Bigint Computing Journal
Volume 4, Issue 2, 2026, pp. 63-67
DOI: To be assigned
ISSN: 3032-5374
https://journal.aira.or.id/bigint/index

Performance Evaluation of BPCS Steganography for Identity Data Embedding in Academic Certificate Images

Suhardi*, Abdul Halim Hasugian

Department of Computer Science, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia

ABSTRACT
Digital academic certificates require protection against unauthorized manipulation while preserving their visual appearance. This study evaluates Bit Plane Complexity Segmentation (BPCS) as a covert identity-data embedding layer for certificate images. The MATLAB implementation converts Pure Binary Code to Canonical Gray Code, partitions bit-planes into 8 × 8 blocks, and embeds payloads in regions whose complexity exceeds a selected threshold. Performance was assessed through threshold sensitivity, payload scaling, grayscale and RGB comparison, a 40,000-bit large-payload feasibility test, consistency across five genuine certificate images, and robustness under common image manipulations. Under pristine lossless conditions, the tested payloads were recovered exactly and stego-image quality remained high, with PSNR values from 68.53 to 84.49 dB. On five genuine certificates, mean PSNR was 83.46 dB with a standard deviation of 0.63 dB. Embedding capacity declined sharply when the complexity threshold exceeded 0.5, while RGB offered additional theoretical capacity. However, resizing, cropping, rotation, noise, blur, and brightness changes produced substantial bit errors or extraction failure. The results therefore support BPCS as a high-capacity, low-distortion data-hiding layer for controlled lossless certificate workflows, but not as a standalone authentication or manipulation-robust security mechanism.
KEYWORDS: BPCS, academic certificate, steganography, PSNR, bit error rate

*Corresponding author: Suhardi, suhardi@uinsu.ac.id

Article History: Received: 2026-07-29; Accepted: 2026-08-15

1. INTRODUCTION

Academic credentials are increasingly issued, stored, and exchanged in digital form, which improves accessibility but also creates risks of alteration, duplication, and fraudulent presentation. Recent research on academic-certificate verification has therefore emphasized tamper evidence, traceability, and machine-verifiable credentials [1], [2]. Many proposed systems rely on blockchain or cryptographic verification, but such mechanisms address authenticity differently from a data-hiding approach that stores identity information directly inside the certificate image.

Steganography conceals the existence of a payload inside a digital carrier, whereas cryptographic authentication is designed to verify origin or detect unauthorized modification [3], [4]. Image steganography is commonly assessed through the trade-off among payload capacity, imperceptibility, security against steganalysis, and robustness to image processing [5], [6]. This distinction is important for academic certificates because a visually unobtrusive embedded identifier may support document handling, yet it should not be interpreted as proof of issuer authenticity by itself.

Bit Plane Complexity Segmentation (BPCS) embeds data in bit-plane regions that appear noise-like according to a complexity threshold. Its original formulation exploits the limited visual sensitivity to changes in complex binary patterns and can offer substantially higher payload capacity than simple least-significant-bit substitution [7], [8]. Related image-steganography research also shows that payload location, color-channel use, and embedding strategy can materially affect distortion and detectability [9], [10].

The practical limitation is robustness. Modern reviews distinguish conventional high-capacity steganography from methods explicitly designed to survive compression, geometric transformation, or statistical steganalysis [11], [12]. Accordingly, this study does not treat BPCS as a complete anti-forgery protocol. Instead, it evaluates whether BPCS can serve as a covert identity-data embedding and recovery layer for academic certificate images under controlled lossless conditions, while quantifying its behavior when the stego image is modified. The contribution is an application-specific performance profile covering embedding capacity, image quality, payload scaling, color mode, cross-certificate consistency, and manipulation robustness.

2. METHODOLOGY

2.1. Dataset and Computational Environment

The experiment used digital academic certificate images in lossless PNG format as cover images and 8-bit ASCII identity strings as the embedded payload. Baseline tests used one 512 × 512-pixel certificate image. Practical consistency was evaluated on five genuine certificate images issued by Universitas Islam Negeri Sumatera Utara, each scaled to 1000 pixels in width while preserving aspect ratio. Sensitive identifiers in the evaluation copies were anonymized. The deterministic implementation was executed in MATLAB R2023a on an Intel Core i5 environment.

