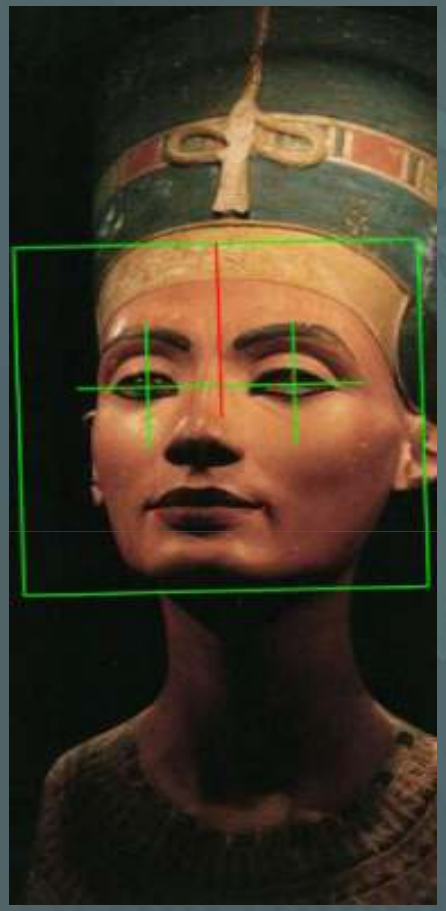
Counter-Fight

אימות והגנת תעודות



פברואר 2009

הבעייה

- בתעודה מזויפת מופיעים נתוני אדם אמיתי, שאינו חשוד, שתמונתו הוחלפה על ידי מתחזה
- כאשר החלפת התמונה מתבצעת בידי מומחים, קשה מאד לגלות את הזיוף
- זייפן עובר בקלות מחסומי ביקורת (ביקורת דרכונים, ביקורות דרכים, קבלת שרות כמתחזה)

הטכנולוגיה המוצעת

- המנגנון המוצע להגנה על תעודות מבוסס על שמירת הנתונים **בתעודה עצמה**
- נחסך הצורך בפנייה למאגר נתונים לצורך אימות
- מרכיבי התעודה, טקסט ונתוני תמונה, מוצפנים בתעודה עצמה
- תווית ברקוד דו-מימדי הינה הרכיב האופטימלי, משיקולי עלות-תועלת
- סביר לאחסן בברקוד כ- 1000 תווי נתונים

טכנולוגית ההצפנה

הקבוצה פיתחה אלגוריתם הצפנה ייחודי

האלגוריתם מבוסס על:

- מנגנון 'כאוטי' – לא מתמטי, לקידוד והצפנה
- מפתח הצפנה חדשני - אקראי (PHR - Pure Human Random)

- ההצפנה המתקבלת הינה בעלת עוצמה חזקה ביותר

נפח הנתונים אינו גדל

- ניסיונות לפריצתה, לא צלחו.

- המנגנון נרשם כפטנט בינלאומי ונמצא בשלב Pending

דרגות האבטחה

- נתוני התעודה (מספרה, שם המחזיק, כתובת, תאריך לידה, צבע עיניים, גובה, תאריך הנפקה) מוצפנים לרצף תווים
  התווים ניתנים לקריאה, אך חסרי מובנות

- ההצפנה אינה מגדילה את נפח הנתונים ומשאירה מקום לנתוני התמונה

- אלמנט איחסון, המהווה חלק אינטגרלי של התעודה, אוצר את המידע והופך אותו לזמין רק למשתמש מורשה
  (מחזיק באלגוריתם ובמפתח)

אלמנט האיחסון

ככל שנפח האיחסון של הרכיב בתעודה גדול יותר, כך גדלה כמות המידע שהתעודה נושאת עימה לאשר ילך נושא התעודה:

- כרטיס חכם
- RFID
- ברקוד

בעתיד אולי יוסכם לעשות שימוש באמצעים אלקטרוניים, כגון Disk-on-Key כיום נפוץ ומקובל רק השימוש בנייר ומרכיבים פלסטיים

כרטיס חכם כרכיב המידע

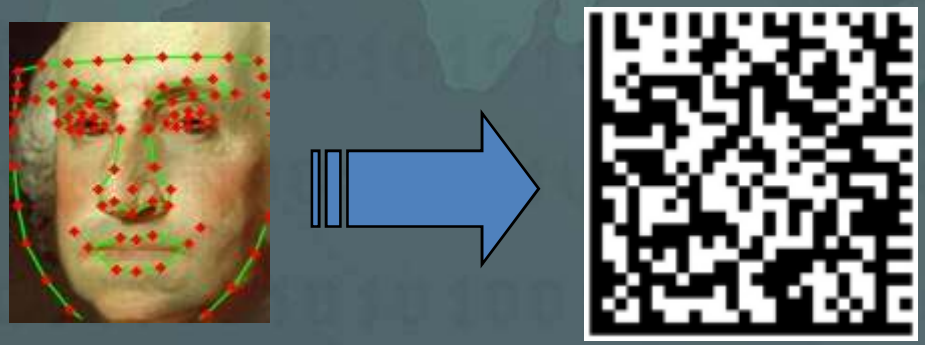
- בכרטיס החכם ניתן לאחסן כמות גדולה של נתונים
- כרטיס חכם, אם ייכלל בתעודה, יאפשר לאחסן את תמונת נושא התעודה המקורי – מוצפנת
- התמונה תצטרף לנתונים האישיים, שגם הם יוצפנו לפני הטמעתם בכרטיס
- מנגנון ממוחשב יציג לנציג הרשויות את התמונה המפוענחת, אותה ישווה הבודק לאדם הנמצא לפניו.

