UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

SURYS

utt université de technologie Troyes

INSTITUT CHARLES DELAUNAY

Sécurisation d'un QR code

Solution pour lutter contre la contrefaçon d'étiquettes

Hoai Phuong Nguyen (CReSTIC/URCA – LM2S/UTT)
Frédéric Morain-Nicolier (CReSTIC/URCA)
Florent Retraint (LM2S/UTT)
Agnès Delahaies (CReSTIC/URCA)
Marc Pic (SURYS)

Plan de présentation

- Contexte et problème étudié
- Solutions proposées
  - Conception des QR codes sécurisés
  - Principe
  - Formulations mathématiques
  - Expérimentations
- Conclusion

Contexte & Problème

- La contrefaçon des produits

  → Des conséquences économiques pour des entreprises, des consommateurs
- Des moyens anti-contrefaçons
  - *Des étiquettes RFID/NFC*
  - *Des hologrammes*
  - *Des microtaggants (nano techno)*
  - *Des encres spéciales*
  - *Des code-barres*
    - *Données transmises sont comparées avec celles stockées sur un serveur*
    - *La reproduction d'une code-barres valables est facile*

    → *La contrefaçon d'étiquette*
- Problème :

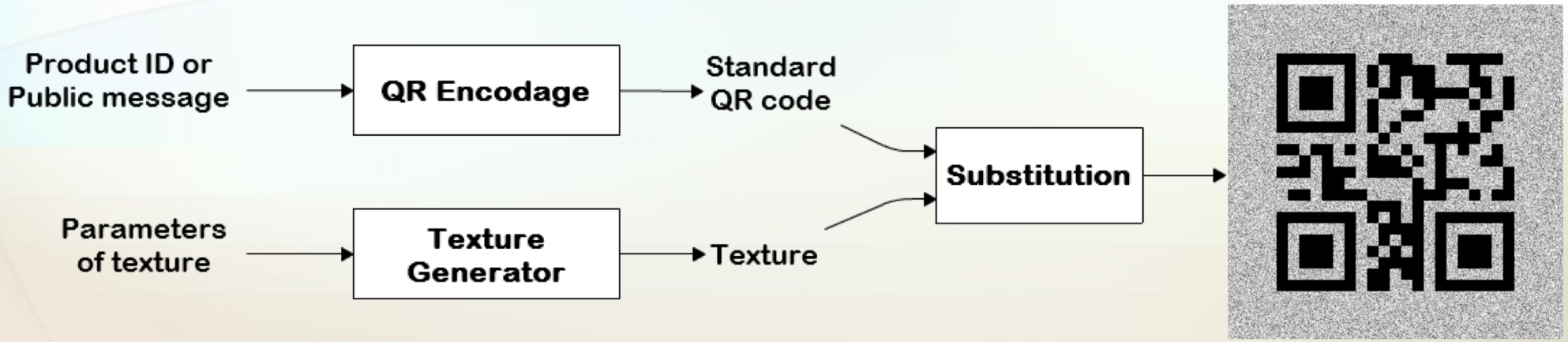
  → *Renforcement les code-barres (i.e. QR) contre sa reproduction*

  → W-QR : W pour *Watermarking*

QR code-barres standard

- *Quick Reponse,* ISO/IEC
- Code binaire en 2 dimensions
- Quantité d'information transmissible importante
- Lecture facile et rapide
- Robuste contre les distorsions
  - Corrections des erreurs
- Facile et pas cher à produire

W-QR: Conception



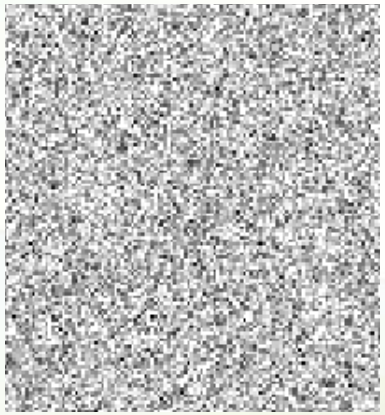
La conception de Watermarked-QR code-barres

