

**Steganography Encrypt & Decrypt password to / from an image.**

# מיני פרויקט אבטחת מערכות תוכנה



נופת מלכה 313530891

מרצה: איציק בייז

**ניתנה הארכה גורפת להגשה עד 12.08.2020 ראה בפורום שכתב המרצה בייז.**

תוכן

[מיני פרויקט אבטחת מערכות תוכנה 0](#_Toc48161105)

[מבוא 2](#_Toc48161106)

[תיאור האלגוריתם 4](#_Toc48161107)

[**אלגוריתם לבדיקת חוזק הסיסמא** 4](#_Toc48161108)

[**הצפנת הסיסמא ע"י הצפנת Exclusive-OR** 5](#_Toc48161109)

[**סריקה איך תמונות נשמרות** 5](#_Toc48161110)

[**הסתרת הסיסמא בתוך תמונה בשיטת LSB** 5](#_Toc48161111)

[מערכת-הצפנה ופענוח סיסמא ל/מ-תמונה 7](#_Toc48161112)

[**PasswordStrength** 8](#_Toc48161113)

[**Conversion** 9](#_Toc48161114)

[**ImaSteganogrAphyP** 10](#_Toc48161115)

[**Crypto –** 11](#_Toc48161116)

[שלבי הרצת התוכנית 12](#_Toc48161117)

[מקורות מידע 22](#_Toc48161118)

מבוא

**סטגנוגרפיה** היא אמנות הסתרת מידע

שלא כמו הצפנה, שם ברור שמוסתר הודעה, הסטגנוגרפיה מסתירה נתונים בתצוגה רגילה, בתוך קובץ כמו תמונה. מבחינת תמונות, לכל מי שאינו מודע לכך שהוא מכיל נתונים נסתרים, זה נראה כמו תמונה רגילה ותמימה.

סטגנוגרפיה שימושית במצבים בהם שליחת הודעות מוצפנות עשויה לעורר חשד, למשל במדינות בהן דיכוי חופש הדיבור. זה משמש לעתים קרובות גם כסימן מים דיגיטלי כדי למצוא מתי נגנבים תמונות או קבצי שמע. ובנימה פחות פרקטית - זה פשוט מגניב.

ישנן כמה טכניקות שונות להסתרת נתונים בתוך קבצים רגילים. אחד השימושיים הנפוצים ביותר ואולי הפשוטים ביותר להבנה הוא טכניקת הסיביות הפחות משמעותית, הידועה בכינויה LSB.

טכניקה זו משנה את הסיביות האחרונות בבת אחת לקידוד הודעה, שהיא שימושית במיוחד במשהו כמו תמונה, כאשר הערכים האדומים, הירוקים והכחולים של כל פיקסל מיוצגים על ידי שמונה ביטים (בייט) שנעים בין 0 ל- 0 255 בעשרוני או 00000000 עד 11111111 בינארית.

שינוי שני הסיביות האחרונות בפיקסלים אדומים לחלוטין מ- 11111111 ל- 11111101 רק משנה את הערך האדום מ- 255 ל- 253, שלמעשה עין בלתי מזוינת נוצר שינוי כמעט בלתי מורגש בצבע אך עדיין מאפשר לנו לקודד נתונים בתוך התמונה.

תמונה שמכילה צילום מסך

התיאור נוצר באופן אוטומטי

דיאגרמה זו מציגה שתי תמונות בעלות 4 פיקסלים בערכים צבעוניים ובינאריים כאחד. כל גוש בינארי מייצג את הערך של הפיקסל המתאים.

הנוסחא לתהליך הצפנת מידע בתוך קובץ, אצלינו הצפנת סיסמא בתוך תמונה, מורכב מ-

cover\_medium + hidden\_data + stego\_key = stego\_medium

cover\_meduim – הקובץ שבתוכו אנחנו מסתירים מידע

hidden\_data – המידע שאנחנו רוצים להסתיר

stego\_key – המפתח שאיתו אנחנו יכולים (אבל לא חייבים) להצפין את המידע

Stego\_meduim – הקובץ הסופי שהוא מאותו סוג של קובץ המקור

**בפרויקט נצפין ונפענח סיסמא ל/מ- תמונה:**

נבקש מהמשתמש להכניס סיסמא חזקה נבדוק תקינות קלט תוך שימוש באלגוריתם לבדיקת חוזק הסיסמא .לאחר מכן נצפין את הסיסמא ע"י שימוש בהצפנת Exclusive-OR את הסיסמא המוצפנת נכניס להצפנה ע"י סטגנוגרפיה של תמונה בטכניקת LSB שתוארה לעיל תוך יצירת תמונה חדשה שהוצפן בה הסיסמא, וכן נפענח את הסיסמא שהוצפנה בתמונה ע"י קלט תמונה שהוצפנה.

התרגיל ימומש בשפת C++, בסביבת Microsoft Visual Studio עם שימוש בספריית OpenCV.

