תכנון לפרויקט קורס - הגשת הצעת פרויקט

חלק ראשון: רקע

<u>מגישות - קבוצה 10:</u>
לאה ברודסקי
יאנה ענהאל צ'יצ'קין
מנו ריי
זיו גימני

<u>המאמר שבחרנו-</u>
Hiding data in images using steganography techniques with compression algorithms

<u>סיכום כללי של המאמר-</u>
המאמר משווה בין שיטות שונות של הסתרת מידע באמצעות סטגנוגרפיה.
בדרך כלל כל שיטה מיושמת בנפרד, אך שילוב של מס' שיטות סטגנוגרפיה וגם שילובם עם קריפטוגרפיה יכולה לספק אבטחה טובה וחזקה יותר.
במאמר מבצעים ניסוי שבו מציעים אלגוריתם המשלב מספר שיטות של הסתרת מידע בתמונה על ידי יישום של DCT לצורך הטמעת התמונה, הצפנה של המידע באמצעות אלגוריתם קריפטוגרפי, יישום של דחיסת DCT, ולבסוף העברת התמונה שבתוכה המידע המוסתר (תמונת סטגו) לצד המקבל שיממש את האלגוריתם בצורה ההפוכה.
בניסוי בחנו את כמות המידע הרב ככל הניתן שהיה אפשר להסתיר בתמונה עם השינויים הכי פחות ניכרים לעין.
את המחקר ערכו באמצעות מדדים שבוחנים את השינוי שעברה תמונת הסטגו שאותם נפרט בהמשך.
<u>תוצאות המחקר :</u>
מהתוצאות ניתן להסיק כי יכולת ההטמעה באלגוריתם המוצע טובה מאוד
ניתן לראות לפי המדדים PSNR ו-MSE כי:
איכות התמונה גבוהה ובעלת אבטחה גבוהה יותר כאשר משתמשים ב- DCT עם LSB מאשר בשימוש LSB בלבד- יש עיוות קטן בתמונה הסטגו.
שיטת DCT היא טובה יותר אך תוצאות המחקר הראו כי השילוב בין שתי השיטות הוא היעיל ביותר ומבטיח יותר אבטחה.

על פי המאמר- ניתן להסתיר את הנתונים בהודעות על ידי צמצום גודלם, מה שמאפשר לנו להעביר את הנתונים בצורה
בטוחה יותר עם פחות עומס.
השימוש ב- LSB וב-DCT מפחית את מספר הביטים\בתים הכללי בקובץ, כך שניתן להעביר אותו מהר יותר באמצעות
חיבורי אינטרנט איטיים יותר, או לתפוס פחות מקום בדיסק.
טכניקה זו יעילה וגם שומרת על : שלמות , קיבולת ועמידות.

חלק שני: הצעות שיפורים

1. שימוש באלגוריתם RSA כדי לאבטח את ההודעות המועברות בערוץ התקשורת.

האלגוריתם שמוצע במחקר לא מתייחס לאבטחת ערוץ התקשרות אלא רק בשיטת ההטמעה של המידע הסודי בתמונה. שימוש בRSA לאבטחת ההודעות משפרת את האבטחה.

ציטוט מהטקסט:

> "Indeed, the receiver sends the public key to the sender by an **insecure communication channel.** Then, the sender generates the stego-image with both keys and sends them through **another insecure channel** to the receiver, who can extract the secret file, which is inserted into the cover image by the embedding procedure."

מאמר- "המקבל שולח את המפתח הציבורי לשולח על ידי ערוץ תקשורת **לא מבוטח**, לאחר מכן השולח מייצר את תמונת הסטגו עם 2 המפתחות ושולח אותם למקבל דרך ערוץ אחר **לא מבוטח**"

2. שיפור אלגוריתם LSB-

במאמר עושים שימוש באלגוריתם LSB סטנדרטי שבחישוב שלו עושים שימוש במודולו 2.
ניתן לשפר את הנוסחה כך שנממש את האלגוריתם עם מודולו של מספר גדול יותר לדוגמא מודולו 3.
זה יגרום לצמצום מספר השינויים והעיוותים בתמונת הכריכה.

ציטוט מהטקסט על אלגוריתם ה-LSB הסטנדרטי:

"PSNR and MSE show that the image quality is high and has a higher level of security, in case of using DCT with LSB than using LSB alone **which mean low distortion in the stego image**"

איכות התמונה גבוהה ובעלת אבטחה גבוהה יותר כאשר משתמשים ב- DCT עם LSB
מאשר בשימוש LSB בלבד-יש עיוות קטן בתמונת הסטגו.
לכן אם נשתמש במודולו גדול יותר עם DCT - עיוות התמונה יקטן עוד יותר.

3.שימוש במדד SSIM במקום PSNR ו-MSE.

SSIM משמש להערכה של עיוות התמונה בתמונה המקורית בדומה למדדים שבמאמר שלנו (PSNR ו-MSE) אך מדד זה מראה תוצאות טובות יותר לעין האנושית.

ציטוט מהמאמר:

"As enactment measurement for image distortion, a practical objective measure for this property are the Mean Squared Error (MSE) and the Peak

Signal to Noise Ratio (PSNR) between the cover image and the stego-image. Mean Square Error (MSE): It is the degree used to quantify the alteration between the preliminary and the distorted or noisy image.”

"…. In truth, traditional PSNR measurements do no longer correspond to an individual’s perception. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB suggest a fairly low quality, i.e., distortion because of embedding can be obvious; however, a high-quality stego image should struggle for 40 dB and above. In this section, we report the experimental results evaluating our approach with the O.CETIIN et al."

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

הנוסחה מחשבת את מדד הדמיון המבני בין 2 תמונות נתונות שהוא ערך בין – 1 ל מינוס 1.
ערך של 1+ מציים ששתי התמונות הנתונות דומות מאוד או זהות.
ערך 1- מציין ששתי התמונות הנתונות שונות מאוד.

חלק שלישי: תכנון

<u>אבני דרך ולו"ז עבודה-</u>

- שבוע 12- מציאת מידע רלוונטי
- שבוע 13- נעבוד על השיפור הראשון
- שבוע 15- נתחיל לעבוד על השיפור השני
- שבוע 17- נתחיל לעבוד על השיפור השלישי
- בסוף מועדי א - הגשת הפרויקט + דו"ח מסכם

<u>אתגרים טכנולוגיים שאיתם נתמודד:</u>

- התאמה לתנאים טכנולוגיים שונים
- התאמה לגורם האנושי - הצורך המשתנה של המשתמש
- שימוש בספריות לא מוכרות (לנו) בפייתון