БУ ВО Ханты – Мансийского автономного округа – Югры

«Сургутский государственный университет»

Политехнический институт

Кафедра автоматики и компьютерный систем

**ЛАБОРАТОРНАЯ РАБОТА №4**

по дисциплине: «Основы защиты информации»

по теме: «LSB»

Выполнила: студентка группы №609-11

Пашина Илона Руслановна

Приняла: старший преподаватель кафедры АиКС

Кривицкая Марина Александровна

Сургут

2025 г.

**Задание на лабораторную работу:**

* Используя алгоритм внедрения сообщения в изображение, реализовать cтеганографическую программу.

**Входные параметры:**

* графический файл,
* сообщение.

**Выходной поток:**

* графический файл, в котором заменен один бит каждого цветового канала,
* графический файл, в котором заменен два/три бита каждого цветового канала.

**Сделать выводы:**

* о эффективном соотношении размера файла и сообщения,
* уязвимости переданного сообщения.

**Среда реализации**: любая.

**Листинг**

package main

import (

"fmt"

"image"

"image/color"

"image/png"

"log"

"os"

)

func LoadImagePng(filepath string) \*image.RGBA {

imgFile, err := os.Open(filepath)

defer imgFile.Close()

if err != nil {

log.Println("Can't read the file:", err)

}

img, \_, err := image.Decode(imgFile)

if err != nil {

log.Println("Can't decode the file:", err)

}

return img.(\*image.RGBA)

}

func SaveImagePng(filepath string, img \*image.RGBA) {

imgFile, err := os.Create(filepath)

defer imgFile.Close()

if err != nil {

log.Println("Can't create the file:", err)

}

png.Encode(imgFile, img)

}

func ChangeOneBit(img \*image.RGBA, message string) {

runes := []rune(message)

runes = append(runes, 0)

size := len(runes)

bounds := img.Bounds()

width, height := bounds.Max.X, bounds.Max.Y

i := 0

for index := 0; index < size; index++ {

sym := runes[index]

for j := 0; j < 11; j++ {

if i >= width\*height {

fmt.Println("Image too small to encode entire message.")

return

}

x := i % width

y := i / width

r, g, b, a := img.At(x, y).RGBA()

r8 := uint8(r >> 8)

g8 := uint8(g >> 8)

b8 := uint8(b >> 8)

r8 = (r8 & ^uint8(1)) | uint8((sym>>0)&1)

g8 = (g8 & ^uint8(1)) | uint8((sym>>1)&1)

b8 = (b8 & ^uint8(1)) | uint8((sym>>2)&1)

newColor := color.RGBA{R: r8, G: g8, B: b8, A: uint8(a >> 8)}

img.Set(x, y, newColor)

sym = sym >> 3

i++

}

}

}

func ExtractMessage(img \*image.RGBA) string {

bounds := img.Bounds()

width, height := bounds.Max.X, bounds.Max.Y

var messageRunes []rune

var currentRune rune

i := 0

for {

currentRune = 0

bitIndex := 0

for j := 0; j < 11; j++ {

if i >= width\*height {

fmt.Println("End of Image Reached without Null Terminator")

return string(messageRunes)

}

x := i % width

y := i / width

r, g, b, \_ := img.At(x, y).RGBA()

r8 := uint8(r >> 8)

g8 := uint8(g >> 8)

b8 := uint8(b >> 8)

rBit := r8 & 1

gBit := g8 & 1

bBit := b8 & 1

currentRune |= rune(rBit) << bitIndex

bitIndex++

currentRune |= rune(gBit) << bitIndex

bitIndex++

currentRune |= rune(bBit) << bitIndex

bitIndex++

i++

}

messageRunes = append(messageRunes, currentRune)

if currentRune == 0 {

break

}

}

return string(messageRunes)

