

Steganography for architects

Description

default watermark

Steganography is hiding one picture (a secret or data) inside another (a host or carrier) image. As with cryptography in general, there are several reasons someone might want to hide content in this way.

- The hidden image could serve as a digital watermark. Thatâ??s to assert your claim on a picture. If someone copies it and distributes it without the ownerâ??s permission then the owner can detect and recover the watermark to prove ownership.
- Hiding one image inside another serves as a means of passing secret messages around. The secret picture could be a map or other confidential data. The carrier image is in full sight. Only someone with the right algorithm can recover the secret data.
- Steganography usually involves hiding a message in an innocuous picture so that no one else knows that it contains a secret message. Thatâ??s different to passing around encrypted files, which already advertise the fact that there is something hidden. Of course, encryption and steganography can work together to enhance image security.
- I assume that bad actors can use steganography to pass around compromising and illegal images. It would make an interesting plot vehicle in a thriller novel: the blackmailer conceals compromising pictures in public display screens or digital posters. With the right key, these reveal their secret content. Such images could conceivably be printed out as posters, to be revealed by special software on mobile phone cameras.
- From my previous post itâ??s clear that the â??least significant bitsâ?•, i.e. the bits at the low end of a binary string of the kind used to specify colour values for a pixel, could contain any kind of information, code, instructions, or malware, not just pictures. Iâ??ll demonstrate that in my next post.



default watermark

Challenges in steganography

- The size of the file containing the host and its secret image should be the same as the host on its own. So the secret image shouldnâ??t be in some extra metadata or extra bits of data. The graphic display program should display both the carrier and its secret content. The secret image should all be in the pixels. Itâ??s all in the surface.
- The secret image should be undetectable by the human eye, i.e. without some translation algorithm that makes it visible.
- The carrier plus its hidden picture should conceal the fact that thereâ??s a secret picture. Itâ??s the type of encryption where no one is aware there is something hidden. The encoding of the hidden picture may have to evade software that detects excessive noise in the image, or a compromised colour range, that would indicate something may be hidden in the image data.
- To enhance the hiddenness of the hidden image it could be encrypted in various ways, requiring a decryption key to expose the secret content.
- If the hidden picture gets scrubbed or distorted by a hacker then that should be apparent in the hacked image.
- If the secret image is to serve as a watermark to prove that it is your image then there needs to be a method of ensuring the integrity of that watermark, and that it doesnâ??t get overwritten by someone elseâ??s watermark.
- The best steganographic techniques will withstand the application of compression algorithms, scale reduction and other manipulations that erase or degrade the hidden image.

Itâ??s sobering to think that the visual field, digital imagery and screen culture generally could harbour hidden images. Presumably hackers, photo sharing platforms or camera software could hijack your own digital photographs with hidden images, and without your awareness.

Thereâ??s an architectural connection here. In so far as architecture deals in structures, functions and surfaces, steganography contributes to the dissimulation of surface.

Bibliography

- Al-Mousaoui, Mohamed. 2007. *Image Steganography: The Art of Information Hiding in Images*. Free on Kindle (no publisher shown)
- Bailey, Karen, and Kevin Curran. 2004. *Steganography: The Art of Hiding Information*. New York: BookSurge Publishing
- Borra, Surekha, Rohit Thanki, and Nilanjan Dey. 2019. *Digital Image Watermarking: Theoretical and Computational Advances*. Boca Raton, FL: CRC Press
- Salton do Prado, Kelvin. 2018. Steganography: Hiding an image inside another. *Towards Data Science*, 18 March. Available online: https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1 (accessed 18 June 2020). m
- Su, Qingtang. 2017. *Color Image Watermarking: Algorithms and Technologies*. Berlin: Walter de Gruyter
- Tanna, Sunil. 2020. *Codes, Ciphers, Steganography and Secret Messages*. High Wycombe, Buckinghamshire, England: Answers 2000 Ltd

Category

1. Architecture

default watermark

Tags

1. encryption
2. steganography

Date Created
July 4, 2020
Author
rcoyne99