

פתיחה:

סטגנוגרפיה (Steganography) היא האומנות של הסתרת מסרים, תמונות או קבצים בתוך הודעה, תמונה או קובץ אחרים. הקובץ החדש הנושא את האובייקט המוטבע נקרא אובייקט הסטגו (stego-object). האובייקט המוטבע הוא המסר שיוסתר באמצעות מפתח סטגו (stego-key) או אלגוריתם. אובייקט הכיסוי (cover object) הוא קובץ הנתונים שיכיל את ההודעה הסודית.

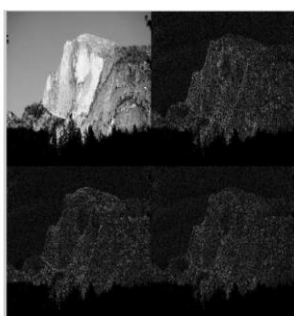
השיטה הפשוטה ביותר לזהות קבצים ששוננו היא להשוות אותם לקבצים המקוריים. לדוגמא, כדי לזהות מידע העובר דרך גרפיקה באתר אינטרנט ניתן לשמור עותקים מקוריים של תוכן האתר, ולאחר מכן להשוות את זה עם התוכן הנוכחי שבאתר. בהנחה שאין שגיאות, ההבדלים יכילו את התוכן המוסתר.

מטרת הסטגנוגרפיה המודרנית היא להיות בלתי ניתנת לזיהוי. לכן, בסטגנוגרפיה המודרנית הדיגיטלית המידע מוצפן ולאחר מכן מוטבע ומוחבא בקובץ הכיסוי באמצעות אלגוריתמים מיוחדים שעשויים לשנות או להוסיף תוכן לקובץ.

בתקשורת סמויה דרך האינטרנט, תמונות דיגיטליות הן אולי הסוג המעשי ביותר של סטגנוגרפיה, בעיקר בשל כמותם הגדולה ברשת האינטרנט. לעומת זאת, בעיה נפוצה בשימוש בתמונות דיגיטליות היא קיבולת לא מספיקה להחבאת התוכן המוסתר.

במטלה זו אשתמש בטכניקת סטגנוגרפיה באמצעות התמרת Wavelet בדידה על תמונות. כך שנעשה שימוש בתמונת כיסוי (cover image) ותמונה סודית (secret image) שאותה נסתיר. התוצאה נקראת התמונה המוטמעת (Embedded image).

נעשה שימוש בהתמרת Wavelet דו-מימדית בדידה מסדר ראשון (2D Single-level discrete wavelet transform). באמצעות הפירוק נקבל מקדם קירוב ושלושה מקדמי מאפיינים. נוכל לראות דוגמא לכך בתרשים הבא:



אלגוריתם הסטגנוגרפיה:

כעת נראה את שלבי האלגוריתם שנעשה בו שימוש במטלה זו:

א. תהליך הטמעת התמונה הסודית באמצעות התמרת Wavelet:

1. ייבוא של תמונת הכיסוי ותמונה סודית באמצעות בחירה מתיקיות המחשב.
2. התאמה של גודל התמונות על ידי ריפוד באפסים (כי בהמשך נבצע פעולות מתמטיות ביניהם).
3. פיצול תמונת הכיסוי והתמונה הסודית לצבעי RGB נפרדים (R- אדום, G- ירוק, B- כחול).
4. ביצוע התמרת Wavelet דו- מימדית בדידה מסדר ראשון על כל אחד מערוצי התמונות בנפרד באמצעות פונקציית Wavelet מסוג Daubechies. ונקבל מקדם קירוב (cA), מקדם אופקי (cH), מקדם אנכי (cV) ומקדם אלכסוני (cD).
5. נניח ערך מסוים למקדם הטמעה שנקרא לו a בטווח של 0 עד 1. ככל שערכו גבוה יותר כך יגדל חוזק התמונה הסודית וככל שערכו קטן יותר כך תגבר שקיפות התמונה הסודית.
6. כדי למצוא את המקדמים של התמונה המוטמעת נשתמש בנוסחאות הבאות:
$$cA_{embedded} = (1 - a) \cdot cA_{cover} + a \cdot cA_{secret}$$
 עבור מקדם קירוב:
$$cH_{embedded} = (1 - a) \cdot cH_{cover} + a \cdot cH_{secret}$$
 עבור מקדם אופקי:
$$cV_{embedded} = (1 - a) \cdot cV_{cover} + a \cdot cV_{secret}$$
 עבור מקדם אנכי:
$$cD_{embedded} = (1 - a) \cdot cD_{cover} + a \cdot cD_{secret}$$
 עבור מקדם אלכסוני:
צריך לחשב כל אחד מהמקדמים לכל ערוץ צבע.
7. ביצוע התמרת Wavelet דו- מימדית בדידה הפוכה מסדר ראשון בעזרת מקדמי התמונה המוטמעת שחישבנו כדי לקבל את ערוצי הצבע (RGB) של התמונה המוטמעת.
8. המרת המקדמים שקיבלנו מ-double ל- 8-bit integer כך שנוכל להציג את התמונה. (נשמור על המקדמים המקוריים גם לשחזור מדויק יותר).
9. נחבר את שלושת ערוצי הצבע של התמונה המוטמעת לכדי תמונה אחת (נעשה זאת גם לערוצים מסוג double), ונקבל את התמונה המוטמעת.
10. נציג על המסך את התמונות ונשמור את התמונה המוטמעת בזיכרון.

ב. תהליך חילוץ התמונה הסודית באמצעות התמרת Wavelet:

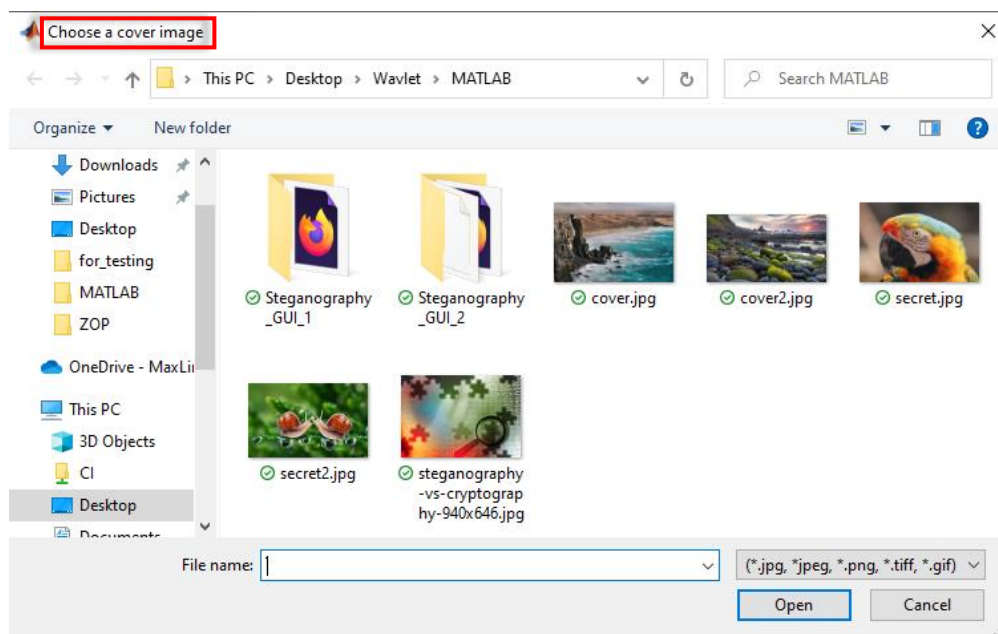
1. ייבוא של תמונת הכיסוי והתמונה המוטמעת.
2. פיצול תמונת הכיסוי והתמונה המוטמעת לצבעי RGB נפרדים (R- אדום, G- ירוק, B- כחול).
3. ביצוע התמרת Wavelet דו- מימדית בדידה מסדר ראשון על כל אחד מערוצי התמונות בנפרד באמצעות פונקציית Wavelet מסוג Daubechies. ונקבל מקדם קירוב (cA), מקדם אופקי (cH), מקדם אנכי (cV) ומקדם אלכסוני (cD).
4. התאמה של גודל המקדמים על ידי ריפוד באפסים (כי בהמשך נבצע פעולות מתמטיות ביניהם).
5. נניח ערך מסוים למקדם הטמעה שנקרא לו a בטווח של 0 עד 1. ככל שערכו גבוה יותר כך יגדל חוזק התמונה הסודית וככל שערכו קטן יותר כך תגבר שקיפות התמונה הסודית (צריך להיות זהה לערך שאיתו השתמשנו להטמיע את התמונה).
6. כדי למצוא את המקדמים של התמונה הסודית נשתמש בנוסחאות הבאות:
$$cA_{secret} = \frac{cA_{embedded} - (1-a) \cdot cA_{cover}}{a} \quad \text{עבור מקדם קירוב:}$$
$$cH_{secret} = \frac{cH_{embedded} - (1-a) \cdot cH_{cover}}{a} \quad \text{עבור מקדם אופקי:}$$
$$cV_{secret} = \frac{cV_{embedded} - (1-a) \cdot cV_{cover}}{a} \quad \text{עבור מקדם קירוב:}$$
$$cD_{secret} = \frac{cD_{embedded} - (1-a) \cdot cD_{cover}}{a} \quad \text{עבור מקדם קירוב:}$$

