

A Watermarking-Assisted Framework for Secure Sharing of QR-Linked Digital Learning Resources in Inclusive Education

Shikha Yadav, Shilpa Sharma*

Research Scholar, School of Computer Applications, Lovely Professional University, Phagwara, Punjab, 144411, India

*Professor, School of Computer Science and Technology, Lovely Professional University
Phagwara, Punjab 144411, India

*Corresponding author: shilpa1381@gmail.com
Email: yadavshikha2808@gmail.com

HOW TO CITE:

Shikha Yadav, Shilpa Sharma (2026).
A Watermarking-Assisted Framework
for Secure Sharing of QR-Linked
Digital Learning Resources in
Inclusive Education.
International Journal of Special
Education, 41(4s), 648-658.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions
of the Creative Commons Attribution
(CC BY)
license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

Digital learning resources such as worksheets, visual aids, annotated diagrams, and QR-linked instructional materials are increasingly shared through mobile platforms and messaging applications in inclusive education contexts. During repeated sharing, these resources may undergo compression, resizing, or format conversion, which can make their origin difficult to verify and may allow unauthorized modification or redistribution to go unnoticed. This paper proposes an invisible QR watermarking-assisted framework for authentication and secure sharing of digital learning resources. Instead of encoding the complete document into a QR code, the proposed framework encodes compact authentication metadata, such as document identifier, institution ID, timestamp, verification URL, and resource hash, into a full-color QR payload. The QR payload is then invisibly embedded into the educational image or document-page image using a deep learning-based watermarking encoder. After transmission through compression-prone platforms, including WhatsApp image-mode sharing, a restoration module is applied before QR payload recovery. Experimental evaluation on a held-out validation set of 500 images shows that the watermarked images maintain acceptable visual quality, with PSNR of 31.02 ± 0.97 dB and SSIM of 0.9169 ± 0.0224 . Real WhatsApp image-mode validation on the same 500 transmitted images achieved an Enhanced Scan Success Rate of 82.8% and a Direct Scan Success Rate of 57.8% when the restoration module was active. Without the restoration module, both scan success rates were 0%. These results indicate the technical feasibility of the proposed framework for source verification and traceability of shared digital learning resources. The study does not evaluate classroom learning outcomes or learner-level educational impact; its contribution is limited to secure sharing, content integrity, and source authentication of QR-

linked digital learning resources.

Keywords: inclusive education; digital learning resources; QR code; invisible watermarking; image authentication; secure sharing; content integrity.

Introduction

The use of digital learning resources has grown substantially across educational systems at different levels. Teachers and special educators routinely prepare and distribute visual worksheets, annotated diagrams, instructional infographics, and QR-linked reference sheets to support learners with diverse learning needs. These materials are commonly shared through mobile messaging applications, email, institutional learning management systems, and cloud-based drives. In many resource-limited or remote settings, mobile platforms such as WhatsApp are often used for distributing educational materials when formal learning management systems are not consistently available.

In inclusive education, the integrity of learning resources carries particular importance. Materials designed for learners with cognitive, sensory, communication-related, or other support needs are often carefully structured and prepared to meet specific accessibility or instructional requirements. When such materials are shared through uncontrolled digital channels, several risks may arise. Images and document-page scans may be recompressed, resized, renamed, or cropped during transmission. A worksheet, instructional guide, or QR-linked learning resource may be modified and re-shared without clear attribution. Over time, the original source, version, or authoring institution may become difficult to identify. These issues reflect a practical challenge in informal digital distribution, especially when educational resources are repeatedly forwarded across platforms.

One widely used mechanism for linking physical or digital materials to online content is the QR code. QR codes, standardized under ISO/IEC 18004, encode text, URLs, or structured data into a machine-readable two-dimensional pattern (ISO/IEC, 2015). In education, QR codes may appear on worksheets, posters, institutional notices,

and instructional documents to provide access to supplementary material, audio-visual resources, answer keys, verification pages, or additional guidance. However, visible QR codes have limitations when used as authentication mechanisms. They can be removed through cropping, replaced with another QR code, duplicated, or visually altered. A visible QR code also occupies space on the learning material and may interfere with the layout, readability, or visual simplicity of a resource designed for a specific learner group.

