossRef]

34. San Agustín Crescencio, P.N.; Hernández González, L.; Guevara López, P.; Ramírez Hernández, J.; Estevez Encarnación, E.S. Integration and Information Retrieval by Multiplexing Visible Tetrachromatic QR Codes Embedded in Printed Images. *DYNA* **2025**, *100*, 307–313. [CrossRef]
35. Kotevski, Z.; Mitrevski, P. Experimental Comparison of PSNR and SSIM Metrics for Video Quality Estimation. In *ICT Innovations 2009, Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 47, pp. 357–366. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.