צריך לחשב כל אחד מהמקדמים לכל ערוץ צבע.
7. ביצוע התמרת Wavelet דו- מימדית בדידה הפוכה מסדר ראשון בעזרת מקדמי התמונה הסודית שחישבנו כדי לקבל את ערוצי הצבע (RGB) של התמונה הסודית.
8. המרת המקדמים שקיבלנו מ-double ל- 8-bit integer כך שנוכל להציג את התמונה.
9. נחבר את שלושת ערוצי הצבע של התמונה הסודית לכדי תמונה אחת ונקבל את התמונה הסודית.
10. כתוצאה מריפוד באפסים נוצרים פסים שחורים בתמונה, לכן נמצא את הפינה הימנית התחתונה ונחתוך לפיה את התמונה עם הפסים כך שנקבל את התמונה בלבד.
11. נציג את התמונה על המסך.

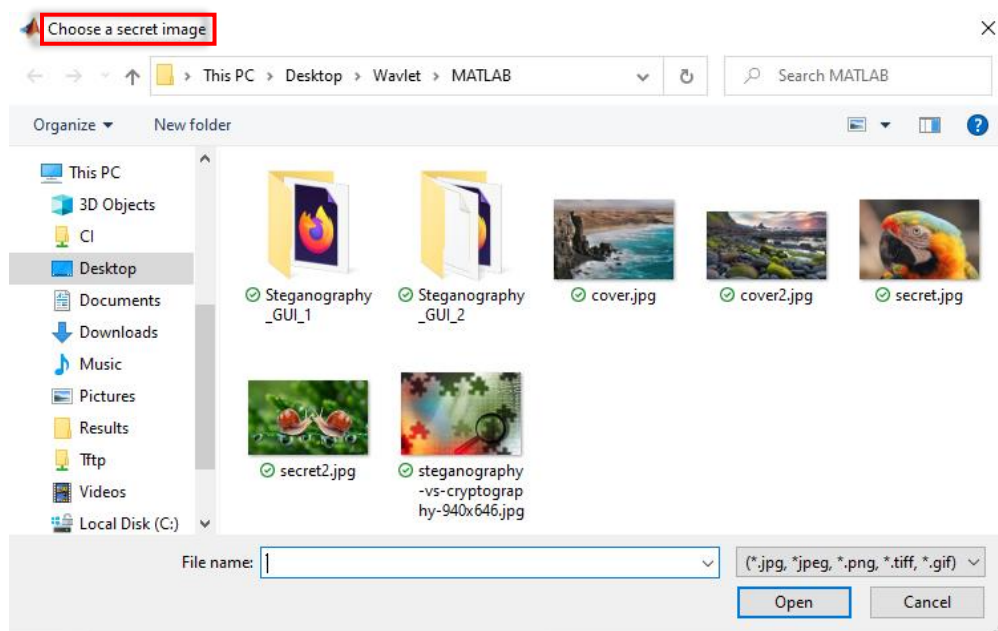
הדגמה:

כעת אראה דוגמא לביצוע הקוד: נריץ את הקוד ב- MATLAB.

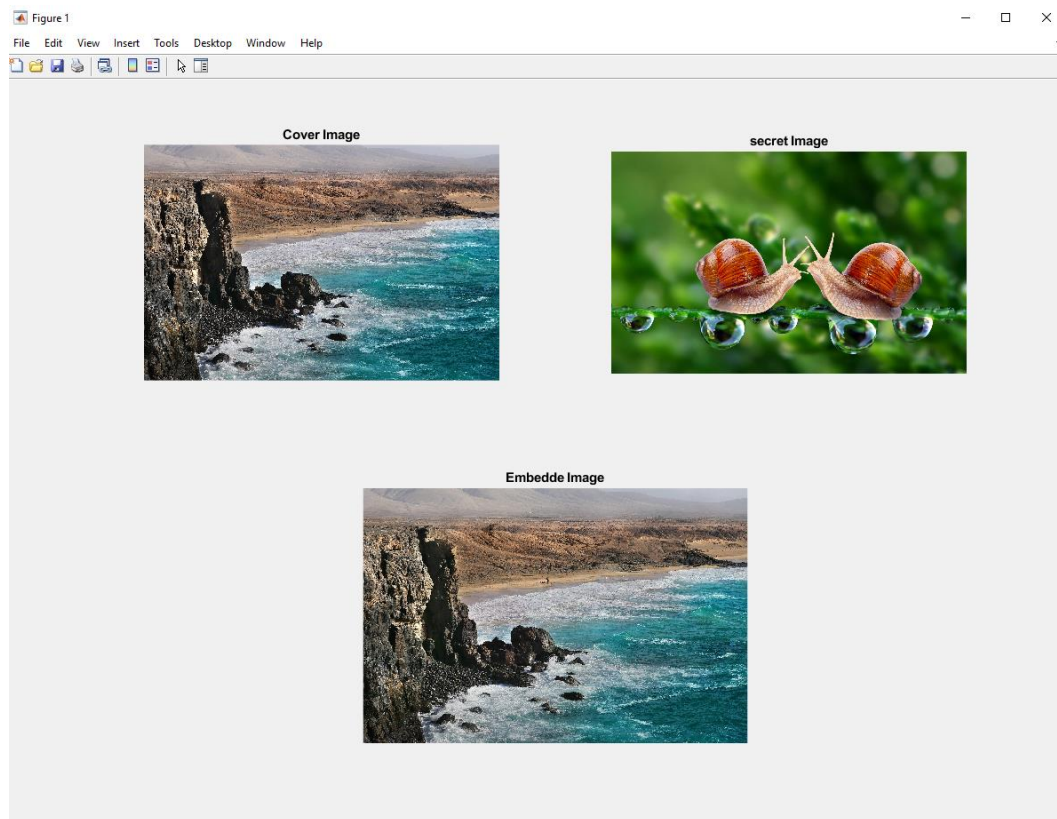
1. נבחר תמונת כיסוי:



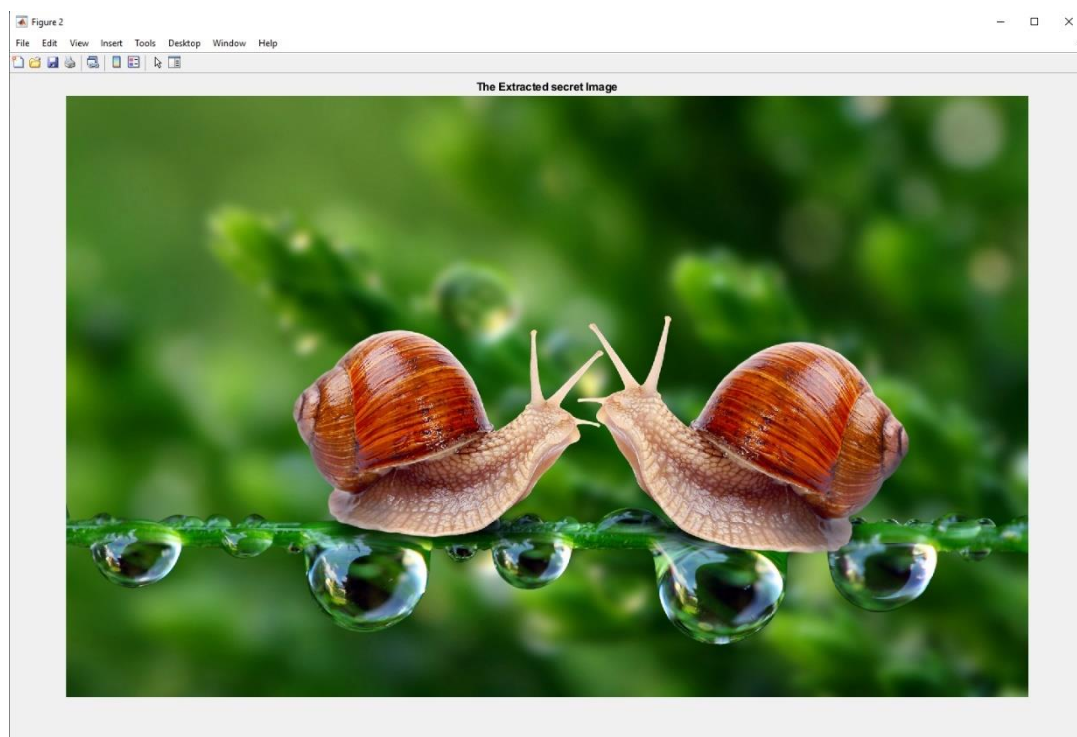
2. נבחר תמונה סודית:



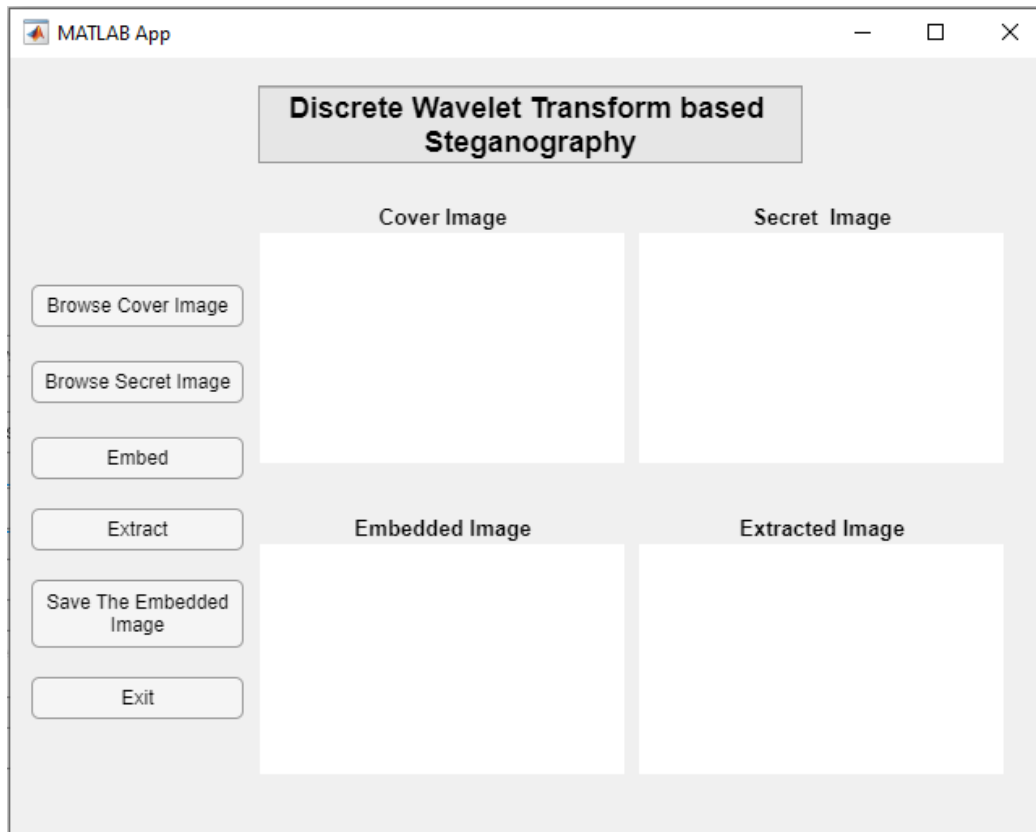
3. התוכנה תציג לנו את התמונות שבחרנו ואת התמונה המוטמעת:



4. התוכנה תציג לנו את התמונה הסודית שחולצה:



בנוסף יצרתי גם GUI לתוכנה שניתן להשתמש בו ונראה כך:



ניתן בעזרת הכפתורים לבצע שלבים שונים של הקוד:

- Browse Cover Image - ייבוא תמונת הכיסוי והצגתה.
- Browse Secret Image - ייבוא התמונה הסודית.
- Embed - יצירת התמונה המוטמעת והצגתה.
- Extract - חילוץ התמונה הסודית והצגתה.
- Save The Embedded Image - שמירת התמונה המוטמעת בתיקייה לבחירת המשתמש.
- Exit - יציאה מה-GUI.

בעיות והצעות לשיפור:

- ברגע שיוצרים את התמונה המוטמעת אנו מקבלים 3 מטריצות, אחת לכל צבע, בעלות ערכים לא שלמים כתוצאה מפעולות החישוב. דבר זה הוא בעיה להצגת התמונה שכן אנו זקוקים לערכים שלמים, לכן המרתי ערכים אלה לערכים שלמים. בעקבות זאת נוצרות שגיאות שיובילו לחילוץ לא מיטבי של התמונה הסודית.
במהלך עבודתי על המטלה ייצאתי גם את התמונה המוטמעת עם ההעגלה של הערכים, וייבאתי אותה לטובת חילוץ התמונה הסודית ממנה, אך קיבלתי את התמונה הסודית עם שגיאות. לכן, בחרתי לחלץ את התמונה הסודית מתוך קובץ התמונה ללא העגלה של הערכים כך שנקבל תמונה סודית מדויקת. אבל בנוסף הקוד שומר את התמונה המוטמעת בתיקיית המחשב שבה רץ הקוד, או לחילופין ב-GUI ישנה אפשרות לשמור אותה בכל תיקייה שנבחר.
• ניתן יהיה לשפר זאת אם נמצא דרך לשמור את התמונה המוטמעת עם הערכים המקוריים, ללא ההעגלה שלהם, בצורה שגם תאפשר להציג את הקובץ כתמונה.

ביבליוגרפיה:

מבוסס על המאמר:

T. Narasimmalou and J. R. Allen, "Optimized discrete wavelet transform based steganography," *2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 2012, pp. 88-91, doi: 10.1109/ICACCCT.2012.6320747.