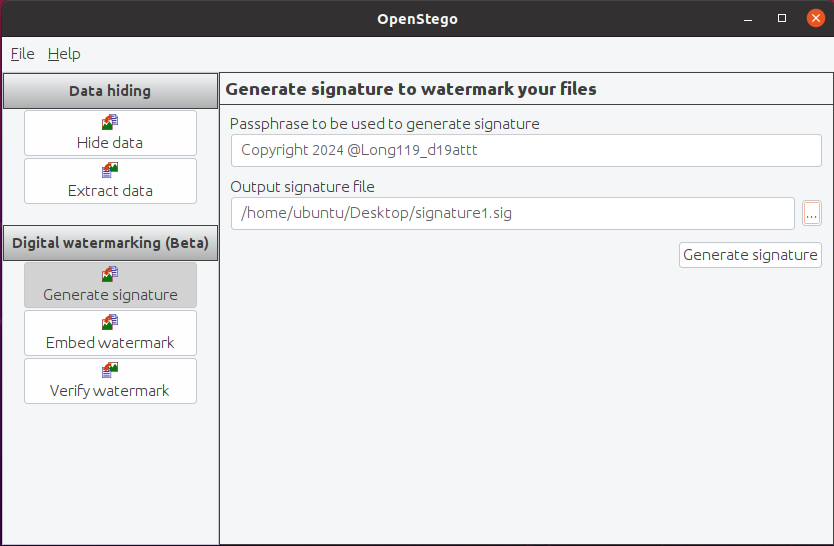
1. Demo OpenStego

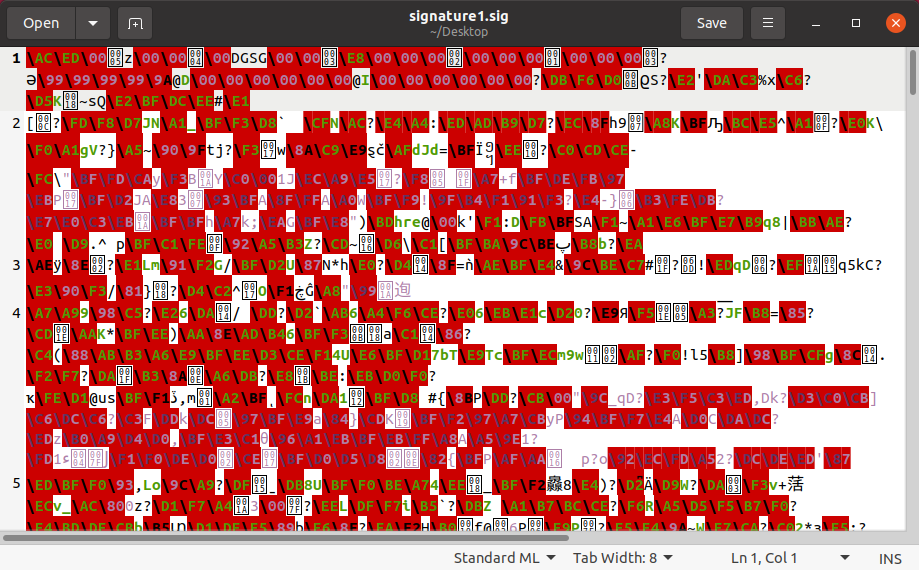
* Máy ảo:
* Ubuntu 20.04 (IP: 192.168.175.128): chứa ảnh gốc, file chữ ký.
* Kali linux (IP: 192.168.175.132): làm nhiễu ảnh đã nhúng thủy vân số.
* Các file và công cụ sử dụng trong demo:
* OpenStego: công cụ tạo chữ ký số, nhúng thủy vân và kiểm tra thủy vân.
* Signature1.sig: file chữ ký số.
* Cat03.jpg, Cat03.png, Cat03.bmp: ảnh gốc.
* Cat03\_watermarked.jpg: ảnh đã nhúng thủy vân số.
* Attack.py: file tấn công làm nhiễu ảnh đã nhúng thủy vân số gồm 17 chức năng, ví dụ: làm mờ, xoay ảnh, lật ảnh, cắt ảnh, phóng to thu nhỏ ảnh,…

1.1. Thực hiện tạo file chữ ký và nhúng thủy vân số vào ảnh

* Tạo file chữ ký: mở OpenStego, chọn chức năng “Generate signature”, chọn cụm từ làm chữ ký và nơi lưu file chữ ký, rồi bấm “Generate signature”.