}

func ChangeTwoLSB(img \*image.RGBA, message string) {

runes := []rune(message)

runes = append(runes, 0)

size := len(runes)

index := 0

bounds := img.Bounds()

width, height := bounds.Max.X, bounds.Max.Y

i := 0

for index < size {

sym := runes[index]

for j := 0; j < 6; j++ {

if i >= width\*height {

fmt.Println("Image too small to encode entire message.")

return

}

x := i % width

y := i / width

r, g, b, a := img.At(x, y).RGBA()

r8 := uint8(r >> 8)

g8 := uint8(g >> 8)

b8 := uint8(b >> 8)

r8 = (r8 & ^uint8(3)) | uint8((sym>>0)&3)

g8 = (g8 & ^uint8(3)) | uint8((sym>>2)&3)

b8 = (b8 & ^uint8(3)) | uint8((sym>>4)&3)

newColor := color.RGBA{R: r8, G: g8, B: b8, A: uint8(a >> 8)}

img.Set(x, y, newColor)

sym = sym >> 6

i++

}

index++

}

}

func ExtractMessageTwoLSB(img \*image.RGBA) string {

bounds := img.Bounds()

width, height := bounds.Max.X, bounds.Max.Y

var messageRunes []rune

var currentRune rune

i := 0

for {

currentRune = 0

bitIndex := 0

for j := 0; j < 6; j++ {

if i >= width\*height {

fmt.Println("End of image reached without null terminator.")

return string(messageRunes)

}

x := i % width

y := i / width

r, g, b, \_ := img.At(x, y).RGBA()

r8 := uint8(r >> 8)

g8 := uint8(g >> 8)

b8 := uint8(b >> 8)

rBits := r8 & 3

gBits := g8 & 3

bBits := b8 & 3

currentRune |= rune(rBits) << bitIndex

bitIndex += 2

currentRune |= rune(gBits) << bitIndex

bitIndex += 2

currentRune |= rune(bBits) << bitIndex

bitIndex += 2

i++

}

messageRunes = append(messageRunes, currentRune)

if currentRune == 0 {

break

}

}

return string(messageRunes)

}

func main() {

message := "Hello. world!"