[להתקנות והורדות סביבת עבודה וספרייה ראה קובץ READEME]

[לבדיקת חוזק הסיסמא עשיתי פונקציות משלי ונעזרתי באתר " <http://www.passwordmeter.com/> " ].

תיאור האלגוריתם

## **אלגוריתם לבדיקת חוזק הסיסמא**

לצורך קביעת חוזק הסיסמא ( אופציונאלי עבור הסתרת המידע ), נשמור משתנה "ציון" שיחשב בכל שינוי של הסיסמא את הציון.

קריטריונים להעלאת הציון:

* ציון += (אורך הסיסמא \* 4)
* ציון += ((מספר האותיות הגדולות -אורך הסיסמא) \* 2)
* ציון += ((מספר האותיות הקטנות -אורך הסיסמא) \* 2)
* ציון += (מספר הספרות \* 4)
* ציון += (מספר הסמלים \* 6)
* ציון += ((מספר הסמלים+ ספרות באמצע הסיסמא) \* 2)

דרישות:

הוספת 2 נקודות עבור כל דרישה המתקיימת:

* אורך הסיסמא חייב להיות לפחות 8 תווים (עד 12 תווים).
* הסיסמא יכולה לכלול אותיות גדולות (A – Z)
* הסיסמא יכולה לכלול אותיות קטנות (a – z)
* הסיסמא יכולה לכלול ספרות (0 – 9)
* הסיסמא יכולה לכלול סמלים (כגון !, @ ...)

קריטריונים להורדת ציון הסיסמא:

* אם הסיסמא מורכבת מאותיות בלבד אזי ציון -= (אורך הסיסמא)
* אם הסיסמא מורכבת מספרות בלבד אזי ציון -= (אורך הסיסמא)
* אם קיים כמות של אותיות גדולות אז ציון -=( הכמות \*2)
* אם קיים כמות של אותיות קטנות אז ציון -=( הכמות \*2)
* אם קיים כמות של מספרים אז ציון -=( הכמות \*2)
* אם קיים רצף של אותיות בסדר עולה או יורד אז ציון -=(מספר המופעים של רצף כלשהו \*3)
* אם קיים רצף של מספרים בסדר עולה או יורד אז ציון -=(מספר המופעים של רצף כלשהו \*3)

בכל מקרה, נשמור על טווח הערכים של הציון להיות עד ציון -100. אך לא ניתן למשתמש להכניס סיסמא פחות מציון 70.

weak: 70-80

moderate: 80-90

Strong: 90-100

## **הצפנת הסיסמא ע"י הצפנת** **Exclusive-OR**

הצפנת XOR (או הצפנת Exclusive-OR) היא שיטה נפוצה להצפנת טקסט לתבנית שלא יכול להיות שבירה לא טריוויאלית על ידי האדם הממוצע. הצפנת XOR נהדרת לאחסון דברים כמו שמירת נתונים כגון סיסמא של משתמש שהוא לא רוצה לשכוח, וסוגי נתונים אחרים המאוחסנים באופן מקומי במחשב משתמשים, שלמרות שלא מדובר בעסקה גדולה אם אתם לא מתמודדים איתם, אתם רוצים להרתיע אנשים מלעשות זאת. הצפנת XOR משמשת לעיתים קרובות כחלק מאלגוריתמים להצפנה מורכבים יותר.

הרעיון שעומד מאחוריו הוא שאם אינכם מכירים את הדמות המקורית או את מפתח ההצפנה של XOR, אי אפשר לקבוע מה זה. עם זאת, הסיבה שזה לא לגמרי מאובטח היא שהנתונים כמעט תמיד מכילים דפוסים (JSON משתמש בתווים '{' ו- '}', XML מכיל הרבה תווים '<' ו- '>' וכו ') כך שאם מישהו מסוגל כדי לקבוע את הדפוס ולפתוח אפילו תו אחד, יהיה להם המפתח לביטול הנעילה של כל השאר.

עם זאת ככל שיהיה הצפנת XOR מאובטחת או לא בטוחה, יש בו הרבה מקרי שימוש תקפים. כל הרתעה שמתווספת לנתונים שאינך רוצה שמשתמשים יתעסקו בהם אך תהיה להם גישה נוחה היא מועמדת ראשונה, כל עוד האבטחה איננה חשובה.

הרעיון הגדרת תו מפתח, ועל כל תו במחרוזת שאתה רוצה להצפין אתה מיישם את המפתח. ברגע שאתה רוצה לבטל את ההצפנה של הנתונים המוצפנים, אתה פשוט עובר על המחרוזת ומפעיל שוב את המפתח.

בתוכנית שלנו: המפתח להלן:

char key[5] = { 'N', '@', 'F','e','400'};

## **סריקה איך תמונות נשמרות**

תמונות בדרך כלל משתמשות ב8-bit / 24-bit color. כאשר משתמשים ב8bit color אפשר להגיע לייצוג של עד 256 צבעים לתמונה . ב24-bit color משתמשים ב24bit כל פיקסל כאשר כל פיקסל מיוצג ע"י שלושה צבעים אדום (red), ירוק(green) וכחול (blue) (RGB).