W-QR: Texture

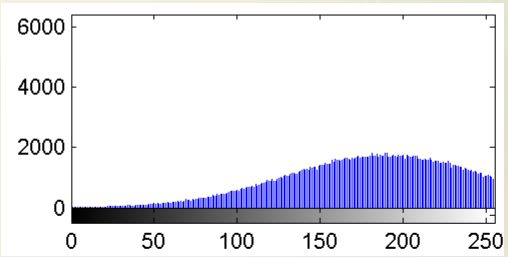
- Une couche de sécurité supplémentaire qui rend la production des code-barres plus sophistiquée.
- Des caractéristiques souhaitées:
  - Ne pas empêcher la lecture d'un code standard
  - Ayant un code imprimé, il est difficile de retrouver son original numérique
  - Sensible à la numérisation et l'impression
    - La reproduction par scanner et réimpression doit abimer la texture
    - La détérioration est détectable

W-QR: CGN texture

- CGN : *Clipping Gaussian Noise*
- Du bruit blanc est ajouté dans une image de gris uniforme
- L'effet « *clipping* »
  - Des niveaux de gris sont codés par 256 niveaux de 0 à 255
  - Certains pixels vont être saturés lors de l'ajout du bruit
    - Les pixels dont la valeur dépasse 255 vont être codés par 255
    - Les pixels dont la valeur est < 0 vont être codés par 0.

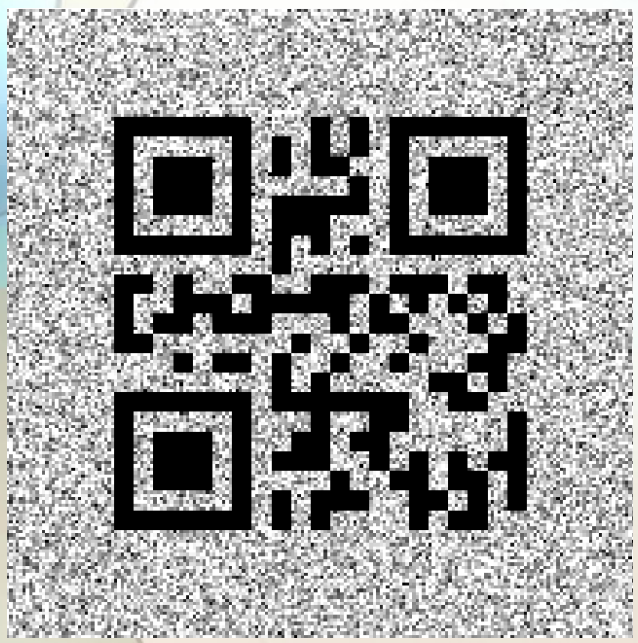


CGN texture (numérique)



Histogramme de CGN texture

W-QR: code sécurisé



W-QR version numérique

Numérisation du W-QR imprimé

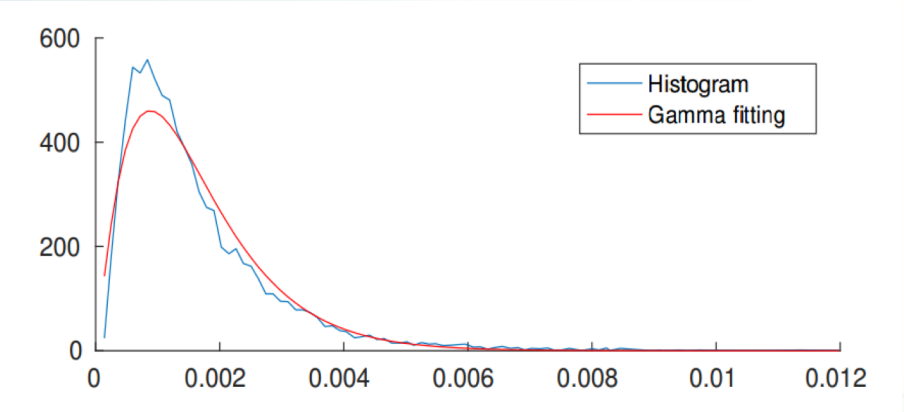
Numérisation du W-QR falsifié par Scan-Reprint

