Stecrypt - dokumentacja

Piotr Banaszkiewicz

09.03.2011

Spis treści

1 Zasada działania programu Stecrypt

Program Stecrypt służy do ukrywania w obrazach tekstów i odczytywania ich stamtąd. Interfejs programu pozwala na wprowadzanie klucza, którym program posługuje się w trakcie szyfrowania i deszyfrowania.

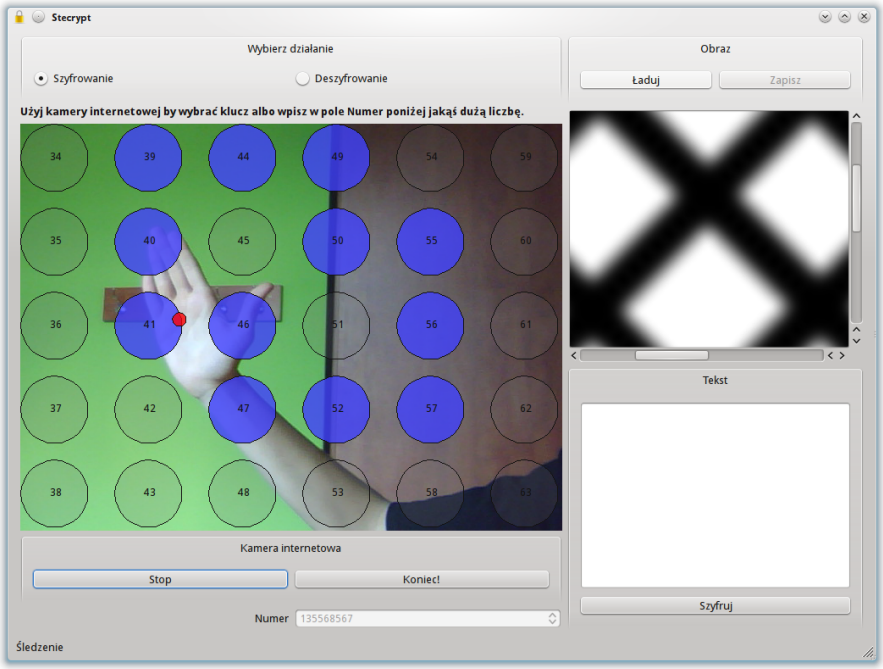
To, co sprawia, że Stecrypt jest wyjątkowy, to możliwość wprowadzania klucza za pomocą kamery internetowej śledzącej położenie pewnego punktu.

Po uruchomieniu programu należy wybrać, co chce się robić: szyfrować czy deszyfrować. Następnie można uruchomić kamerę internetową, kliknąć lewym przyciskiem myszy na śledzonym obiekcie i za jego pomocą zaznaczać kółka. Te posłużą do wyliczenia wartości klucza szyfrującego/deszyfrującego. Po skończonym zaznaczaniu kółek należy nacisnąć "Koniec!".

Alternatywą, np. w sytuacji braku kamery, jest możliwość wybrania liczby-klucza ręcznie.

Kolejnym krokiem jest załadowanie obrazu (źródłowego lub już poddanego steganografii), ewentualne wprowadzenie tekstu do zaszyfrowania oraz kliknięcie przycisku "Szyfruj" lub "Deszyfruj".

Cały program jest stworzony z wykorzystaniem frameworka Qt w wersji 4.



Rysunek 1: Zrzut ekranu działającego programu Stecrypt.

2 Kamera internetowa

Uwaga! Program Stecrypt został napisany z myślą o kamerach internetowych przesyłających obraz w rozdzielczości 640x480 i w odpowiednim formacie. Autor

programu nie daje gwarancji, że Stecrypt będzie działał poprawnie z innymi konfiguracjami, chociaż nie jest to wykluczone.

Do obsługi kamery wykorzystana została biblioteka opencv w wersji 2. Ponadto w celu wyświetlania obrazu stworzono nowy widżet Qt.

Algorytmem używanym do śledzenia punktu jest algorytm optical flow (przepływ optyczny) metodą Lucasa–Kanade'a. Biblioteka opencv daje możliwość bardzo łatwego wykorzystania tego algorytmu.

Na podstawie położenia śledzonego punktu zaznaczane są koła. Przy rozdzielczości 640x480 px jest ich 30, rozłożonych w pięciu wierszach po sześć kół.

