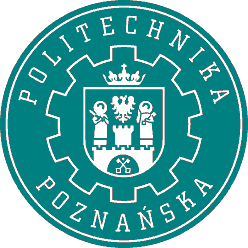
**POLITECHNIKA POZNAŃSKA**

**WYDZIAŁ INFORMATYKI**

**INSTYTUT INFORMATYKI**

Zastosowanie steganografii do wymiany informacji na forum internetowym

KOZA  
BARTOSZ KOSTANIAK

Promotor: prof. dr hab. inż. Jerzy Brzeziński   
Instytut Informatyki   
Politechniki Poznańskiej

**KARTA PRACY DYPLOMOWEJ**

(kserokopia z podpisami)

**Spis treści**

[1. Wstęp 3](#_Toc438506422)

[1.1 Cel i zakres pracy 4](#_Toc438506423)

[1.2 Struktura pracy 4](#_Toc438506424)

[2. Wprowadzenie 5](#_Toc438506425)

[2.1 Rys historyczny 5](#_Toc438506426)

[2.2 Idea steganografii 5](#_Toc438506427)

[2.3 Nośniki informacji umożliwiające zaimplementowanie steganografii 5](#_Toc438506428)

[2.4 Narzędzia komunikacji w Internecie 5](#_Toc438506429)

[2.4.1 Czat internetowy 5](#_Toc438506430)

[2.4.2 Forum internetowe 5](#_Toc438506431)

[2.5 Steganografia w plikach graficznych 5](#_Toc438506432)

[3. Przedstawienie użytych technologii 6](#_Toc438506433)

[3.1 NodeJS 6](#_Toc438506434)

[3.2 MeteorJS 6](#_Toc438506435)

[3.3 MongoDB 6](#_Toc438506436)

[3.4 AngularJS (wersja 1.x) 6](#_Toc438506437)

[3.5 Preprocessory 6](#_Toc438506438)

[3.5.1 CoffeeScript 6](#_Toc438506439)

[3.5.2 Jade 6](#_Toc438506440)

[3.5.3 Less 6](#_Toc438506441)

[3.6 Narzędzia do zarządzania projektem 6](#_Toc438506442)

[3.6.1 Git 6](#_Toc438506443)

[3.6.2 TravisCI 6](#_Toc438506444)

[3.7 Narzędzia do testowania 6](#_Toc438506445)

[3.7.1 GulpJS 6](#_Toc438506446)

[3.7.2 Jasmine 6](#_Toc438506447)

[3.7.3 Karma 6](#_Toc438506448)

[3.7.4 Protractor 6](#_Toc438506449)

[4. Budowa aplikacji 7](#_Toc438506450)

[4.1 Struktura plików i folderów 7](#_Toc438506451)

[4.2 Modele w bazie danych 7](#_Toc438506452)

[4.3 Jednostki w aplikacji 7](#_Toc438506453)

[5. System uwierzytelniania i autoryzacji 8](#_Toc438506454)

[5.1 Rejestrowanie i logowanie użytkowników 8](#_Toc438506455)

[5.2 Role 8](#_Toc438506456)

[5.3 Struktura ról 8](#_Toc438506457)

[6. Algorytm steganograficzny 9](#_Toc438506458)

[6.1 9](#_Toc438506459)

[7. Zakończenie 10](#_Toc438506460)

[Literatura 11](#_Toc438506461)