Base de données

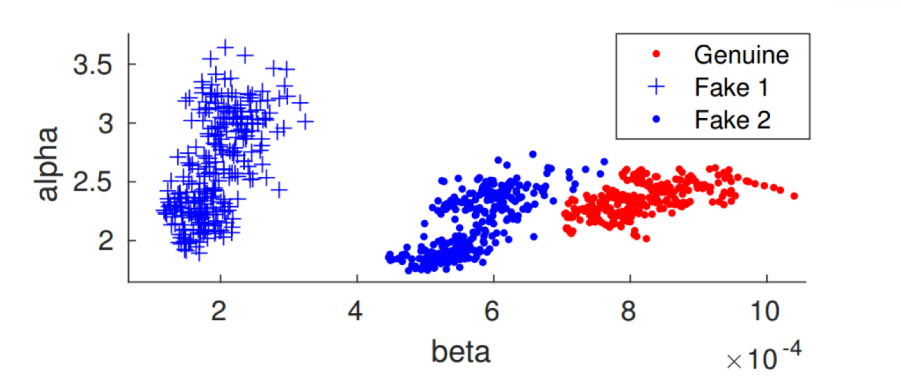
- Matériels
  - 270 W-QR codes numériques
    - 500x500 pixels
  - Impression par l'imprimante P1 (600dpi) → 270 codes authentiques
  - Impression par l'imprimante P1 (600dpi), numérisation à 600dpi puis réimpression par P1 → 270 codes falsifiés type 1
  - Impression par l'imprimante P2 (600dpi) → 270 codes falsifiés type 2
    - P2 est du même modèle que P1
- Tous les codes imprimés sont numérisés avec la camera d'un téléphone Samsung S6.

La détection

- NLV : *Variance locale du bruit (Noise Local Variance)*
  - Calculée pour tous les blocs 8x8 du bruit d'image (partie texturée)
  - La distribution de l'NLV peut être approximée par une distribution Gamma.
- ***A watermarking technique to secure printed QR codes using a statistical test.***
  - *GlobalSIP 2017: 288-292*

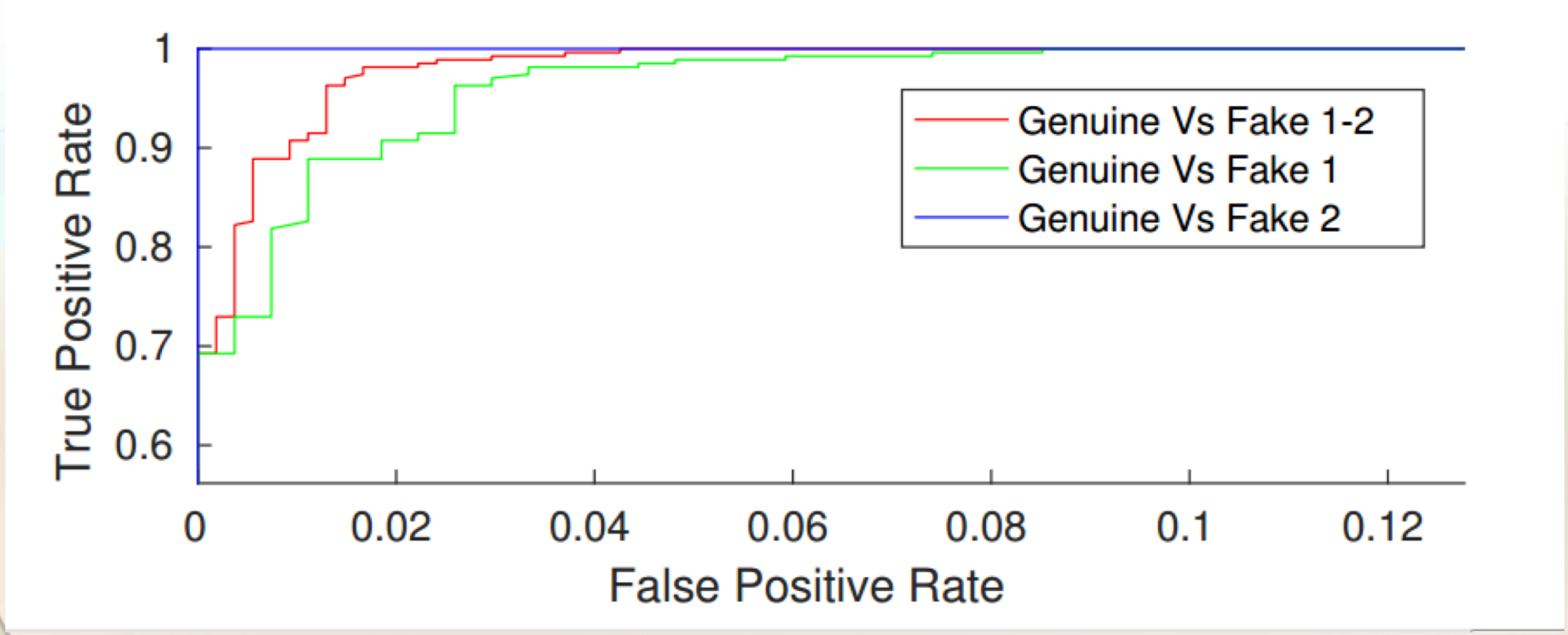


Distribution de l'NLV



Comparaison des paramètres de la distribution du NLV entre images originales et falsifiées