Digital watermarking provides an alternative way to support authentication. In invisible watermarking, information is embedded within an image in a manner that is not easily visible during normal viewing, while still remaining recoverable during verification. The embedded information may be used for ownership protection, source identification, authentication, or traceability. Classical watermarking approaches have used spatial-domain and transform-domain embedding strategies, including pixel-based modification, DCT, DWT, and SVD-based techniques (Cox et al., 2008). These approaches provide useful foundations, but many of them are designed for relatively compact payloads and may be sensitive to combined distortions such as JPEG compression, chroma subsampling, resizing, and platform-side recompression.

Deep learning-based watermarking has extended the capability of watermark embedding and recovery by using trainable encoder-decoder architectures. Methods such as HiDDeN (Zhu et al., 2018), StegaStamp (Tancik et al., 2020), MBRS (Jia et al., 2021), and PIMoG (Fang et al., 2022) demonstrate that neural networks can learn to embed and recover hidden information under selected distortion conditions. However, many existing deep watermarking methods focus on binary messages, short text payloads, or compact

identifiers. The use of a full-color QR image as an invisible watermark payload, especially for authentication of digital learning resources, remains less explored.

This paper proposes and evaluates a watermarking-assisted framework in which compact authentication metadata is first encoded as a full-color QR image and then invisibly embedded into a digital learning resource using a deep learning-based watermarking encoder. The contribution of this paper is technical and framework-based. Its relevance to inclusive education lies in the protection of digital learning resource integrity and traceability. The proposed framework allows QR-linked learning resources to carry an invisible authentication layer that can persist through routine sharing operations and support source verification without adding visible marks to the learning image.

Literature Review

Digital Learning Resources and Inclusive Education

Inclusive education aims to ensure that all learners, including learners with disabilities and special educational needs, can access meaningful and quality learning opportunities within appropriate educational settings (UNESCO, 2017). This requires instructional materials that are accessible, structured, and suitable for different cognitive, sensory, linguistic, and communication-related needs. In inclusive education contexts, teachers and special educators often use visual worksheets, annotated diagrams, instructional charts, symbol-supported materials, and QR-linked reference sheets to support learning.

The distribution of such materials has increasingly shifted toward digital channels. In many practical settings, mobile platforms such as WhatsApp are used for quick sharing of educational images and document-page scans. While this improves access and circulation, it also creates a challenge for source verification and content integrity. When a learning resource is repeatedly shared through informal digital channels, its original source may become unclear, and the image may be recompressed, resized, renamed, or modified before reaching the final user.

QR Codes in Education

QR codes are widely used to connect printed or digital learning resources with online information (ISO/IEC, 2015). Law and So (2010) discussed the use of QR codes in educational settings and highlighted their value for connecting learning materials with digital information. In inclusive education, QR-linked resources may also help provide additional explanations, multimodal support, or structured access to supplementary material. However, visible QR codes have limitations when used for authentication, as they can be removed, replaced, or copied. For authentication purposes, a compact QR payload carrying verification metadata can be embedded invisibly as a watermark, allowing the learning resource to retain its visible layout.

Digital Watermarking

Digital watermarking is a technique in which information is embedded into a host image so that it can later be detected or recovered (Cox et al., 2008). Classical methods have used spatial-domain and transform-domain strategies including DCT, DWT, and SVD-based representations. For digital learning resources shared through mobile platforms, the watermarking problem is more complex because shared images may undergo JPEG recompression, chroma subsampling, resizing, and platform-side processing (Wallace, 1992).