לכן, הגודל של התמונה הינו בעל קשר ישיר למספר הפיקסלים והגדרת הצבע שבה התמונה משתמשת. למשל תמונה בגודל של 640X480 אשר משתמשת ב256 צבעים תיהיה בגודל של 307K (640\*480 bytes) בעוד שתמונה בגודל של 1024X768 אשר מוגדרת להיות 24bit color תיהיה בגודל של 2.36 MB (1024\*768\*3 bytes).

בשביל לא להגיע לקבצי תמונות בגודל עצום פותחו שיטות כיווץ שונות כגוןBitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG). לא כולן מתאימות לביצוע steganography אולם GIF ו8-bit BMP יותר מתאימות.

## **הסתרת הסיסמא בתוך תמונה בשיטת LSB**

הדרך הכי נפוצה להסתיר את המידע נקראת "הטמעת LSB " (least significant bit insertion). בדרך זו אנחנו לוקחים את הLSB של כל byte בcoever\_image (התמונה שמשמשת להסתר המידע) ודורסים אותו עם הhidden\_data שלנו. אם נשתמש בתמונות של 24-bit color אז כמות השינויים לא תיהיה נראית לעין האנושית.

[ראה דוגמא שהובאה במבוא על 2 סיביות]

שיטה סטגנוגרפית זו היא, בניגוד לשיטות אחרות, מחביאה את המסר הסמוי ב-data של הקובץ ולא ב-data-meta עיקר שיטה זו הוא להחביא חלקים קטנים מהמסר בכל אחד ממרכיבי התמונה(פיקסלים) באופן כזה שלא נראה לעין. כך, בעת קריאת התמונה ניתן לחלץ מאותם פיקסלים את המידע ולחברו יחדיו לכדי מסר שלם. את השיטה ניתן לממש כך שבתוך כל byte של data מחביאים כל כמות של סיביות (עד 8 כמובן), כאשר שככל שמחביאים פחות – הערוץ אינו נראה לעין, וככל שמחביאים יותר כך נפח הערוץ הסמוי גדל. במימוש שלי בחרתי להחביא סיבית אחת בכל byte של data . יש לשים לב שלכאורה השינויים שנעשים לקובץ בשיטה זו יהיו נראים לעיניי המתבונן, אך כאשר מדובר בסיבית אחת של שינוי בכל byte של data מקורי השינוי הוא זעיר מאוד ואינו נראה לעין כלל.

ייצוג פיקסל בתמונת Bitmap יכול להיעשות באופנים שונים, וכך ניתן לייצג פיקסל בדיוקים שונים. נניח ואנו מייצגים פיקסל על ידי 32 סיביות, איך נדע אילו מהסיביות שייכות לאיזה ערוץ צבע? לצורך כך, נמצא שדה ה- BitField אשר מכיל mask שאומר כיצד יש לקרוא כל פיקסל, כלומר איזה ביטים שייכים לאיזה ערוץ צבע.

בשיטה סטגנוגפית זו, נמצא שלב נוסף באלגוריתם והוא קידוד המידע. המידע כאמור מגיע אלינו כרצף בתים, ואנו רוצים לפצלו, כך שלכל byte של data נקודד בדיוק סיבית אחת.

בפרויקט שלנו הסיסמא(בביטים) + גודל הסיסמא(בביטים) יוצפנו לתמונה בשיטת LSB בקידוד של סיבית אחת. את הסיסמא נפענח מתמונה כך שנפרק את גודל הסיסמא מהסיסמא עצמה ולאחר מכן נשלח את הסיסמא לפיענוח.

בתוכנית שלנו נשתמש בטעינת תמונה – בתמיכה בפורמט BMP .

מערכת-הצפנה ופענוח סיסמא ל/מ-תמונה

**מימוש – steganography system**

הפרויקט ימומש בשפת C++, בסביבה Microsoft Visual Studio 2019.

לפרויקט 3 מחלקות עיקריות :

* **PasswordStrength- מחלקה לבדיקת חוזק הסיסמא.**
* **-Conversion מחלקה להמרות השונות.**
* **ImaSteganogrAphyP- מחלקה שפועלת להצפנת הסיסמא המוצפנת לתוך תמונה, ופיענוח הסיסמא מתוך התמונה המוצפנת.**
* **Crypto- פונקציית הצפנה ופיענוח סיסמא.**

למערכת יש פונקציית ה main - קובץ ההרצה של התוכנית שיאפשר למשתמש:

* 1. בדיקת חוזק הסיסמא
     1. משתמש מכניס סיסמא (תוך בדיקת תקינות הסיסמא).
     2. למשתמש יש אפשרות לראות הסבר מפורט מהי סיסמא חזקה.
     3. למשתמש יש אפשרות לראות ציון הסיסמא ופירוט חישוב חיסור הנקודות.
     4. למשתמש יש אפשרות לשפר את הסיסמא במידה והציון לא מוצא חן בעיניו.
  2. הצפנת הסיסמא לתוך תמונה
     1. בקשה מהשתמש להכניס סיסמא (תוך בדיקת תקינות הסיסמא).
     2. להצפין את הסיסמא עם אלגוריתם ההצפנה.
     3. להציג למשתמש את הסיסמא לאחר הצפנה.
     4. בקשה משתמש לבחור את הקובץ שבו תוצפן הסיסמא המוצפנת.
     5. משתמש בוחר שם לתמונה החדשה שתוצפן בה הסיסמא.
     6. יצירת קובץ של התמונה החדשה אחר הצפנת הסיסמא המוצפנת בתוכה.
  3. פיענוח הסיסמא מתוך תמונה
     1. בקשה מהמשתמש להכניס את שם קובץ התמונה שבה הוצפנה כבר הסיסמא המוצפנת(כמובן שהתמונה הוצפנה לפי שיטת מערכת זו).
     2. פיענוח הסיסמא המוצפנת מתוך התמונה שהוצפנה בה הסיסמא.
     3. לפענח את הסיסמא מתוך הסיסמא המוצפנת.
     4. להציג למשתמש את הסיסמא המקורית.
     5. הצגה למשתמש התמונות של לפני ואחרי הצפנת התמונה.

## **PasswordStrength**

המחלקה תחשוף את הפונקציות הבאות:

פונקציות המחלקה:

בנאי-

PasswordStrength();

בנאי דריסה- בעת סגירת התוכנית מנקה מקום בזיכרון

~PasswordStrength();

פונקציה עבור חוזק הסיסמא – חישוב עפ"י הקריטריונים המוגדרים בסעיף "אלגוריתם לחישוב חוזק הסיסמא".

פונקציה שבודקת את חוזק הסיסמה על פי הקריטריונים:

קלט: סיסמא, תו שהמשתמש הכניס לביצוע הדפסות שונות.

פלט: תו מהמשתמש כדי להמשיך לשלבים השונים.

char printStrongPass(char\* input ,char chack)

הפונקציה מבצעת :

1. פעולות חישוב על הורדת ניקוד.
2. הדפסה במידה והמשתמש רוצה לדעת על מה ירדו לו נקודות.
3. חישוב ציון לפני הורדה
4. חישוב ציון לאחר הורדה
5. הדפסת סוג חוזק הסיסמא

פונקציה שנותנת למשתמש אפשרויות על הסיסמא

void passwordOption();

פונקציה שמבקשת סיסמא ותמונה לבחירה

void getPasswordAndPhoto();

פונקציה שמחלצת את הסיסמא ומציגה למשתמש אותה

void extractPassAndPrint();

## **Conversion**

מחלקה לביצוע סוגי המרות שונות.

פונקציות המחלקה:

בנאי-

conversion();

בנאי דריסה- בעת סגירת התוכנית מנקה מקום בזיכרון

~conversion();

-Geteer&Setter

רצף תווים להחזרה של הפונקציה

void ch(char\*);

void ch(int,char);

char\* ch()const;

המרה מבינארי לרצף תווים- קלט רצף תווים בינאריים

פלט- גודל הסיסמא.

עבור הוצאת גודל הסיסמא -צריך 8 ביטים הראשונים שנוציא בבתים הראשונים, שזה כפי הנ"ל עבור גודל הסיסמא .

int binaryToChar(char\*);

המרה מבינארי למחרוזת-קלט רצף תווים בינאריים

פלט- הסיסמא המוצפנת.

עבור פיענוח הסיסמא המוצפנת מתמונה מהביט ה8 ואילך- שאר הביטים של הסיסמא

char\* binaryToStr(char\*);

המרה ממחרוזת לבינארי-קלט רצף תווים: הסיסמא המוצפנת + גודל הסיסמא

פלט-רצף תווים בינאריים

עבור הצפנת גודל הסיסמא בהתחלה ואחר מכן הצפנת הסיסמא המוצפנת לתמונה(8 ביטים ראשונים שמכניסים עבור גודל הסיסמא)

char\* strToBinary(const char\*);

## **ImaSteganogrAphyP**

פונקציות המחלקה:

בנאי-

ImgSteganogrAphyP();

בנאי דריסה- בעת סגירת התוכנית מנקה מקום בזיכרון

~ImgSteganogrAphyP();

פונקציה מקבלת כקלט שלושה רצפים של תווים:

הסיסמא מתורגמת לביטים STRBIN, שם תמונה לפני הצפנה, שם תמונה לאחר הצפנה

הפונקציה מבצעת הצפנת סיסמא לתוך תמונה נבחרת חדשה.

void ImgStegAnographyP(char\*, char\*, char\*);

פונקציה מקבלת כקלט רצף של תווים: שם התמונה שהוצפן בה סיסמא מוצפנת

ומחזירה כפלט- רצף של תווים שהם הסיסמא המוצפנת שבתמונה.

char\* decipheringPss(char\*);

## **Crypto –**

פונקציה להצפנה ופיענוח סיסמא:

מקבלת כקלט סיסמא / סיסמא מוצפנת (בהתאמה להצפנה ופענוח).