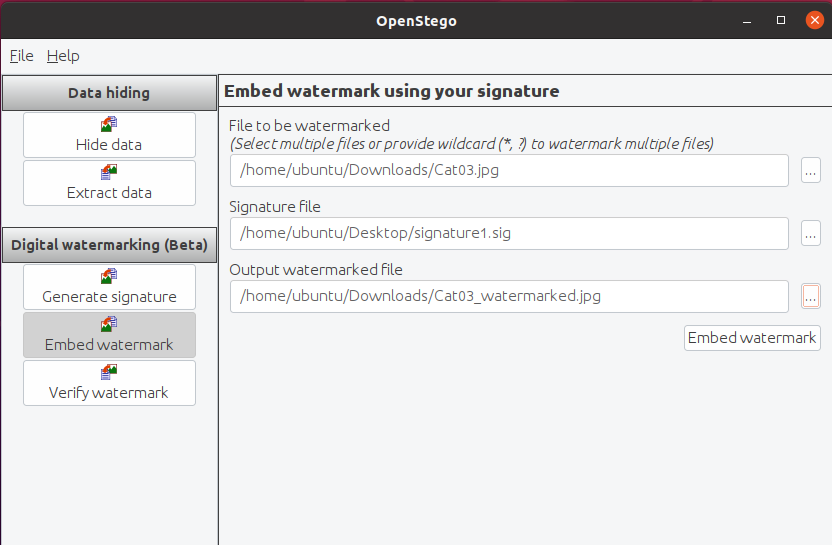


(Tạo file chữ ký)

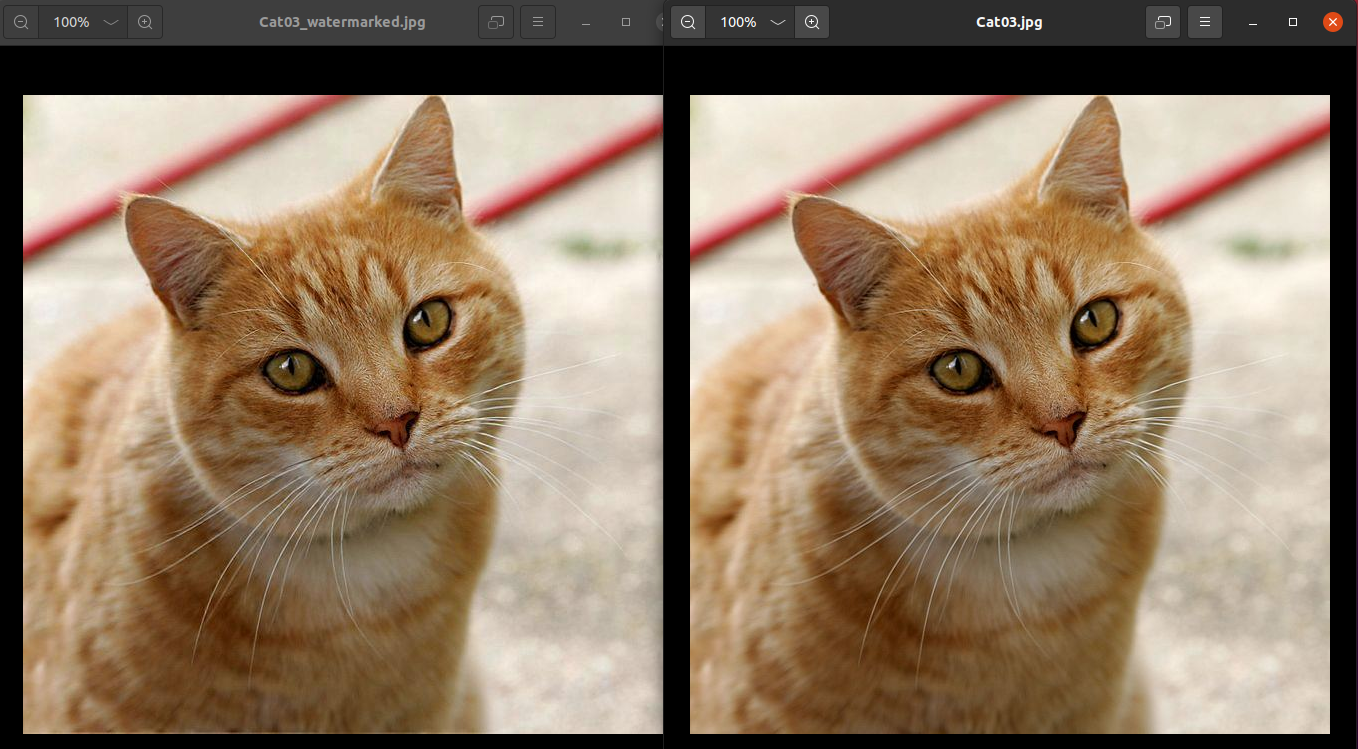


(Tạo chữ ký thành công)

* Nhúng thủy vân số: trong OpenStego, chọn chức năng “Embed watermark”, chọn file muốn nhúng thủy vân số, file chữ ký và vị trí lưu file đã nhúng thủy vân số rồi bấm “Embed watermark”.