Deep Learning-Based Watermarking and Restoration

Deep learning-based watermarking has improved robustness through learned encoder-decoder architectures. HiDDeN (Zhu et al., 2018) introduced an end-to-end trainable framework for data hiding with a noise layer. StegaStamp (Tancik et al., 2020) extended learned watermarking toward robust invisible hyperlink embedding under physical-world distortions. MBRS (Jia et al., 2021) improved robustness against JPEG compression using a mini-batch strategy. PIMoG (Fang et al., 2022) focused on screen-shooting noise simulation. U-Net-style architectures (Ronneberger et al., 2015) and residual denoising networks such as DnCNN (Zhang et al., 2017) are also relevant to watermark

recovery, as a restoration module placed before decoding can improve decoder input while preserving the hidden QR-related signal.

Research Gap

Most existing watermarking methods are designed for binary messages, compact text strings, or general multimedia protection. These payloads do not directly provide a scanner-readable authentication object after recovery. The specific problem of embedding compact QR-based authentication metadata into educational images, maintaining visual readability, and recovering the hidden QR after compression-prone mobile sharing represents the research gap addressed in this study.

Proposed Framework

System Overview

The proposed framework is designed to support authentication and secure sharing of QR-linked digital learning resources. It consists of four functional components: authentication metadata encoding and QR payload generation, invisible QR watermark embedding, sharing and distortion, and restoration-assisted QR recovery and verification. Figure 1 illustrates the complete system pipeline.

The main design choice is that the authentication payload is not displayed visibly on the learning resource. Instead, it is carried invisibly within the educational image or document-page image. This avoids adding a visible QR mark that may disturb the layout, readability, or visual simplicity of the learning material.

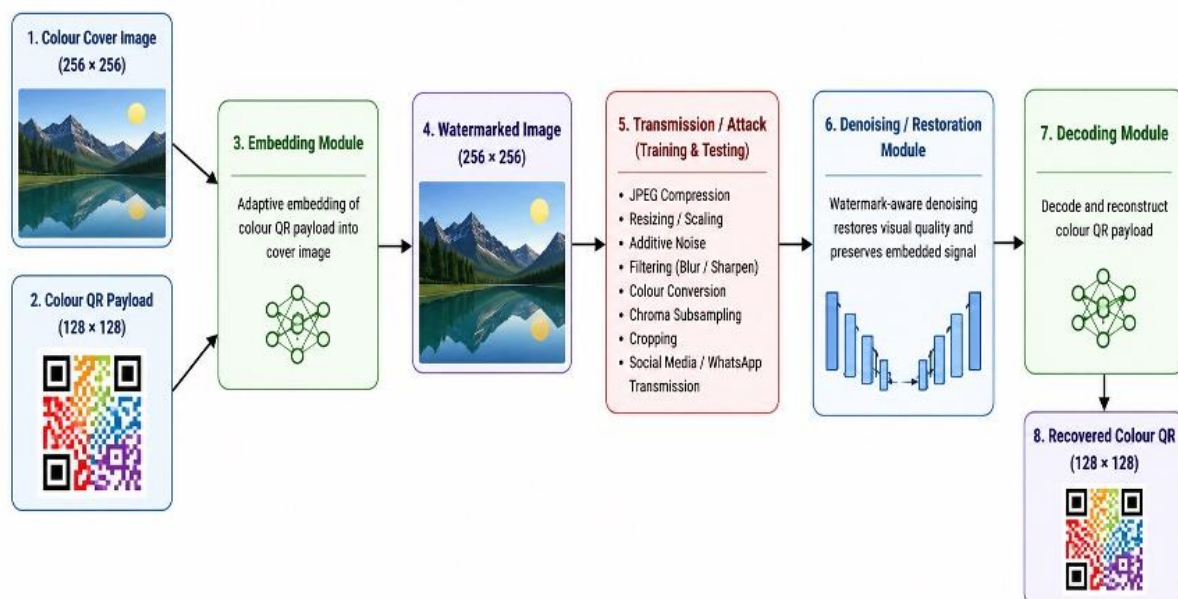


Figure 1. Overview of the proposed invisible QR watermarking pipeline. A full-color QR payload encoding compact authentication metadata is adaptively embedded into the cover image by the encoding module. The watermarked image is transmitted through compression-prone platforms such as WhatsApp. A watermark-aware denoising and restoration module processes the received image before the decoding module reconstructs the hidden QR payload for source verification.