# Wstęp

Wraz z wykształceniem się u człowieka umiejętności komunikacji powstał problem skutecznego przekazywania tajnych informacji, takich których zawartość mogłaby być znana tylko przez nadawcę i odbiorcę. Jak bezpiecznie przesłać list do adresata, tak aby pośrednik nie był w stanie jej odczytać? Jak wysłać do króla wiadomość, której nikt inny nie byłby w stanie odczytać? Jak przekazać polecenia dla szpiega, który znajduje się za linią frontu? Te i wiele innych pytań towarzyszy ludzkości praktycznie od powstania cywilizacji. Najczęstszym rozwiązaniem tych problemów będzie szyfrowanie wiadomości przez nadawcę i odszyfrowania jej za pomocą tajnego klucza przez odbiorcę. Dziedzinę nauki zajmującą się przekazywaniem informacji w sposób zabezpieczony przed niepowołanym dostępem nazywamy kryptologią. Dzieli się ona na kryprografię, czyli gałąź wiedzy o utajnianiu wiadomości oraz kryptoanalizę, czyli gałąź wiedzy o przełamywaniu zabezpieczeń oraz deszyfrowaniu wiadomości. Przekazywanie informacji z pomocą kryptografii ma jednak jedną, ale zasadniczą wadę: obecność tajnego komunikatu jest jawna, choć treść jest zaszyfrowana. Steganografia rozwiązuje ten problem. Jest to nauka o komunikacji w taki sposób, aby obecność komunikatu nie mogła zostać wykryta. Połączenie tych dwóch dziedzin nauki daje nam najwyższy możliwy poziom bezpieczeństwa w przekazywaniu tajnych wiadomości.

Warto też zauważyć jak bardzo na przestrzeni dziejów zmieniały się narzędzia komunikacji. Zaczynając od prostej mowy, pisma, przechodząc przez radio, telewizję, a kończąc na Internecie człowiek zyskał bardzo wiele możliwości przesyłania dowolnej wiadomości (np. w formie pliku graficznego, filmu) na dowolną odległość. Dzięki temu implementacja steganografii w dwudziestym pierwszym wieku jest teoretycznie ograniczona jedynie przez ludzką wyobraźnię.

Motywacją do podjęcia tematu była chęć stworzenia jak najbezpieczniejszego narzędzia do komunikacji w Internecie. Praktycznie każda większa korporacja, rządy państw nieustannie zbierają informację na temat każdego użytkownika przeglądającego witryny WWW. Dzięki forum steganograficznemu przeciętny człowiek, bez większych umiejętności informatycznych, będzie w stanie wymieniać wiadomości, nie obawiając się o szpiegowanie ze stron trzecich. Istnieje co prawda tzw. Darknet (pl. Ciemny Internet), czyli miejsce gdzie istnieje wolność absolutna, jednakże jest on trudny w obsłudze dla przeciętnego użytkownika.

## Cel i zakres pracy

Celem niniejszej pracy jest stworzenie w pełni funkcjonalnego forum internetowego wraz z zaimplementowanym mechanizmem do ukrywania tajnych wiadomości. Aplikacja powinna umożliwiać rejestrację i logowanie użytkowników, tworzenie, edycję, przeglądanie i usuwanie sekcji, tematów oraz postów. Posty powinny należeć do tematów, a tematy do sekcji. Należy umożliwić wgranie pliku graficznego i przypisanie go do danego postu.

## Struktura pracy

Dalsza część pracy zorganizowana jest w sposób następujący. Rozdział 2 zawiera ...

# Wprowadzenie

## Rys historyczny

## Idea steganografii

## Nośniki informacji umożliwiające zaimplementowanie steganografii

## Narzędzia komunikacji w Internecie

### Czat internetowy

### Forum internetowe

## Steganografia w plikach graficznych

# Przedstawienie użytych technologii

## NodeJS

## MeteorJS

## MongoDB

## AngularJS (wersja 1.x)

## Preprocessory

### CoffeeScript

### Jade

### Less

## Narzędzia do zarządzania projektem

### Git

### TravisCI

## Narzędzia do testowania

### GulpJS

### Jasmine

### Karma

### Protractor

# Budowa aplikacji

## Struktura plików i folderów

## Modele w bazie danych

## Jednostki w aplikacji

# System uwierzytelniania i autoryzacji

## Rejestrowanie i logowanie użytkowników

## Role

## Struktura ról

## Panel administracyjny

# System ukrywania wiadomości

## 

# Zakończenie

# Literatura

1. Autorzy: Tytuł, Informacje wydawnicze, data
2. Autorzy: Tytuł, Informacje wydawnicze, data