2.2. BPCS Embedding and Extraction

a. Bit-plane Conversion**:** To mitigate the Hamming Cliff effect [7], the image is converted from Pure Binary Code (PBC) to Canonical Gray Code (CGC) using $g_i = b_i \oplus b_{i+1}$ and $g_n = b_n$, before being decomposed into eight bit-planes per color channel.

b. Complexity Segmentation: Each bit-plane is partitioned into 8×8 blocks. The normalized complexity is calculated as:

$$\boldsymbol{\alpha} = \frac{k}{112} \quad (1)$$

where k is the total adjacent bit transitions (0–1/1–0) out of a maximum 112 transitions. Blocks satisfying $\boldsymbol{\alpha} \geq \boldsymbol{\alpha_0}$ are classified as embeddable noise-like regions.

c. Embedding & Conjugation: Eligible blocks accommodate the secret data. If a payload block's complexity is below $\boldsymbol{\alpha_0}$, it undergoes XOR conjugation ($\boldsymbol{\alpha}^* = 1 - \boldsymbol{\alpha}$) to mimic noise. Out of 64 bits per block, 63 bits carry payload data, while 1 bit serves as a conjugation flag, eliminating the need for a separate metadata map.

d. Extraction: The decoder autonomously recalculates block complexity without a secret key, reads the 1-bit flag to reverse conjugation if necessary, and extracts the payload until a predefined header terminates the process.

2.3. Evaluation Measures and Experimental Scenarios

Image distortion was evaluated using Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). These measures quantify pixel-level fidelity, although MSE-based metrics do not fully represent perceptual image quality and should be interpreted alongside the application context [13], [14]. For an image with M × N pixels and C channels, the metrics are computed as follows.

$$MSE = \frac{1}{M \times N \times C} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{C} [I(i,j,k) - K(i,j,k]^2 \quad (2)$$

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (3)$$

Embedding capacity was measured as both the proportion of noise-like blocks and the net payload bits available after the one-bit conjugation flag was deducted. Recovery under pristine conditions was considered valid only when the extracted payload was bit-for-bit identical to the embedded payload. For manipulation testing, Bit Error Rate (BER) was calculated as the percentage of payload bits that differed after extraction. The experimental sequence covered threshold sensitivity, payload-size scaling, grayscale versus RGB operation, a 40,000-bit feasibility load, five-certificate consistency, and twelve image-manipulation attacks plus an unmodified baseline. The distinction between imperceptibility and robustness follows broader information-hiding evaluations in which successful low-distortion embedding does not imply survival under post-processing [15], [16], [17].

3. RESULTS AND DISCUSSION

3.1. Complexity Threshold and Embedding Capacity

The baseline 512 × 512 grayscale image contained a large set of embeddable noise-like blocks at low and moderate thresholds. Figure 1 shows that the available block proportion changed only slightly from $\alpha_0 = 0.1$ to 0.3, declined to 47.42% at $\alpha_0 = 0.4$, and then fell sharply to 19.05% at $\alpha_0 = 0.5$. At $\alpha_0 = 0.6$ and 0.7, capacity was almost exhausted. This pattern identifies α_0 around 0.3–0.4 as the practical range in the tested certificate image when high capacity is required.

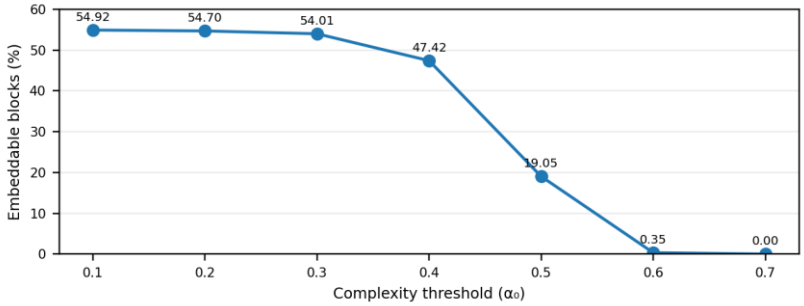

Figure 1. Embedding Capacity as a Function of the BPCS Complexity Threshold

A 96-character identity payload used only 13 blocks, so threshold changes within $\alpha_0 = 0.1$–0.5 did not materially change the observed distortion. Table 1 summarizes this low-load condition. All extractions were valid, with PSNR near 75.9 dB and MSE near 0.0017.