Wartość klucza obliczana jest z zaznaczonych kółek. Ich ID (wpisany w środku koła) to wykładnik potęgi o podstawie 2. Ogólny wzór jest taki:

$$k = \sum_{n \in \mathbb{A}} (2^n + 2^{n-32})$$

gdzie $\mathbb{A}$ to zbiór identyfikatorów wszystkich zaznaczonych kółek.

Wydajność algorytmu Lucasa-Kanade'a może pozostawiać trochę do życzenia, szczególnie gdy użytkownik korzysta z bardzo szybkiej kamery. Gwoli ścisłości: algorytm korzysta z dwóch ramek obrazu, jednakże nie kolorowych, lecz monochromatycznych. Inaczej aplikacja zacinałaby się o wiele mocniej.

3 Szyfrowanie, deszyfrowanie i steganografia

Szyfrowanie jak i deszyfrowanie korzysta z algorytmu XOR. Jest to bardzo łatwy algorytm do zaimplementowania. Jego charakterystyczną cechą jest identyczność funkcji szyfrującej i deszyfrującej. Mianowicie:

$$B = A \oplus k$$

$$A = B \oplus k$$

Tekst wejściowy, o maksymalnej długości 512 znaków, jest "przedłużany" o tyle znaków o wartości 1 (`char k = 1`), ile trzeba, by jego długość była podzielna przez 8.

3.1 Szyfrowanie

Klucz sam w sobie ma długość 8B (typ: `unsigned long long`), dlatego tekst wejściowy musi zostać podzielony na 8-bajtowe kawałki, które dopiero poddawane są operacji alternatywy wykluczającej. Wynik tej operacji jest dzielony z powrotem na bajty i zapisywany w tablicy znaków. Dopiero po zaszyfrowaniu całego tekstu następuje operacja zapisywania w obrazie, czyli steganografia. Po dwa bity z każdego bajta zapisywane są na najmniej znaczących bitach kolorów zielonego i niebieskiego. Zapisywanie to polega na sprawdzeniu podzielności przez 2 oraz podniesieniu/zmniejszeniu wartości danego koloru o 1.

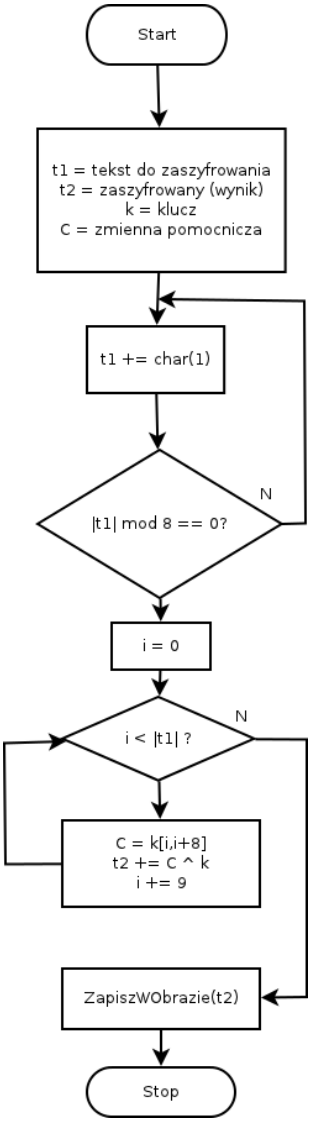
3.2 Deszyfrowanie

Deszyfrowanie polega na odczytywaniu wartości 8 bajtów z 32 kolejnych pikseli. Następnie te bajty poddawane są operacji alternatywy wykluczającej i dodawane do tekstu wyjściowego.