(Thực hiện nhúng thủy vân số)

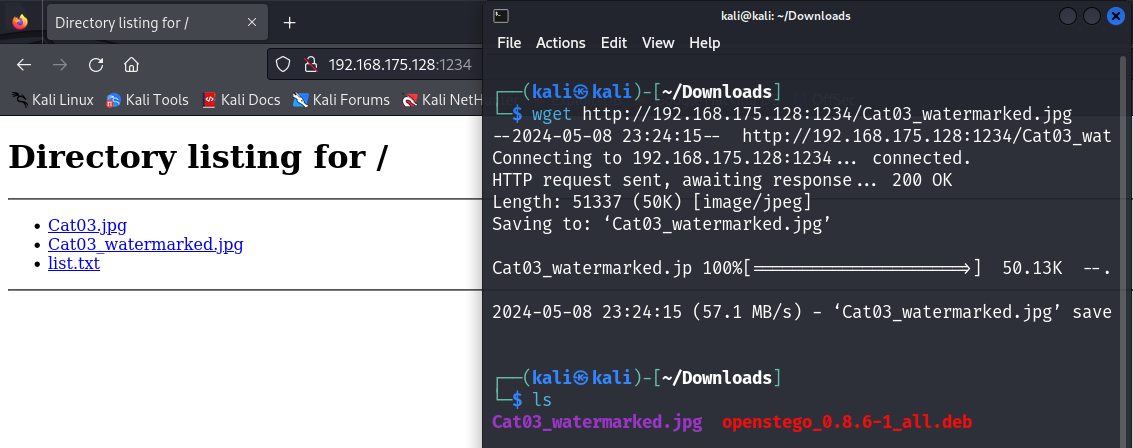


(So sánh ảnh đã nhúng thủy vân số và ảnh gốc)

* Đưa ảnh đã nhúng thủy vân số lên mạng.

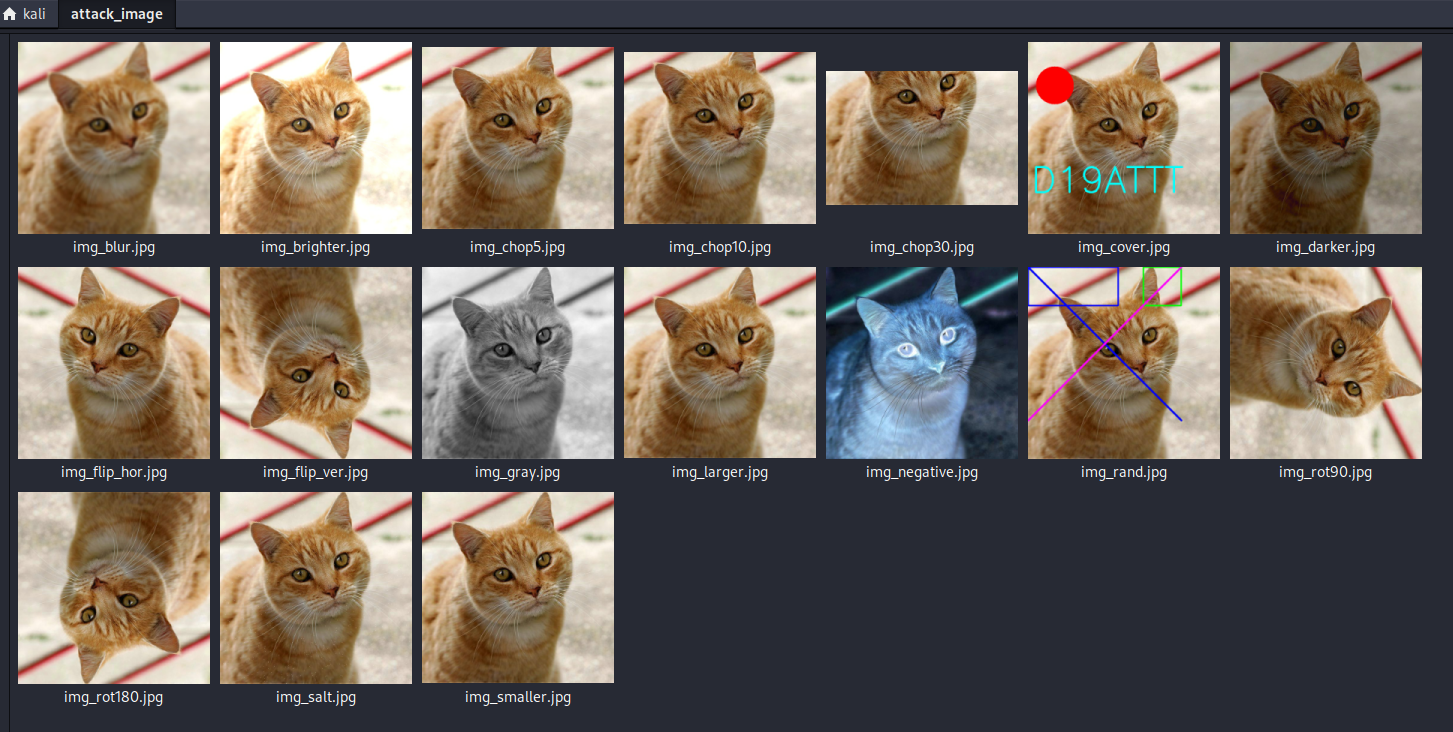
1.2. Tấn công làm nhiễu ảnh đã nhúng thủy vân số