Table 1. Threshold Sensitivity Under a 96-Character Identity Payload

α_0	PSNR (dB)	MSE	Blocks used	Extraction
0.1	75.91	0.00167	13	Valid
0.2	75.89	0.00167	13	Valid
0.3	75.83	0.00170	13	Valid
0.4	75.89	0.00167	13	Valid
0.5	75.90	0.00167	13	Valid

3.2. Payload Size and Image Quality

Increasing the payload reduced PSNR and increased MSE because more cover blocks were replaced. The short, medium, and long payloads corresponded to approximately 0.001, 0.003, and 0.018 bits per pixel, respectively. Table 2 shows that even the 582-character test remained visually low-distortion by the reported pixel metrics, while extraction remained exact in the unmodified stego file.

Table 2. Effect of Payload Size on Stego-Image Quality

Payload	Characters	Bits	Approx. bpp	PSNR (dB)	MSE	Blocks
Short	33	264	0.001	79.62	0.00071	5
Medium	96	768	0.003	75.83	0.00170	13
Long	582	4,656	0.018	68.53	0.00912	74

3.3. Grayscale, RGB, and Large-Payload Feasibility

With the same 96-character message and $\alpha_0 = 0.3$, RGB produced a global PSNR of 79.84 dB compared with 75.83 dB for grayscale. The entire 768-bit message was accommodated in the red channel, leaving the green and blue channels unchanged. Therefore, the higher RGB PSNR is partly a consequence of averaging zero error across untouched channels rather than evidence of better per-channel fidelity. Table 3 reports the direct comparison.

Table 3. Grayscale and RGB Performance for the Same 96-Character Payload

Mode	PSNR (dB)	MSE	Payload distribution	Extraction
Grayscale	75.83	0.00170	Single channel	Valid
RGB	79.84	0.00068	768, 0, 0 bits (R,G,B)	Valid

The extended feasibility test embedded 5,000 characters, equivalent to 40,000 bits, at $\alpha_0 = 0.3$. In grayscale, the payload occupied 635 of 32,768 total bit-plane blocks, corresponding to 1.94% block utilization. In RGB, the same payload still fit within the red channel. This test demonstrates substantial capacity headroom for textual metadata, but it should not be interpreted as an experimentally established absolute saturation limit.

3.4. Consistency Across Genuine Certificate Images

Five genuine certificate images with different layouts and owner records were evaluated at $\alpha_0 = 0.3$ after proportional scaling to 1000 pixels in width. All five payloads were recovered exactly in the unmodified PNG files. The mean PSNR was 83.46 dB with a standard deviation of 0.63 dB, and the mean MSE was approximately 0.00030. Table 4 shows the certificate-level results.

Table 4. BPCS Results on Five Genuine Certificate Images at $\alpha_0 = 0.3$

Certificate	Resolution (px)	Characters	PSNR (dB)	MSE	Extraction
Certificate 01	1000 × 664	106	83.16	0.00031	Valid
Certificate 02	1000 × 667	117	83.43	0.00029	Valid
Certificate 03	1000 × 722	122	84.49	0.00023	Valid
Certificate 04	1000 × 708	131	83.44	0.00029	Valid
Certificate 05	1000 × 713	144	82.79	0.00034	Valid

The higher PSNR values relative to the 512 × 512 baseline are consistent with the lower payload-to-image ratio created by the larger image dimensions. The small dispersion observed across these five certificates supports within-sample consistency, but the sample is too limited to establish invariance across institutions, scanners, compression pipelines, or substantially different certificate designs.

3.5. Robustness Against Image Manipulation

Robustness testing produced a clear contrast with the pristine-file results. Only the unmodified baseline achieved BER = 0%. Noise, cropping, resizing, rotation, blur, and brightness adjustment changed the bit planes sufficiently to corrupt or prevent payload recovery. Table 5 summarizes the baseline and twelve manipulation conditions.