Authentication Metadata and QR Payload Generation

The verification payload consists of compact authentication metadata, not the complete document. These fields are combined into a structured metadata string M . A QR code generator

conforming to the QR code symbology standard (ISO/IEC, 2015) encodes this metadata string into a QR payload Q represented as a 128×128 RGB image. Table 1 presents the metadata fields considered in the proposed framework.

Table 1

Authentication Metadata Fields Used for QR Payload Generation

Metadata field	Example value	Purpose
Document ID	EDU-IMG-2026-0471	Unique identifier for the learning resource
Author / institution ID	INST-EDU-AUTH	Links resource to originating educator or institution
Timestamp	2026-05-15T09:30:00Z	Records creation, publication, or version time
Verification URL	Official verification endpoint	Enables online source verification
Version number	v2.1	Identifies resource revision for version tracking
Resource hash	a3f7b2...	Supports integrity checking through a compact digest
Encrypted token	Secure authentication string	Adds optional security layer for verification

The QR payload generation step can be expressed as $Q = QR(M)$, where M represents the authentication metadata and Q represents the generated QR payload.

Invisible QR Watermark Embedding

Let C denote the cover image (the educational image) and Q the full-color QR payload. The embedding function E produces the watermarked image $W = E(C, Q)$. The encoder embeds the QR payload into the cover image using color-space guidance such as YCbCr representation, where luminance and chrominance information are treated separately. The embedding follows a residual principle: $W \approx C$. The difference $W - C$ represents the hidden embedding signal. During training, image-quality losses control distortion. PSNR and SSIM (Wang et al., 2004) are used to measure visual fidelity.

Sharing and Distortion Model

After embedding, the watermarked image W is shared through a compression-prone platform. The sharing or attack operator A represents the distortions introduced during transmission: $W_a = A(W)$. WhatsApp image-mode transmission introduces JPEG recompression, chroma

subsampling, resizing, and platform-side processing, which may weaken the hidden QR signal.

Restoration-Assisted QR Recovery

A learned restoration module R is applied to the attacked image W_a before decoding: $W_d = R(W_a)$. The restoration module follows a residual encoder-decoder design inspired by U-Net-style architectures (Ronneberger et al., 2015) and residual denoising networks (Zhang et al., 2017). Its role is to make the image more suitable for QR payload extraction while preserving the hidden signal. The decoder D then estimates the hidden QR payload: $Q' = D(W_d)$.

Verification Workflow and Evaluation Metrics

After obtaining the recovered QR image Q' , the verification process attempts to read the QR payload. If recovered successfully, the metadata string M can be extracted and used for source verification. Two scan-level evaluation modes are used. The Direct Scan Success Rate (DSSR) scans the recovered QR without additional preprocessing. The Enhanced Scan Success Rate (ESSR) applies a fixed enhancement-assisted scanning protocol before scanning. QR Module Recovery Accuracy

(QMRA) measures the proportion of correctly recovered binary QR modules averaged across all evaluation images.

Method

This study is positioned as a technical feasibility investigation. No classroom experiment was conducted. No learner outcomes, teacher surveys, or disability participant data were collected or measured.

The evaluation used a held-out validation set of 500 images treated as digital learning-resource image proxies. Each image was resized to 256×256 pixels before watermark embedding. The QR payload was generated from representative authentication metadata and rendered as a 128×128 RGB QR image. All 500 watermarked validation images were transmitted through WhatsApp image mode, and the received images were retained as inputs for restoration-assisted QR recovery.

Image quality was measured using PSNR, SSIM (Wang et al., 2004), and MSE. QR recovery was evaluated using QMRA, DSSR, and ESSR. QR scanning was performed using a standard Python-

based QR decoding library. In enhanced scanning, a fixed preprocessing protocol was applied including contrast normalization, thresholding, sharpening, and alternative scan attempts. All validation images were held out from training, and fixed random seeds were used for reproducibility.