La détection



Performance de classification du détecteur proposé

La détection

Limites:

- Du bruit n’est pas i.i.d
- La distribution gamma du NLV n’est pas stable entre des images authentiques

→ Pertes de puissance des test statistiques

La détection évoluée

Solution proposée

- → Transformer l'image en LBP (*Local Binary Pattern*)
  - → Eliminer l'impact de la non conformité des sources de lumière
- → Transformer l'image LBP en DCT (*Discrete Cosine Transform*) pour avoir une présentation dans la domaine fréquentielle.
- → Confirmer l'I.I.D caractéristique des coefficients DCT entre des images (par expérimentations) → modélisation statistique
- → Pour chaque coefficient, construire un test statistique
- → Fusionner les tests statistiques de tous les coefficients.

La détection évoluée

Pour chaque coefficient DCT:

- Z l'ensemble de valeurs du coefficient.
- $Z = \bigcup_{i=1}^{N} Z_i$ d'où $Z_i = \{z_j \mid j \in I_i\}$, sous-ensemble de taille constante M.
- z_i sont i.i.d et d'écart-type σ
- $X = \left\{ x_i = \frac{1}{M-1} \sum_{j \in I_i} \left(z_j - \bar{z}_i\right)^2 \mid i = 1, 2, \ldots, N \right\}$

$$X \sim \Gamma\left(\frac{M}{2}, \frac{2\sigma^2}{M}\right)$$

La détection évoluée

Pour chaque coefficient DCT:

- Un test d'hypothèse est proposé
- H_0 pour une image authentique, H_1 pour une image falsifiée

$$\begin{cases} H_0 : & X \sim \Gamma(a, b_0) \\ H_1 : & X \sim \Gamma(a, b) \end{cases}$$

où $a = \frac{M}{2}$, b_0 est une constante connue et $b \neq b_0$

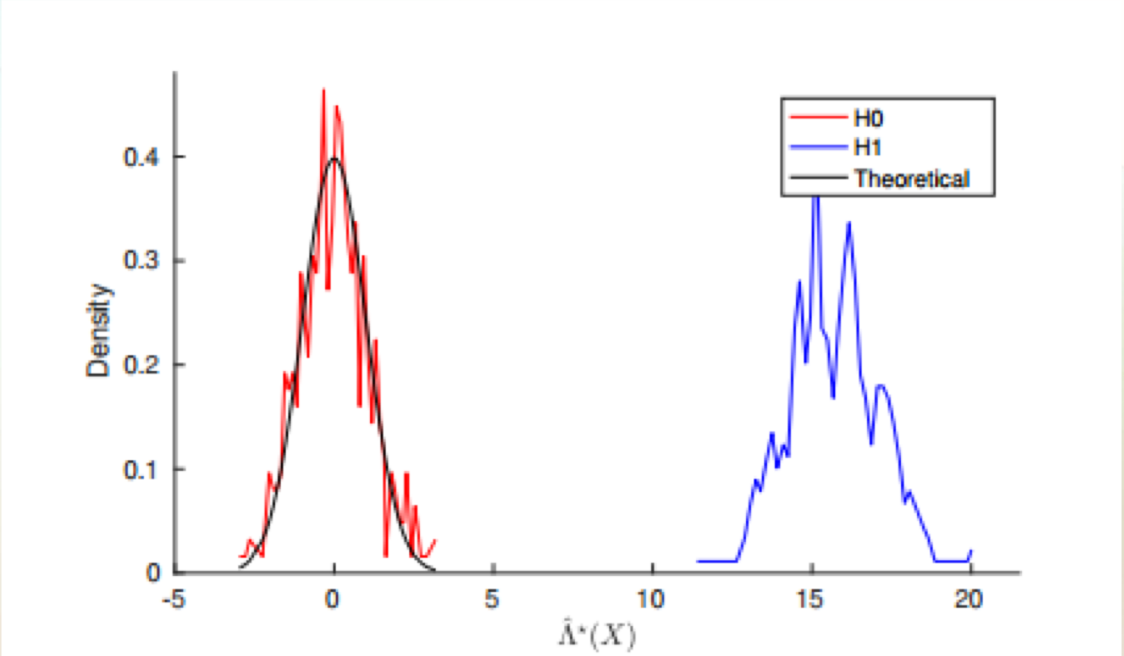
La détection évoluée

b connue

$\widehat{\Lambda}^*(X)$: Logarithme du rapport de vraisemblance *(simplifié et normalisé)*