Table 5. Robustness of the Embedded Payload Under Image Manipulation

Condition	PSNR (dB)	BER (%)	Extraction status
No attack	—	0.00	Intact

Condition	PSNR (dB)	BER (%)	Extraction status
Gaussian noise, var=0.001	30.04	100.00	Failed
Gaussian noise, var=0.005	23.58	100.00	Failed
Salt & pepper, d=0.01	24.12	19.69	Corrupted
Salt & pepper, d=0.05	17.12	50.35	Corrupted
Cropping 5 px + resize	14.22	100.00	Failed
Cropping 20 px + resize	11.87	100.00	Failed
Resize 75% + restore	28.82	100.00	Failed
Resize 50% + restore	23.81	100.00	Failed
Rotation 2°	11.53	100.00	Failed
Rotation 5°	10.02	100.00	Failed
Gaussian blur, σ=1	23.67	83.96	Corrupted
Brightness +15	24.64	100.00	Failed

The failure mechanism is consistent with the algorithm design. Extraction depends on the received 8 × 8 bit-plane structure and on the complexity classification of individual blocks. Pixel-level changes can alter both the embedded bits and the set of blocks interpreted as eligible. The resulting behavior confines reliable recovery to controlled workflows that preserve the stego file without recompression or geometric transformation.

3.6. Comparative Discussion and Methodological Limitations

The observed capacity profile is consistent with the central BPCS principle that complex bit-plane regions can carry relatively large payloads with limited visible distortion [7], [8]. More recent steganography reviews likewise emphasize that high payload and imperceptibility do not automatically imply resistance to steganalysis or post-processing [5], [6], [11]. Compared with LSB-oriented approaches that modify predictable low-order positions, BPCS offers a different capacity strategy based on complexity segmentation, while color channels can provide additional embedding space [9], [10].

The robustness results are the most important practical limitation. Contemporary robust information-hiding research explicitly introduces error correction, transform-domain features, or attack-aware designs to survive compression and geometric change [15], [16]. Robust watermarking research also demonstrates that attack resistance requires design objectives beyond pristine-image PSNR alone [17]. The current implementation includes none of those mechanisms. Consequently, the reported 100% extraction rate applies only to the tested unmodified lossless files, not to certificates that have been resized, compressed, photographed, scanned, or otherwise processed.

A second limitation concerns security interpretation. BPCS conceals identity data but does not cryptographically bind that payload to the issuing institution. An attacker who understands the embedding procedure could potentially replace hidden data in a pristine file. Academic-certificate systems that require issuer authenticity and tamper evidence therefore need a cryptographic or ledger-based verification layer in addition to steganography [1], [2]. Future experiments should also expand the certificate sample, report steganalysis detectability, evaluate OCR readability after embedding, test signed or authenticated payloads, and compare BPCS against robust watermarking or error-corrected steganography under standardized attack conditions.

4. CONCLUSION

This study evaluated BPCS as a covert identity-data embedding layer for digital academic certificate images. Under unmodified PNG conditions, the implementation produced high pixel-level fidelity and exact extraction across the tested payloads. PSNR ranged from 68.53 to 84.49 dB in the pristine embedding experiments, and five genuine certificates produced a mean PSNR of 83.46 dB with a standard deviation of 0.63 dB. The complexity threshold strongly affected available capacity, with a pronounced decline above $\alpha_0 = 0.5$, while RGB provided additional theoretical embedding space.

The robustness tests substantially narrow the practical claim. Common operations such as resizing, cropping, rotation, noise, blur, and brightness modification caused partial or total payload corruption. BPCS should therefore be positioned as a high-capacity, low-distortion data-hiding mechanism for controlled lossless workflows rather than as a standalone anti-forgery or robust verification solution. Future work should combine the hidden identity payload with digital signatures or authenticated encryption, add error-correction or robust embedding mechanisms, evaluate detectability through steganalysis, and validate the approach on larger multi-institutional certificate datasets.

ACKNOWLEDGMENT

The authors thank the Department of Computer Science, Universitas Islam Negeri Sumatera Utara, for academic support during this research.

DECLARATIONS

Artificial Intelligence Use

Generative AI was used only to assist with language editing during manuscript revision. The authors reviewed the final text and remain responsible for the article content, analysis, and conclusions.