Ethics Statement

This study is purely technical in nature. No human participants, learner data, clinical data, or personal information were collected or used at any stage. The study involved no interaction with learners, teachers, or any individuals with disabilities. Accordingly, formal ethical approval was not required for this research. All experimental data consist of publicly available benchmark images from the MS COCO 2017 validation set, which carries no personal or identifiable information.

Results

Table 2 presents the image quality measurements obtained after invisible QR watermark embedding and before transmission-related distortion. Figure 2 illustrates the visual effect of embedding on a representative cover image.

Table 2

Image Quality After Invisible QR Watermark Embedding (N = 500)

Metric	Value	Interpretation
PSNR	31.02 ± 0.97 dB	Indicates acceptable visual fidelity after embedding
SSIM	0.9169 ± 0.0224	Indicates strong structural similarity between original and watermarked images
MSE	0.000809	Indicates low pixel-level distortion across cover images



Figure 2. Visual imperceptibility of the embedded QR watermark. (a) Original cover image. (b) Watermarked image after invisible QR payload embedding. (c) Residual map amplified by a factor of 20 for visibility, revealing the spatial structure of the embedded signal. The watermarked image is visually indistinguishable from the original at normal viewing, consistent with PSNR = 31.02 dB and SSIM = 0.9169.

The PSNR value of 31.02 dB and SSIM value of 0.9169 indicate that the embedded QR payload introduces limited visual distortion. The low MSE further supports that the watermarked images remain close to their originals at the pixel level.

Table 3 presents the effect of the restoration module on QR payload recovery after WhatsApp image-mode transmission. Figure 3 shows the full distribution of per-image QMRA scores.

Table 3

Effect of Restoration Module on QR Recovery After WhatsApp Image-Mode Transmission (N = 500)

Condition	QMRA (%)	ESSR	DSSR
With restoration module	90.61 ± 19.42	414/500 (82.8%)	289/500 (57.8%)
Without restoration module	49.11 ± 6.72	0/500 (0.0%)	0/500 (0.0%)
Improvement	+41.50 pp	+414 cases	+289 cases

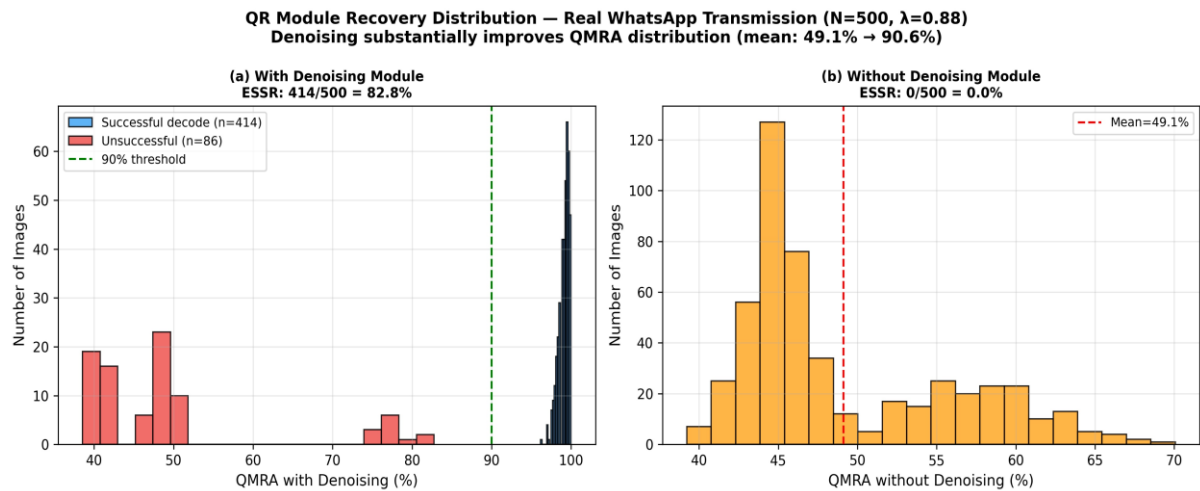


Figure 3. Distribution of per-image QMRA scores across 500 validation images after real WhatsApp image-mode transmission. (a) With the denoising and restoration module active: the majority of images achieve QMRA above 90%, with ESSR of 82.8% (414/500). (b) Without the restoration module: QMRA scores cluster between 40–65%, with a mean of 49.1%, and no image achieves a successful scan (ESSR = 0%).