Sous l'hypothèse H_0:

$\widehat{\Lambda}^*(X) \sim N(0,1)$



La détection évoluée

b inconnue

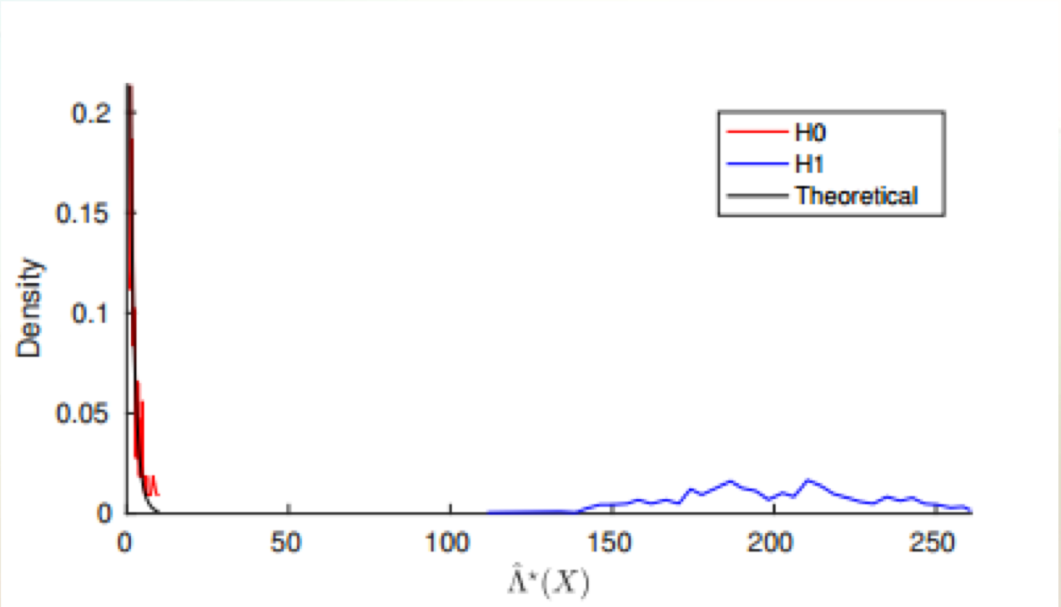
$\widehat{\Lambda}^*(X)$: Logarithme du rapport de vraisemblance *(simplifié et normalisé)*

Sous l'hypothèse H_0:

$\widehat{\Lambda}^*(X) \sim \mathrm{X}^2(1)$

Sous l'hypothèse H_1:

$\widehat{\Lambda}^*(X)$ suit un khi-deux décentré



Travail restant

- Réfléchir sur la stratégie de fusionnement des tests statistiques
  - Les puissances de détection pour tous les coefficients ne sont pas identiques
  - Identifier les coefficients les plus signifiants en fonction des configurations de la texture.
  - Est-il efficace d'utiliser tous les coefficients?