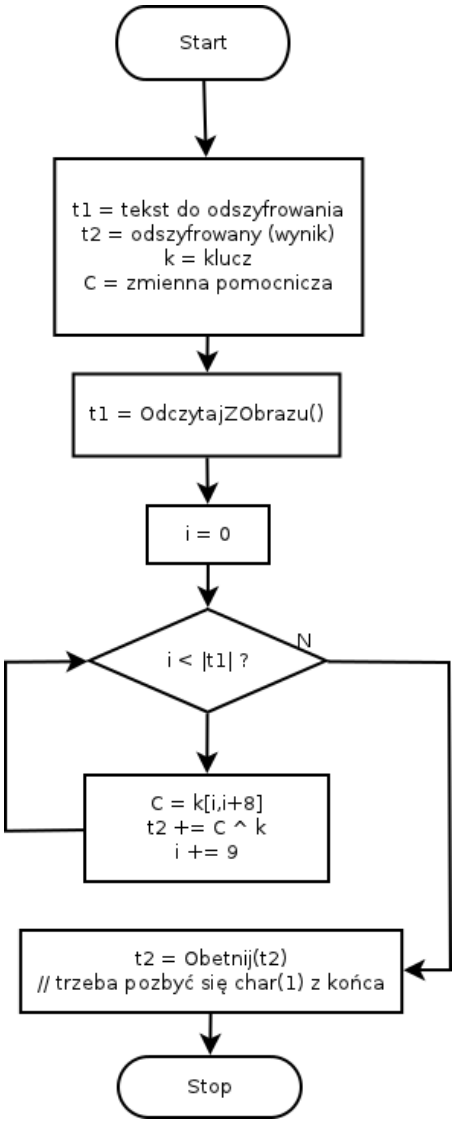
3.3 Formaty graficzne

Ze względu na kompresję stratną, wiele formatów graficznych może nie być w stanie współpracować z wykorzystanym tutaj algorytmem do steganografii. Dlatego też aplikacja Stecrypt wymusza stosowanie, tak do szyfrowania, jak i do deszyfrowania, obrazów BMP o głębi koloru minimum 24 bity (po 8 bitów na każdy kolor).

3.4 Schematy blokowe



Rysunek 2: Uproszczony schemat blokowy szyfrowania.



Rysunek 3: Uproszczony schemat blokowy deszyfrowania.

4 Kompilacja i uruchomienie

Aplikacja, jak zostało wspomniane, wymaga do działania i do kompilacji bibliotek Qt (w wersji minimum 4.5) oraz OpenCV (min. 2.0). Również program make powinien być zainstalowany.

Jeśli biblioteki te są już zainstalowane w systemie, aplikację można skompilować wydając następujące polecenia:

```
$ qmake stecrypt.pro -r -spec linux-g++ CONFIG+=release
$ make -w
```

Inną opcją kompilacji jest import całego projektu w programie Qt Creator.

Uruchomienie skompilowanego pliku wykonywalnego sprowadza się do:

```
$ ./stecrypt
```

Dostarczona w archiwum skompilowana wersja jest przeznaczona na platformę x86, chociaż niewykluczone, że zadziała także i na x86_64.

5 Licencja

Program Stecrypt jest wydany na licencji GNU LGPL, której tekst jest zamieszczony poniżej.

```
                   GNU LESSER GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.


  This version of the GNU Lesser General Public License incorporates
the terms and conditions of version 3 of the GNU General Public
License, supplemented by the additional permissions listed below.

  0. Additional Definitions.

  As used herein, "this License" refers to version 3 of the GNU Lesser
General Public License, and the "GNU GPL" refers to version 3 of the GNU
General Public License.

  "The Library" refers to a covered work governed by this License,
other than an Application or a Combined Work as defined below.

  An "Application" is any work that makes use of an interface provided
by the Library, but which is not otherwise based on the Library.
Defining a subclass of a class defined by the Library is deemed a mode
of using an interface provided by the Library.

  A "Combined Work" is a work produced by combining or linking an
Application with the Library.  The particular version of the Library
with which the Combined Work was made is also called the "Linked
Version".

  The "Minimal Corresponding Source" for a Combined Work means the
Corresponding Source for the Combined Work, excluding any source code
for portions of the Combined Work that, considered in isolation, are
based on the Application, and not on the Linked Version.

  The "Corresponding Application Code" for a Combined Work means the
object code and/or source code for the Application, including any data
and utility programs needed for reproducing the Combined Work from the
Application, but excluding the System Libraries of the Combined Work.

  1. Exception to Section 3 of the GNU GPL.

  You may convey a covered work under sections 3 and 4 of this License
without being bound by section 3 of the GNU GPL.
```

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among

these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

5.1 Licencja wykorzystanych bibliotek

Biblioteka Qt jest również na licencji GNU LGPL, natomiast biblioteka OpenCV wydawana jest na licencji BSD. Każda z nich pozwala na wykorzystywanie programu w celach edukacyjnych.

Spis rysunków