Without the restoration module, QMRA reached 82.8%, and DSSR reached 57.8%. Table 4 decreased to 49.11% and neither direct nor enhanced scanning succeeded. With the restoration module active, QMRA increased to 90.61%, ESSR

Table 4

Real WhatsApp Image-Mode Scan Success Across 500 Transmitted Images

Measure	Successful cases	Total cases	Rate (%)
Direct Scan Success Rate (DSSR)	289	500	57.8
Enhanced Scan Success Rate (ESSR)	414	500	82.8

Comparative Analysis

A comparative analysis is presented to position the proposed framework relative to selected approaches for image authentication and watermarking. A direct head-to-head experimental comparison was not conducted because the compared methods were not reimplemented under

the same dataset, payload, attack model, and evaluation protocol. The comparison is therefore indicative and scope-based, focusing on functional requirements of educational resource authentication.

Table 5

Requirement-Wise Comparison of Authentication Approaches for Educational Resource Sharing

Requirement	Visible QR	Conventional watermarking	Deep watermarking	Proposed framework
Maintains visible layout of learning resource	No	Yes	Yes	Yes
Supports compact metadata authentication	Partial	Partial	Partial	Yes
Provides hidden authentication layer	No	Yes	Yes	Yes
Supports QR-based verification	Yes	No	No/Partial	Yes
Uses restoration before extraction	N/A	No	Partial	Yes
Evaluated under WhatsApp-style sharing	N/A	No	Partial	Yes

Visible QR codes satisfy QR-based verification but do not preserve a hidden authentication layer and may interfere with the layout of a learning resource. Conventional watermarking methods support hidden embedding but are not designed for QR-based verification after platform-level compression. Deep learning watermarking methods provide stronger adaptive embedding and recovery, but their payloads are commonly binary or short text strings. The proposed framework combines invisible QR metadata embedding, restoration-assisted recovery, and WhatsApp image-mode validation within an educational-resource authentication context.

Discussion

The results indicate that invisible QR watermarking can be technically feasible for supporting authentication of digital learning resources shared through compression-prone platforms. Without restoration, scan success was not achieved, whereas with restoration the framework reached an ESSR of 82.8%. This shows that the restoration module is an essential

component of the pipeline, especially when the shared image has undergone platform-side compression.

The PSNR of 31.02 ± 0.97 dB and SSIM of 0.9169 ± 0.0224 suggest limited embedding distortion. As shown in Figure 2, the residual map amplified by a factor of 20 reveals the hidden embedding signal spatially, while the watermarked image remains visually indistinguishable from the original. Since no human observer study was conducted, these values should be interpreted as evidence of limited measured distortion rather than direct evidence of perceptual invisibility.

The gap between DSSR (57.8%) and ESSR (82.8%) is important to note. This suggests that the QR structure was partially preserved in many cases but was not always sufficiently clean for direct decoding. The high standard deviation in QMRA under restoration (± 19.42 pp), visible in Figure 3, reflects per-image variability in the degree of compression introduced during WhatsApp transmission. Images with visually complex or high-

frequency content may experience different compression artifacts compared to simpler layouts.

The relevance of this framework to inclusive education is limited to resource integrity and traceability. The study does not evaluate classroom learning outcomes, learner-level accessibility impact, teacher usability, or educational effectiveness. The framework provides a technical method for helping verify whether a shared digital resource can be traced back to its intended source. From a security perspective, the hidden nature of the embedded QR watermark may reduce the risk of casual removal or unattributed redistribution, though it does not provide a complete security guarantee against active adversaries.