פלט סיסמא מוצפנת / סיסמא (בהתאמה להצפנה ופענוח).

הגדרת תו מפתח, ועל כל תו במחרוזת שאתה רוצה להצפין אתה מיישם את המפתח. ברגע שאתה רוצה לבטל את ההצפנה של הנתונים המוצפנים, אתה פשוט עובר על המחרוזת ומפעיל שוב את המפתח.

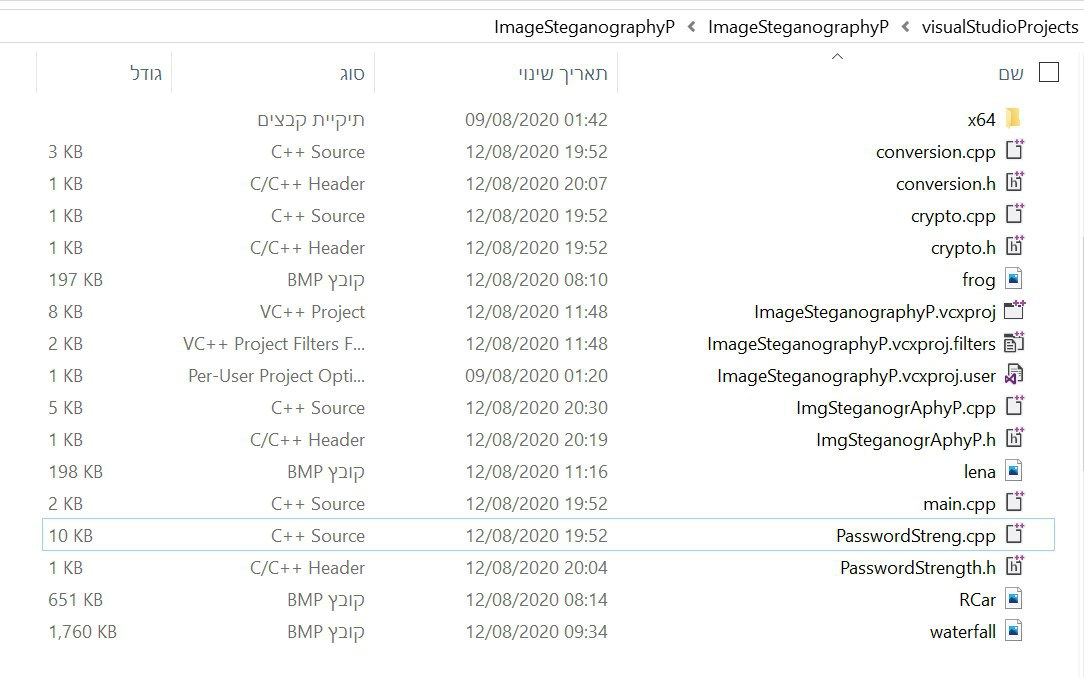
char\* encryptDecrypt(char\*);

בתוכנית שלנו: המפתח להלן:

char key[5] = { 'N', '@', 'F','e','400'};

שלבי הרצת התוכנית

הספרייה ללא התמונות המפוענחות:



הרצה 1:

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 1

Press '0' if you want an explanation of the password strength

Otherwise press any button to enter the password:

0

Password length must be at least 8 characters (up to 12 characters).

- The password can be uppercase(A - Z)

- The password can be lowercase(a - z)

- Password can contain digits(0 - 9)

- The password can contain symbols(such as!, @ ...)

A user cannot enter a password less than a score of 70.

weak: 70 - 80

moderate : 80 - 90

Strong : 90 - 100

Please enter your password

msh12457!

Press '0' if you want to know what the score was about and what the password strength score is

Otherwise press any button

0

The strength of your password Before the Subtraction of the score is 94

subtracting:-4 subtracting points- The amount of lowercase letters

subtracting:0 subtracting points- The amount of capital letters

subtracting:-8 subtracting points- The amount of digits

subtracting:0 subtracting points- sequence of digit in ascending or descending order

subtracting:0 subtracting points- sequence of letters in ascending or descending order

The strength of your password is: 82

the srtong of password: - Moderate

Do you want to improve the password strength score Press 0

otherwise click any button

0

Press '0' if you want an explanation of the password strength

Otherwise press any button to enter the password:

f

Please enter your password

Msh12457!

Press '0' if you want to know what the score was about and what the password strength score is

Otherwise press any button

f

The strength of your password is: 100

the srtong of password: - Strong

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 2

Do you want to use the images in the database prass '0' .

To insert a new image prass '1'

For default image Click any button :

0

To image of car Tap '0'

To image of Waterfall Tap '1'

To image of frog Tap '2'

0

Encrypted: 3.TzuqD

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 3

after the seganographly

Msh12457!

