Hiding Messages in Ghost-Imaging Measurements

RESEARCHERS

Kobra Hassanzadeh (hassanzadeh.k@tabrizu.ac.ir), **Sohrab Ahmadi-Kandjani**, **Reza Kheradmand** and **Seyed Amir Mortazavi**, University of Tabriz, Iran

REFERENCES

1. J.H. Shapiro. Phys. Rev. A **78**, 061802(R) (2008).
2. H.-C. Liu and W. Chen. Opt. Lasers Eng. **130**, 106094 (2020).
3. X. Wang et al. Laser Photon. Rev. **18**, 2300820 (2024).
4. K. Hassanzadeh et al. Sci. Rep. **16**, 19054 (2026).

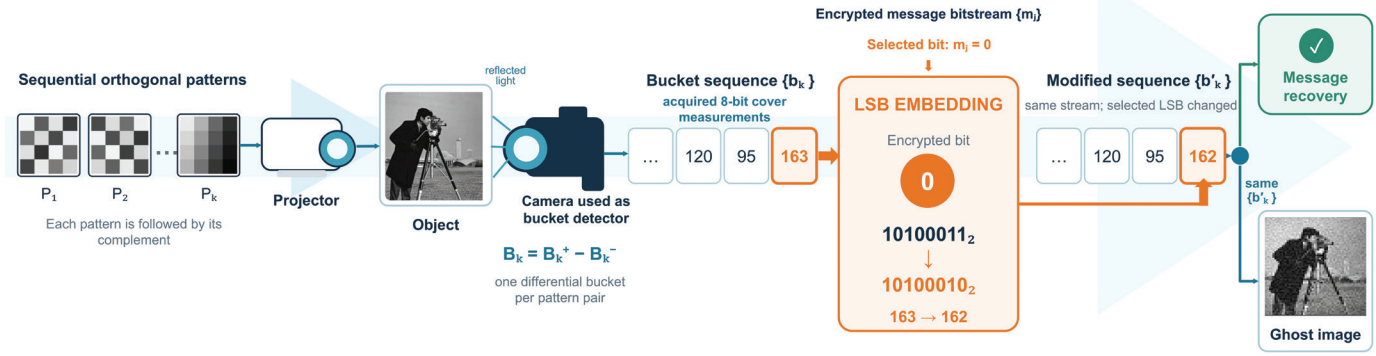
Ghost imaging forms an image in an unconventional way. Rather than recording a spatial picture directly, the system illuminates an object with known patterns, one at a time. For each pattern, a single-pixel "bucket" detector records only the total returned intensity—one value, not an image. Correlating each value with the pattern that produced it reveals the object's spatial structure. The resulting bucket sequence is the measurement stream from which the ghost image is reconstructed.[1]

That measurement stream offers an unusual place to hide information. Steganography conceals the existence of a message, unlike encryption, which obscures its content without necessarily hiding its presence. Previous ghost-imaging studies concealed the bucket data of one image within those of another,[2] while other optical approaches introduced holographic authentication elements.[3] Neither approach used least-significant-bit embedding directly in an experimentally acquired orthogonal ghost-imaging stream before reconstruction.

In new work this year, we used this pre-reconstruction stream as the cover medium itself.[4] Complementary two-dimensional discrete-cosine-transform patterns illuminated the object sequentially; their differential bucket intensities were normalized and quantized into an 8-bit sequence. A text message was converted to binary, scrambled with a logistic-map-generated keystream, and inserted into selected least-significant bits. The modified sequence served two functions: An authorized receiver could recover the message, while the ghost image could be reconstructed from the same data. The logistic map provided lightweight scrambling, not standalone cryptographic security.

We evaluated the method in simulations and a laboratory ghost-imaging experiment. For five 100 × 100 grayscale scenes at the full 10,000-bit payload, recovery was error-free, and reconstructed images remained nearly unchanged—with a peak signal-to-noise ratio of 50.24–50.78 dB and structural similarity index measure (SSIM) of 0.9961–0.9991. Across payloads from 5% to 100%, every tested message was recovered and SSIM remained above 0.996. In the experiment, complementary 64 × 64 patterns generated the measurement stream; reconstructions before and after embedding showed close visual agreement and similar intensity histograms and pixel-correlation distributions.

The advance lies not only in how the message is encoded, but where it is placed: It goes inside measurements generated by the imaging process before a spatial image exists. Under the controlled conditions and statistical comparisons reported here, the bucket stream carried hidden information while preserving its imaging function. This establishes a proof of concept for measurement-domain steganography in a compact single-pixel architecture. OPN



Measurement-domain message embedding in orthogonal ghost imaging. Each complementary pattern pair produces one differential bucket value. An encrypted message bit replaces the least-significant bit of a selected bucket value (163→162); the modified sequence supports both message recovery and ghost-image reconstruction.