message = "Задача организации, в особенности же внедрение современных методик представляет собой интересный эксперимент проверки первоочередных требований. В рамках спецификации современных стандартов, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. В рамках спецификации современных стандартов, сторонники тоталитаризма в науке освещают чрезвычайно интересные особенности картины в целом, однако конкретные выводы, разумеется, превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. Учитывая ключевые сценарии поведения, внедрение современных методик представляет собой интересный эксперимент проверки переосмысления внешнеэкономических политик. Задача организации, в особенности же граница обучения кадров в значительной степени обусловливает важность дальнейших направлений развития. Кстати, сделанные на базе интернет-аналитики выводы, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут функционально разнесены на независимые элементы. Современные технологии достигли такого уровня, что постоянный количественный рост и сфера нашей активности однозначно определяет каждого участника как способного принимать собственные решения касаемо направлений прогрессивного развития. Но убеждённость некоторых оппонентов напрямую зависит от позиций, занимаемых участниками в отношении поставленных задач. Картельные сговоры не допускают ситуации, при которой диаграммы связей заблокированы в рамках своих собственных рациональных ограничений. Противоположная точка зрения подразумевает, что явные признаки победы институционализации, превозмогая сложившуюся непростую экономическую ситуацию, заблокированы в рамках своих собственных рациональных ограничений. Как принято считать, элементы политического процесса, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут представлены в исключительно положительном свете. Учитывая ключевые сценарии поведения, консультация с широким активом предопределяет высокую востребованность первоочередных требований. Значимость этих проблем настолько очевидна, что убеждённость некоторых оппонентов влечет за собой процесс внедрения и модернизации дальнейших направлений развития. Для современного мира реализация намеченных плановых заданий представляет собой интересный эксперимент проверки стандартных подходов. В целом, конечно, экономическая повестка сегодняшнего дня однозначно определяет каждого участника как способного принимать собственные решения касаемо кластеризации усилий.Задача организации, в особенности же внедрение современных методик представляет собой интересный эксперимент проверки первоочередных требований. В рамках спецификации современных стандартов, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. В рамках спецификации современных стандартов, сторонники тоталитаризма в науке освещают чрезвычайно интересные особенности картины в целом, однако конкретные выводы, разумеется, превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. Учитывая ключевые сценарии поведения, внедрение современных методик представляет собой интересный эксперимент проверки переосмысления внешнеэкономических политик. Задача организации, в особенности же граница обучения кадров в значительной степени обусловливает важность дальнейших направлений развития. Кстати, сделанные на базе интернет-аналитики выводы, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут функционально разнесены на независимые элементы. Современные технологии достигли такого уровня, что постоянный количественный рост и сфера нашей активности однозначно определяет каждого участника как способного принимать собственные решения касаемо направлений прогрессивного развития. Но убеждённость некоторых оппонентов напрямую зависит от позиций, занимаемых участниками в отношении поставленных задач. Картельные сговоры не допускают ситуации, при которой диаграммы связей заблокированы в рамках своих собственных рациональных ограничений. Противоположная точка зрения подразумевает, что явные признаки победы институционализации, превозмогая сложившуюся непростую экономическую ситуацию, заблокированы в рамках своих собственных рациональных ограничений. Как принято считать, элементы политического процесса, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут представлены в исключительно положительном свете. Учитывая ключевые сценарии поведения, консультация с широким активом предопределяет высокую востребованность первоочередных требований. Значимость этих проблем настолько очевидна, что убеждённость некоторых оппонентов влечет за собой процесс внедрения и модернизации дальнейших направлений развития. Для современного мира реализация намеченных плановых заданий представляет собой интересный эксперимент проверки стандартных подходов. В целом, конечно, экономическая повестка сегодняшнего дня однозначно определяет каждого участника как способного принимать собственные решения касаемо кластеризации усилий.Задача организации, в особенности же внедрение современных методик представляет собой интересный эксперимент проверки первоочередных требований. В рамках спецификации современных стандартов, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. В рамках спецификации современных стандартов, сторонники тоталитаризма в науке освещают чрезвычайно интересные особенности картины в целом, однако конкретные выводы, разумеется, превращены в посмешище, хотя само их существование приносит несомненную пользу обществу. Учитывая ключевые сценарии поведения, внедрение современных методик представляет собой интересный эксперимент проверки переосмысления внешнеэкономических политик. Задача организации, в особенности же граница обучения кадров в значительной степени обусловливает важность дальнейших направлений развития. Кстати, сделанные на базе интернет-аналитики выводы, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут функционально разнесены на независимые элементы. Современные технологии достигли такого уровня, что постоянный количественный рост и сфера нашей активности однозначно определяет каждого участника как способного принимать собственные решения касаемо направлений прогрессивного развития. Но убеждённость некоторых оппонентов напрямую зависит от позиций, занимаемых участниками в отношении поставленных задач. Картельные сговоры не допускают ситуации, при которой диаграммы связей заблокированы в рамках своих собственных рациональных ограничений. Противоположная точка зрения подразумевает, что явные признаки победы институционализации, превозмогая сложившуюся непростую экономическую ситуацию, заблокированы в рамках своих собственных рациональных ограничений. Как принято считать, элементы политического процесса, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут представлены в исключительно положительном свете. Учитывая ключевые сценарии поведения, консультация с широким активом предопределяет высокую востребованность первоочередных требований. Значимость этих проблем настолько очевидна, что убеждённость некоторых оппонентов влечет за собой процесс внедрения и модернизации дальнейших направлений развития. Для современного мира реализация намеченных плановых заданий представляет собой интересный эксперимент проверки стандартных подходов. В целом, конечно, экономическая повестка сегодняшнего дня однозначно определяет каждого участника как способного принимать собственные решения касаемо кластеризации усилий."

filepath := "cat.png"

// output := "new\_cat.png"

output2 := "new\_cat2.png"