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

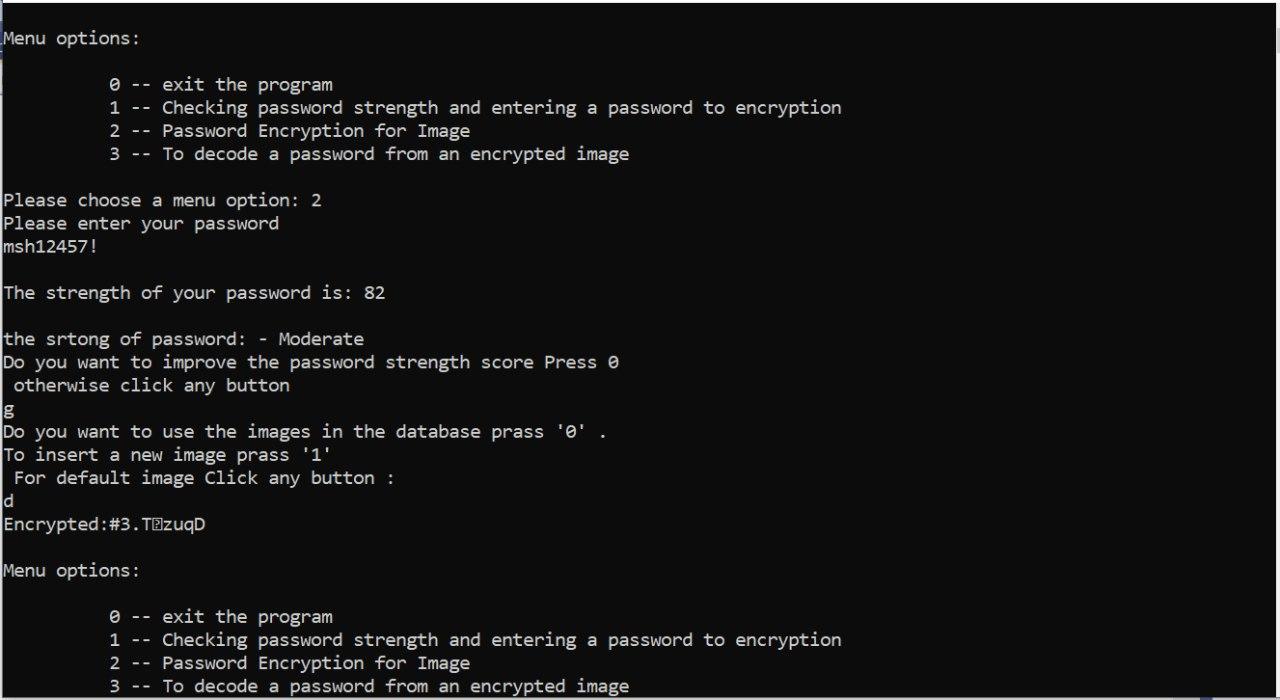
Please choose a menu option: 0

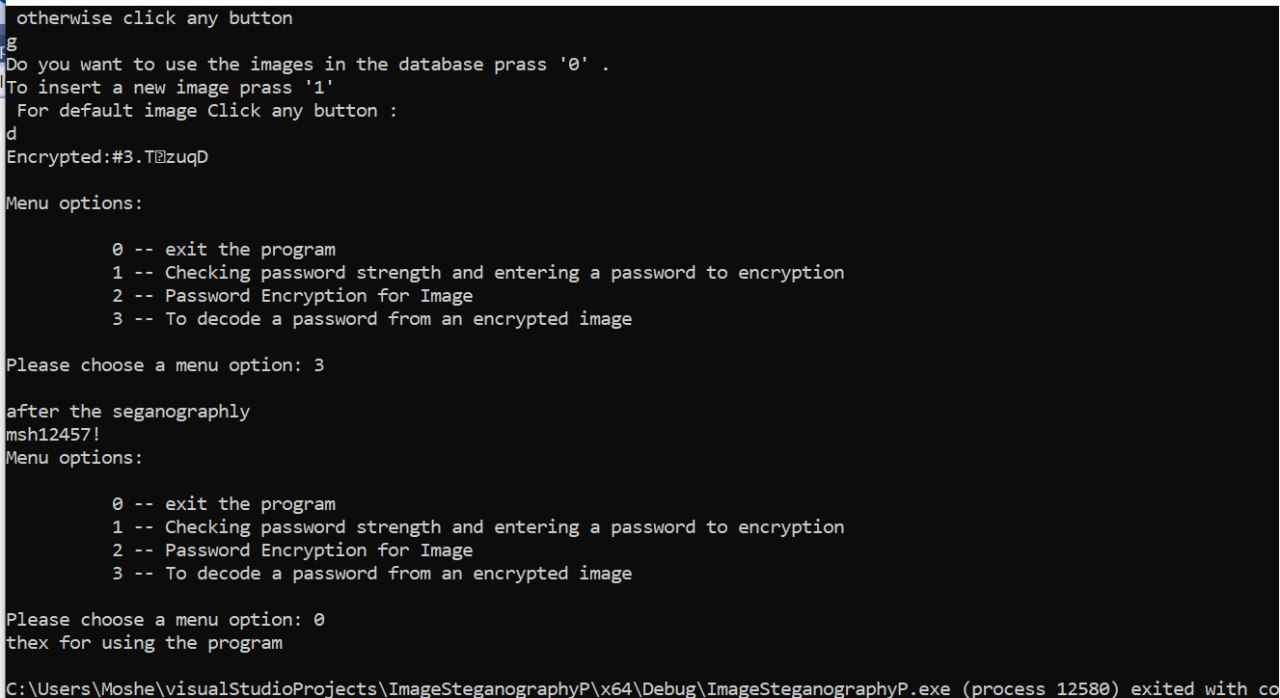
thex for using the program

C:\Users\Moshe\visualStudioProjects\ImageSteganographyP\x64\Debug\ImageSteganographyP.exe (process 18600) exited with code 3.

To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.

Press any key to close this window . . .





הרצה 2:

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 2

Please enter your password

msh1245

Your password is shorter than 8 characters.

Please enter a password between 8 and 12 characters

msh12457

The strength of your password is: 66

the srtong of password: - Your password is too weak. Please enter a new password