Conclusion

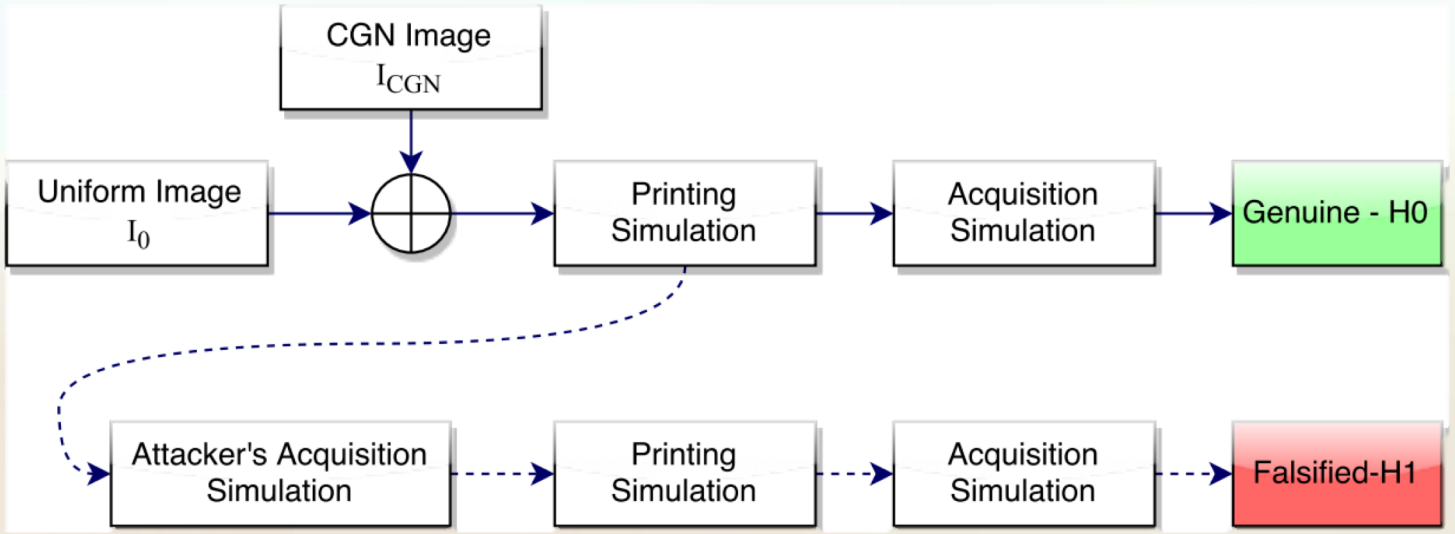
- Proposition d'une solution pour sécuriser les QR code-barres dans le but de lutter contre la contrefaçon.
- Nous travaillons actuellement sur une version évoluée de la texture et du test statistique
  - Comportement statistique plus stable
  - Améliorer la performance de la détection
- Test du code sur du papier ordinaire avec une imprimante laser. Planification de tests sur d'autres supports avec différentes techniques d'impression.

Merci pour votre attention

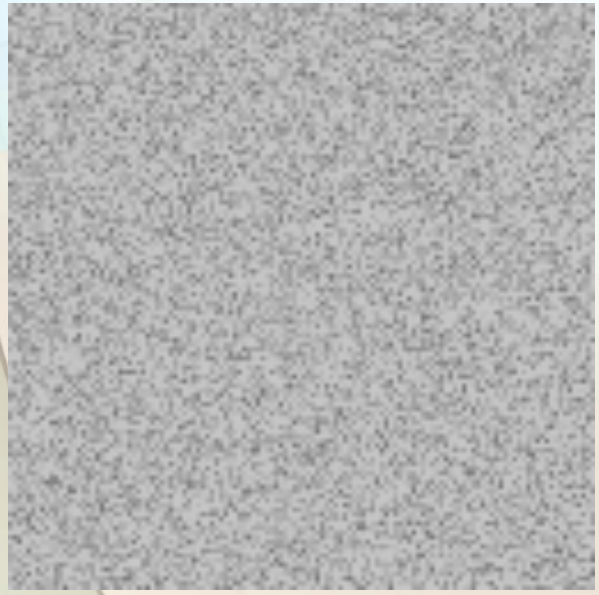
Avez-vous des questions?

La détection évoluée

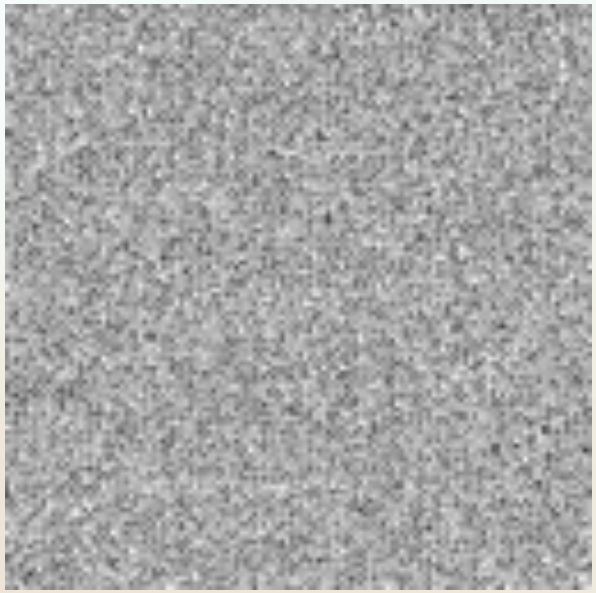
- Simulation des images



La détection évoluée



Version numérique



Simulation de la version authentique

Simulation de la version falsifiée

La détection évoluée

- Simulation du processus de l'impression