Steg removal in corporate environment

Samuel Johnson
1731010035

A brief overview

- Corporate environment deals with confidential data/code like new operating system (Windows), proprietary software (Photoshop) code, etc.
- Strict policies can be enforced to restrict employees from bringing physical writeable media (Flash drives, CDs etc) to office premises.
- The only option a disgruntled employee is left with is to hide the data in a message and send via the corporate e-mail.

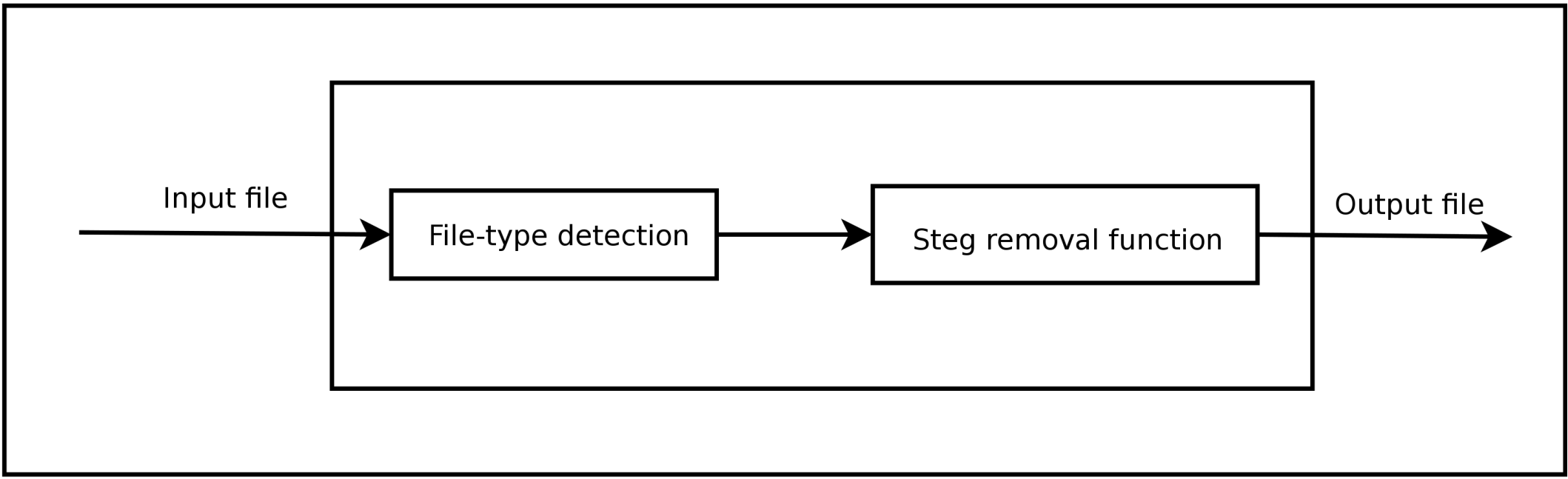
Existing systems

- Systems exists that detects certain kinds of steganography.
- However, they are largly limited by the types of steganography that they can detect.
- Newer / proprietary forms of steg which are not present in the signature database are often missed by these algorithms.

Proposed System

- The proposed system does away with the *detection* part and concentrates only on *removal* of *almost all* forms steganography.
- The system, instead of relying on signatures, uses a transformation function that deteriorates any possible forms of steganography.
- The function is file-type specific, thus a limited number of such functions is enough to cover major forms of steganography.

Design


Input file
File-type detection
Steg removal function
Output file

File-type detection implementation

- The first step to steg removal in our design is to find out the file type.
- Once the type of file is found, file-type specific operations can be carried out.
- Every file type contais a unique signature in its header called the 'Magic number'.
- The file-type is detected using this magic number.

File-type detection code

```
const char *magic_full;
magic_t magic_cookie;
magic_cookie = magic_open(MAGIC_MIME);
if (magic_cookie == NULL) {
  printf("unable to initialize magic library\n");
  return 1;
}
if (magic_load(magic_cookie, NULL) != 0) {
  printf("cannot load magic database - %s\n",
  magic_error(magic_cookie));
  magic_close(magic_cookie);
  return 1;
}
magic_full = magic_file(magic_cookie, actual_file);
```

Image Module

```
void imagemod(){
printf("Loading image specific steg module.\n");
}
```

Text Module

```
void textmod(){
printf("Loading text specific steg module.\n");
}
```

Thank you