## STEGANALYSIS OF INVISIBLE SECRETS PRO (JPEG FORMAT)

Invisible Secrets Pro hides the (encrypted) secret files in the header of the cover JPEG file. Structurally, the JPEG format consists of an ordered collection of parameters, markers, and entropy-coded data segments. Parameters and markers are in turn often organized into marker segments. A marker segment consists of a marker followed by a sequence of related parameters. Markers serve to identify the various structural parts of the compressed data formats. All markers are assigned two-byte codes: an X'FF' byte followed by a byte which is not equal to 0 or X'FF'. The following marker are used by ISP:

| | |
|---|---|
| X'FFD8' | Start of image |
| X'FFD9' | End of image |
| X'FFDB' | Define quantization tables |
| X'FFFE' | Comment |

The first parameter following the marker in a marker segment is the two-byte length parameter. This length parameter encodes the number of bytes in the marker segment, including the length parameter and excluding the two-byte marker.

### ISP Embedding Scheme for JPEG Cover Images

Compress the secret message (file) if the user chooses to do so

1. Encrypt the file based on the algorithm and password that user specifies. ISP supports five encryption algorithms: Blowfish, Twofish, RC4, Cast128 and GOST
2. Read the JPG file and add two X'FFFE' (comment) marker segments before the X'FFDB' marker segment (define quantization table). The second X'FFFE' marker segment ends up with X'FFFF'. The content of the comment segment is the encrypted file.

Because the data is embedded in the header between two easily identifiable markers, the detection program simply searches for the markers in the header.