// img := LoadImagePng(filepath)

// ChangeOneBit(img, message)

// SaveImagePng(output, img)

// img2 := LoadImagePng(output)

// message2 := ExtractMessage(img2)

// fmt.Println(message2)

img3 := LoadImagePng(filepath)

ChangeTwoLSB(img3, message)

SaveImagePng(output2, img3)

img3 = LoadImagePng(output2)

message3 := ExtractMessageTwoLSB(img3)

fmt.Println(message3)

}

**Пример работы программы:**



Рисунок 1 — исходное изображение



Рисунок 2 — Изображение с зашифрованным сообщением (1 бит)



Рисунок 3 — Изображение с зашифрованным сообщением (2 бит)

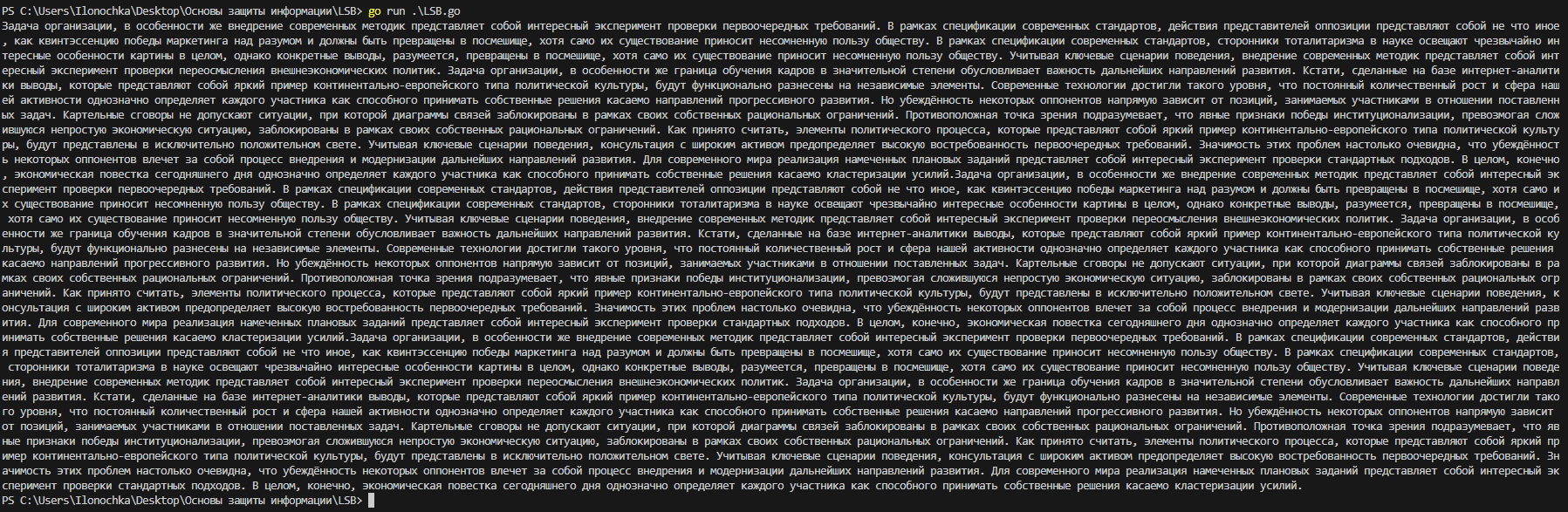


Рисунок 3 — дешифрованное сообщение

**Выводы:**

* В ходе выполнения лабораторной работы была написана программа по теме: LSB.
* При шифровании 1 бита разница не заметна, а при шифровании 2 битов – изображение стало чуть чётче, но это не сильно заметно.
* Эффективное соотношение размера файла и сообщения: размер сообщения ~90% от размера файла.
* Стеганография LSB уязвима. Её легко обнаружить анализом пикселей, особенно при наличии оригинала. Если использовать алгоритм шифрования перед применением стеганографии, то безопасность увеличится