RFID כרכיב המידע

- האמצעי, מבוסס על גלי רדיו, מאפשר הטמעת כמות גדולה יחסית של נתונים
- אפשר לאחסן בו תמונה ונתוני טקסט של נושא התעודה - מוצפנים
- חסרונו : ניתן לקרוא אותו ממרחק, מבלי שנושא התעודה יהיה מודע לעובדה שמעתיקים את זהותו
- הרכיב מהווה איום על פרטיותו של האדם. רשויות רבות פסלו את הרכיב לשימוש בתעודות

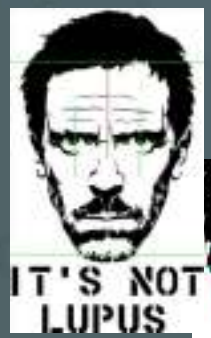
תווית ברקוד כרכיב מידע

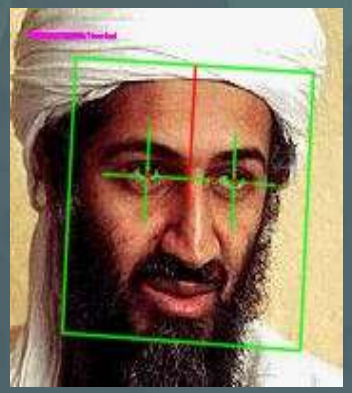
- הברקוד הדו-מימדי מאפשר לאחסן ולקרוא כ- 1000 תווי נתונים
- נפח האיחסון אינו מאפשר לאחסן תמונה מלאה בנוסף לנתונים האישיים
- ניתן למצות מהתמונה את מאפייניה הייחודיים, להצפין אותם ולהטמיעם בברקוד
- התעודה הופכת לבסיס נתונים נייד

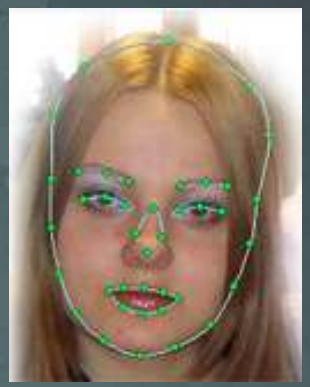


מאפייני התמונה

- טכנולוגיית זיהוי פנים הפכה לזמינה ביותר בעידן הממוחשב
- בשילוב מערכות זיהוי קלסתר ממוחשב,
  ניתן להפיק פרמטרים רבים מתמונת המקור :
  מיקום העיניים, מיקום האף והגבות,
  מרחקים מדודים וקואורדינטות מרכיבי הפנים
  (טביעת פנים, בדומה לטביעת אצבע)







ההטמעה המוצפנת של זיהוי התמונה

- בברקוד הדו-מימדי ניתן להטמיע את פרמטרי הקלסתר
- מדבקת ברקוד (מוצפנת) תודבק באחד מאזורי התעודה
- לא ניתן לייצר מדבקה מתמונה ללא מערכת ההצפנה
- אם תוחלף התמונה לא תתקבל התאמה = תעודה מזויפת

אימות מדבקת הברקוד

- סריקת התמונה, פענוח התוכן ועיבוד הנתונים, יאמתו שהתמונה לא הוחלפה
- מכשירי סריקה ניידים יכולים להיות מותקנים בניידות משטרה, הכוללות כבר כיום מסופי מחשב
- ניתן לבנות מזוודה ניידת לביקורת מזדמנת - (כגון מחסום דרכים)
- כמובן שבנקודות ביקורת שגרתיות - אין בעייה להפעיל אלגוריתם פענוח ואימות (במשטרה, בביקורת דרכונים, משרדי ממשלה)

הנפקת המדבקה (או ספח לתעודה)

- מנפיק מורשה המחזיק בפרטי התעודה ובתמונה הזהה לתעודה (תעודת זיהוי, דרכון) יכול להנפיק את המדבקה גם ללא נוכחות פיזית של נושא התעודה
- המדבקה מופקת מהעתק התמונה ומהפרטים הרשומים במחשב משרד הפנים
- בתעודה חדשה תוצמד המדבקה במשרד המפיק
- לתעודה קיימת ניתן לשלוח המדבקה בדואר (אפילו כאמצעי זמני – עד לזימון והנפקת תעודה בפורמט חדש, אם יוחלט)

מנגנון האימות

- חשוב שמנגנון הפענוח יהיה באתר מרכזי מאובטח באופן זה ניתן יהיה להגן עליו פיזית למניעת גילוי מנגנון ההצפנה ומפתח ההצפנה

- נקודות הביקורת צריכות להיות מקושרות למרכז הפענוח, אשר יקלוט את תשדורת הבקשה לשרות ויחזיר את הפרטים המפוענחים (בדומה לפעולת מסופי משיכת המזומן בבנקים)

- ההתייחסות לתמונה תהיה : דרגת אמינותה
  ניתן לעשות שימוש גם בקשר אינטרנטי ובקשר סלולארי

- הערה :
  ניתן להקים מרכזי פענוח נוספים, בכל אתר שהלקוח יחפוץ, בהעדר תלות במאגר נתונים יחיד

העלות

- ההנפקה הפיזית של מדבקת הברקוד כרוכה בעלות זניחה. ניתן גם להפיק שתי מדבקות להכפלת העמידות בפני בלאי הזמן
- החומרה לנקודת הבדיקה הינה בעלות סבירה של מאות דולרים לסורק אופטי (SCANNER)
- הסורק מסוגל לקרוא את התמונה וגם את הברקוד
- השימוש בטכנולוגיה יחייב:
  - ❖תשלום בגין הנפקת מדבקה
  - ❖תשלום בגין פענוח, לפי צריכה (או תשלום שנתי קבוע)