* Truy cập vào địa chỉ IP của máy Ubuntu để lấy ảnh đã nhúng thủy vân số.



(Tải ảnh đã nhúng thủy vân số)

* Tiến hành tấn công làm nhiễu: chạy file attack.py bằng python3 rồi nhập đường dẫn đến ảnh vừa tải, ảnh sau khi làm nhiễu được lưu trong thư mục attack\_image.

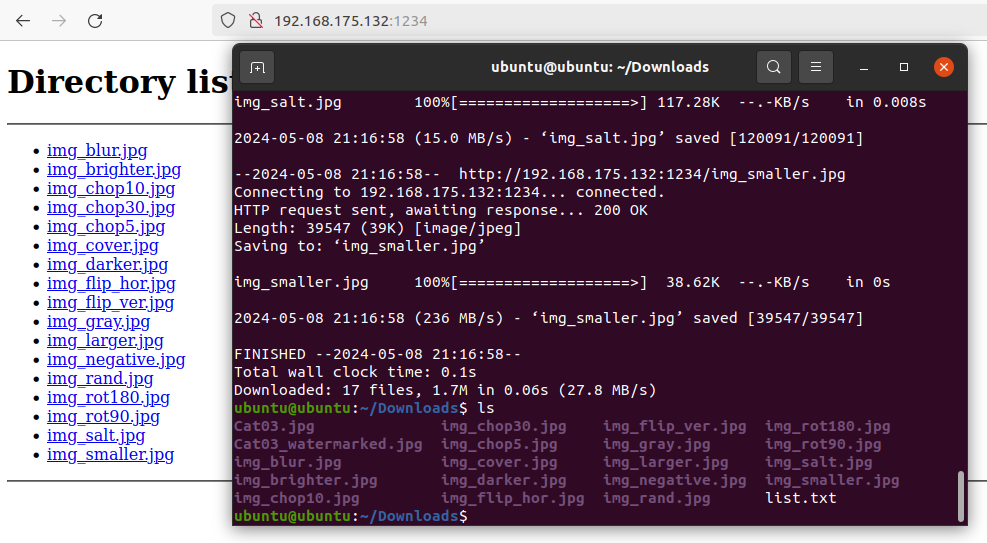


(Ảnh sau khi thực hiện tấn công)

* Gửi ảnh đã bị làm nhiễu lên mạng.