Limitations

Several limitations should be noted. First, this study measures only technical feasibility. No classroom learning outcomes, learner-level accessibility impacts, or disability participant evaluations were conducted. Second, the evaluation was conducted under a specific sharing condition — WhatsApp image-mode transmission on 500 images — which does not represent all digital distribution platforms. Third, DSSR (57.8%) was lower than ESSR (82.8%), indicating that many recovered QR outputs required enhancement-assisted preprocessing. Fourth, the comparison with existing

approaches is indicative and scope-based, not a strict empirical benchmark. Fifth, platform and device variability were not fully characterized. Sixth, the system does not address all aspects of document security such as legal certification, cryptographic signing, or access control.

Conclusion

This paper presented an invisible QR watermarking-assisted framework for secure sharing and source authentication of digital learning resources in inclusive education contexts. The proposed method encodes compact authentication metadata into a full-color QR payload and invisibly embeds it into an educational image. Experimental results on 500 held-out validation images showed limited embedding distortion ($\text{PSNR} = 31.02 \pm 0.97$ dB, $\text{SSIM} = 0.9169 \pm 0.0224$), and confirmed that the watermark remains imperceptible under normal viewing. Real WhatsApp image-mode validation achieved ESSR of 82.8% and DSSR of 57.8% with the restoration module active, while scan success was 0% without restoration. These findings indicate that restoration-assisted invisible QR watermarking can support source verification and traceability of shared digital learning resources. The study is limited to technical feasibility and does not claim improvement in classroom learning outcomes or learner-level educational impact.

References

- Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital watermarking and steganography* (2nd ed.). Morgan Kaufmann.
- Fang, H., Jia, Z., Ma, Z., Chang, E., & Zhang, W. (2022). PIMoG: An effective screen-shooting noise-layer simulation for deep-learning-based watermarking network. In *Proceedings of the 30th ACM International Conference on Multimedia* (pp. 2267–2275). <https://doi.org/10.1145/3503161.3548049>
- ISO/IEC. (2015). *ISO/IEC 18004:2015 — Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*. International Organization for Standardization.
- Jia, Z., Fang, H., & Zhang, W. (2021). MBRS: Enhancing robustness of DNN-based watermarking by mini-batch of real and simulated JPEG compression. In *Proceedings of the ACM International Conference on Multimedia* (pp. 41–49). <https://doi.org/10.1145/3474085.3475324>
- Law, C. K., & So, S. (2010). QR codes in education. *Journal of Educational Technology Development and Exchange*, 3(1), 85–100.
- Ronneberger, O., Fischer, P., & Brox, T. (2015). U-Net: Convolutional networks for biomedical image segmentation. In *Medical Image Computing and Computer-Assisted Intervention* (pp. 234–241). https://doi.org/10.1007/978-3-319-24574-4_28

- Tancik, M., Mildenhall, B., & Ng, R. (2020). StegaStamp: Invisible hyperlinks in physical photographs. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 2117–2126).
- UNESCO. (2017). *Defining the scope of inclusive education: Think piece*. <https://unesdoc.unesco.org/ark:/48223/pf0000265773>
- Wallace, G. K. (1992). The JPEG still picture compression standard. *IEEE Transactions on Consumer Electronics*, 38(1), xviii–xxxiv. <https://doi.org/10.1109/30.125072>
- Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4), 600–612. <https://doi.org/10.1109/TIP.2003.819861>
- Zhang, K., Zuo, W., Chen, Y., Meng, D., & Zhang, L. (2017). Beyond a Gaussian denoiser: Residual learning of deep CNN for image denoising. *IEEE Transactions on Image Processing*, 26(7), 3142–3155. <https://doi.org/10.1109/TIP.2017.2662206>
- Zhu, J., Kaplan, R., Johnson, J., & Fei-Fei, L. (2018). HiDDeN: Hiding data with deep networks. In *Proceedings of the European Conference on Computer Vision* (pp. 657–672).