Please enter your password

msH12457!

The strength of your password is: 100

the srtong of password: - Strong

Do you want to use the images in the database prass '0' .

To insert a new image prass '1'

For default image Click any button :

0

To image of car Tap '0'

To image of Waterfall Tap '1'

To image of frog Tap '2'

0

Encrypted:#3

TzuqD

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 3

after the seganographly

msH12457!

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

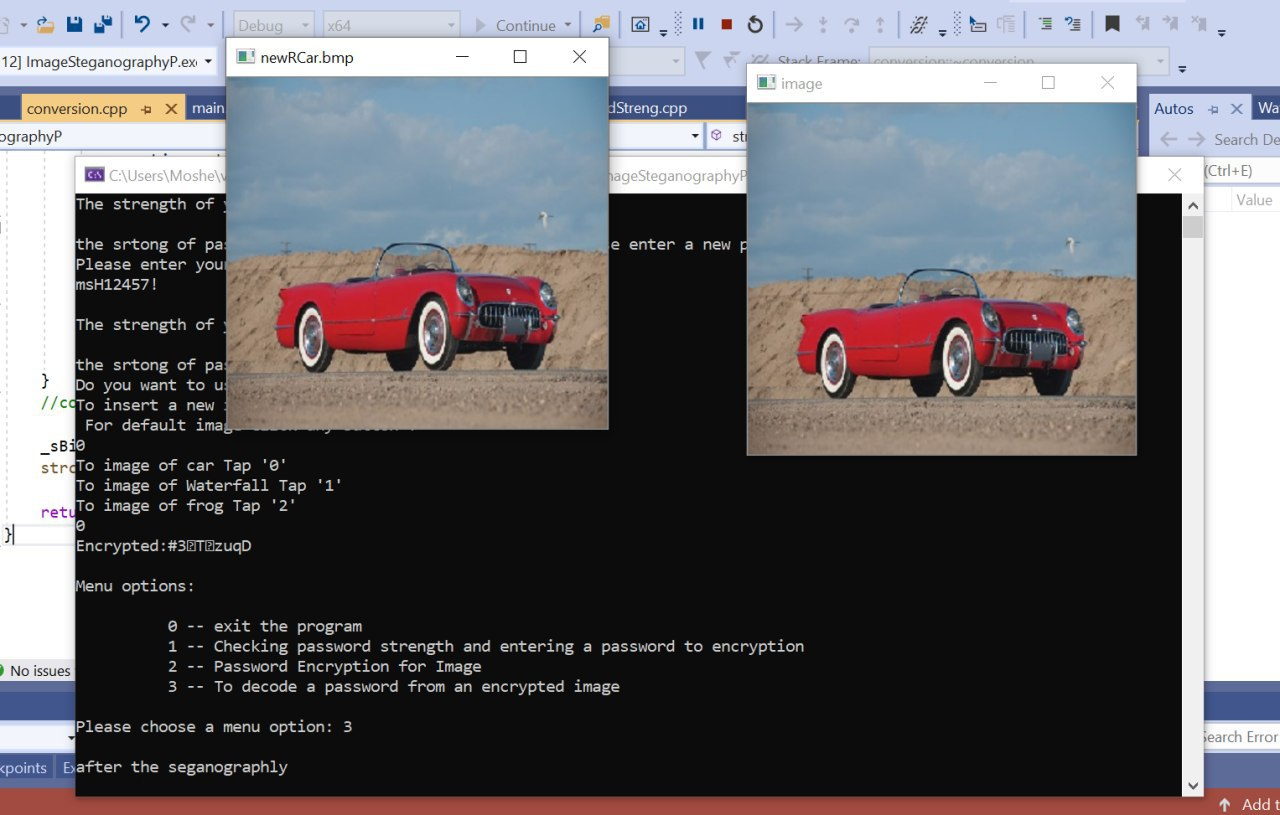
Please choose a menu option: 0

thex for using the program

C:\Users\Moshe\visualStudioProjects\ImageSteganographyP\x64\Debug\ImageSteganographyP.exe (process 15312) exited with code 3.