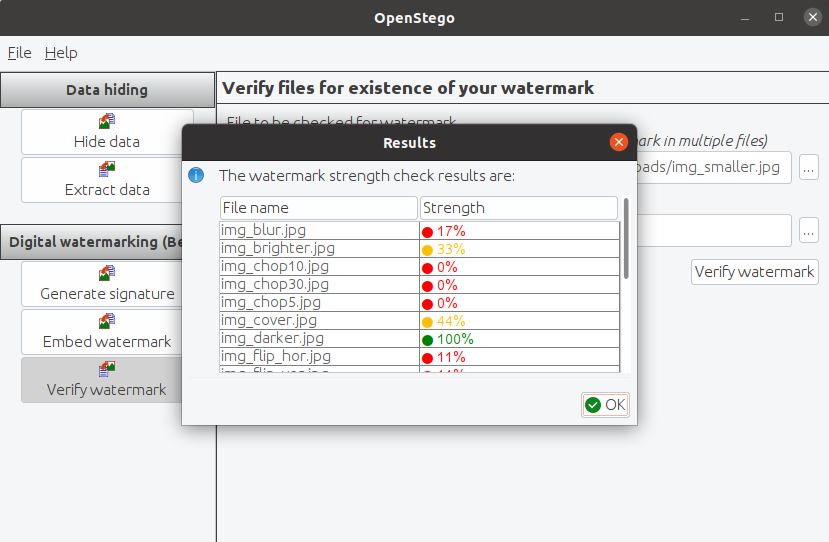
1.3. Xác thực thủy vân số

* Truy cập địa chỉ IP của máy Kali trên trình duyệt và tải ảnh bị làm nhiễu về.



(Tải ảnh bị làm nhiễu)

* Thực hiện xác thực thủy vân số: trong OpenStego, chọn chức năng “Verify watermark”, chọn ảnh muốn xác thực và chọn file chữ ký, rồi bấm “Verify watermark”.



(Thực hiện xác thực thủy vân số)

|  |  |
| --- | --- |
| **Tên ảnh** | **Độ chính xác** |
| img\_blur.jpg | 17% |
| img\_brigher.jpg | 33% |
| img\_chop10.jpg | 0% |
| img\_chop30.jpg | 0% |
| img\_chop5.jpg | 0% |
| img\_cover.jpg | 44% |
| img\_darker.jpg | 100% |
| img\_flip\_hor.jpg | 11% |
| img\_flip\_ver.jpg | 11% |
| img\_gray.jpg | 88% |
| img\_larger.jpg | 0% |
| img\_negative.jpg | 0% |
| img\_rand.jpg | 33% |
| img\_rot180.jpg | 0% |
| img\_rot90.jpg | 11% |
| img\_salt.jpg | 56% |
| img\_smaller.jpg | 44% |

(Bảng đo độ chính xác của ảnh định dạng jpg)

* Làm tương tự với ảnh Cat03.png và Cat03.bmp, ta có 2 bảng sau:

|  |  |
| --- | --- |
| **Tên ảnh** | **Độ chính xác** |
| img\_blur.png | 17% |
| img\_brigher.png | 75% |
| img\_chop10.png | 0% |
| img\_chop30.png | 0% |
| img\_chop5.png | 0% |
| img\_cover.png | 44% |
| img\_darker.png | 100% |
| img\_flip\_hor.png | 0% |
| img\_flip\_ver.png | 0% |
| img\_gray.png | 100% |
| img\_larger.png | 0% |
| img\_negative.png | 0% |
| img\_rand.png | 38% |
| img\_rot180.png | 0% |
| img\_rot90.png | 0% |
| img\_salt.png | 56% |
| img\_smaller.png | 44% |

(Bảng đo độ chính xác của ảnh định dạng png)

|  |  |
| --- | --- |
| **Tên ảnh** | **Độ chính xác** |
| img\_blur.bmp | 17% |
| img\_brigher.bmp | 75% |
| img\_chop10.bmp | 0% |
| img\_chop30.bmp | 0% |
| img\_chop5.bmp | 0% |
| img\_cover.bmp | 50% |
| img\_darker.bmp | 100% |
| img\_flip\_hor.bmp | 0% |
| img\_flip\_ver.bmp | 0% |
| img\_gray.bmp | 100% |
| img\_larger.bmp | 0% |
| img\_negative.bmp | 0% |
| img\_rand.bmp | 38% |
| img\_rot180.bmp | 0% |
| img\_rot90.bmp | 0% |
| img\_salt.bmp | 44% |
| img\_smaller.bmp | 44% |

(Bảng đo độ chính xác của ảnh định dạng bmp)

1.4. Nhận xét

* Định dạng ảnh có ảnh hưởng đến độ chính xác, ảnh sử dụng định dạng nén mất dữ liệu (jpg) cho độ chính xác kém, còn ảnh sử dụng định dang nén không mất dữ liệu (png) và không nén (bmp) cho độ chính xác tốt hơn.
* Thuật toán DWT Dugar không thể xác định được thủy vân số với kiểu tấn công cắt, xoay, lật, phóng to và ảnh âm bản.
* Thuật toán DWT Dugar thể hiện tốt trước kiểu tấn công thay đổi độ sáng và màu.