Author Contributions

Suhardi: Conceptualization, methodology, software development, experimentation, formal analysis, visualization, and writing—original draft. Abdul Halim Hasugian: Supervision, conceptual guidance, methodology review, validation, and writing—review and editing. All authors reviewed and approved the final manuscript.

Funding

This research received no external funding.

Conflict of Interest

The authors declare no conflict of interest.

Ethics Approval / Ethical Clearance

Not applicable. This study did not involve research with human participants or animals. The certificate images were used as digital test data, and sensitive identifiers in the evaluation copies were anonymized.

Data Availability Statement

The data supporting the findings of this study are presented within the article. Additional anonymized evaluation data and implementation materials may be obtained from the corresponding author upon reasonable request.

REFERENCES

[1] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A systematic literature review on blockchain-based systems for academic certificate verification," IEEE Access, vol. 11, pp. 64679–64696, 2023. doi: 10.1109/ACCESS.2023.3289598

[2] S. K. Patel, S. Chandran, and P. Kumar, "Secure digital academic certificate verification system using blockchain," International Journal of Information and Computer Security, vol. 24, no. 3/4, pp. 236–257, 2024. doi: 10.1504/IJICS.2024.141600

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999. doi: 10.1109/5.771065

[4] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010. doi: 10.1016/j.sigpro.2009.08.010

[5] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Computer Science Review, vols. 13–14, pp. 95–113, 2014. doi: 10.1016/j.cosrev.2014.09.001

[6] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey," Information Sciences, vol. 609, pp. 1451–1488, 2022. doi: 10.1016/j.ins.2022.07.120

[7] E. Kawaguchi and R. O. Eason, "Principles and applications of BPCS steganography," in Security and Watermarking of Multimedia Contents, Proc. SPIE 3528, pp. 464–473, 1999. doi: 10.1117/12.337436

[8] Y. Arianto, R. Ardiansyah, and R. J. Al Kautsar, "Implementasi steganografi menggunakan metode Bit Plane Complexity Segmentation pada citra digital," Jurnal Informatika Polinema, vol. 4, no. 1, pp. 31–34, 2017. doi: 10.33795/jip.v4i1.141

[9] K. Kordov and S. Zhelezov, "Steganography in color images with random order of pixel selection and encrypted text message embedding," PeerJ Computer Science, vol. 7, e380, 2021. doi: 10.7717/peerj-cs.380

[10] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285–287, 2006. doi: 10.1109/LSP.2006.870357

[11] R. Apau, M. Asante, F. Twum, J. B. Hayfron-Acquah, and K. O. Peasah, "Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review," PLOS ONE, vol. 19, no. 9, e0308807, 2024. doi: 10.1371/journal.pone.0308807

[12] K. D. Michaylov and D. K. Sarmah, "Steganography and steganalysis for digital image enhanced forensic analysis and recommendations," Journal of Cyber Security Technology, vol. 9, no. 1, pp. 1–27, 2025. doi: 10.1080/23742917.2024.2304441

[13] Z. Wang and A. C. Bovik, "Mean squared error: Love it or leave it? A new look at signal fidelity measures," IEEE Signal Processing Magazine, vol. 26, no. 1, pp. 98–117, 2009. doi: 10.1109/MSP.2008.930649

[14] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, 2004. doi: 10.1109/TIP.2003.819861

[15] S. Debnath, R. K. Mohapatra, and R. Dash, "Secret data sharing through coverless video steganography based on bit plane segmentation," Journal of Information Security and Applications, vol. 78, 103612, 2023. doi: 10.1016/j.jisa.2023.103612

[16] S. Debnath, R. K. Mohapatra, and R. Dash, "A robust secret data sharing through coverless video steganography based on average DC coefficient on bit plane segmentation," Computers & Electrical Engineering, vol. 120, 109766, 2024. doi: 10.1016/j.compeleceng.2024.109766

[17] N. I. Elbatawy, A. A. Karawia, M. M. El-Gayar, and Y. M. Fouda, "An improved blind watermarking scheme for color image copyright protection using Hahn moments," Scientific Reports, vol. 16, art. no. 13027, 2026. doi: 10.1038/s41598-026-42088-9