To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.

Press any key to close this window . . .



הרצה 3:

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 2

Please enter your password

mshH12457!

The strength of your password is: 100

the srtong of password: - Strong

Do you want to use the images in the database prass '0' .

To insert a new image prass '1'

For default image Click any button :

0

To image of car Tap '0'

To image of Waterfall Tap '1'

To image of frog Tap '2'

2

Encrypted:#3.-|tsR

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 3

after the seganographly

mshH12457!

Menu options:

0 -- exit the program

1 -- Checking password strength and entering a password to encryption

2 -- Password Encryption for Image

3 -- To decode a password from an encrypted image

Please choose a menu option: 0

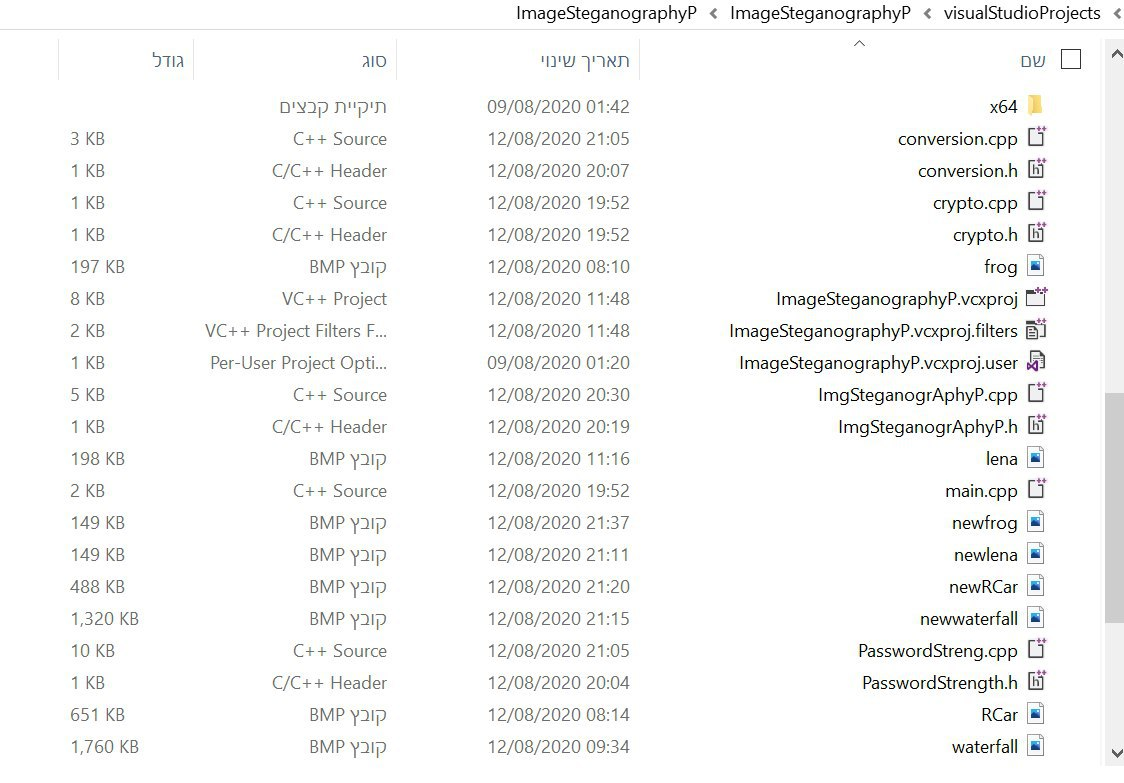
thex for using the program

C:\Users\Moshe\visualStudioProjects\ImageSteganographyP\x64\Debug\ImageSteganographyP.exe (process 23240) exited with code 3.

To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.

Press any key to close this window . . .

הספרייה עם התמונות המפוענחות:



ראה את 3 התמונות המפוענחות לאחר ההרצה

מקורות מידע

לבדיקת חוזק סיסמא:

<http://www.passwordmeter.com/>

לשימוש בספרייה OpenCV:

<https://docs.opencv.org/2.4/doc/user_guide/ug_mat.html>

https://www.youtube.com/watch?v=M-VHaLHC4XI&list=PLvv4vffx7TzxHq7bdoZ2gAQOyBaiNl6e6&index=31&t=0s

הסבר על הצפנה ופענוח סיסמא מ/ל- תמונה:

<https://www.garykessler.net/library/steganography.html>

<https://www.researchgate.net/publication/51963913_Steganography_Algorithm_to_Hide_Secret_Message_inside_an_Image>

להצפנה ופיענוח סיסמא:

<https://en.wikipedia.org/wiki/XOR_cipher>