Authentification par codes graphiques: optimisation du canal d'impression-acquisition

Anh Thu Phan Ho, Bao An Hoang Mai, Wadih Sawaya, Patrick Bas

Authentification par codes graphiques: optimisation du canal d'impression-acquisition

Anh Thu PHAN HO[1], Bao An MAI HOANG[1], Wadih SAWAYA[1], Patrick BAS[2]

[1]Institut Mines-Telecom, Telecom Lille
CRIStAL UMR 9189, Rue Guglielmo Marconi, 59651 Villeneuve d'Ascq, France

[2]CNRS - Ecole Centrale de Lille
CRIStAL UMR 9189, Cité Scientifique, 59651 Villeneuve d'Ascq, France

Anh-thu.Phanho@telecom-lille.fr, Bao-an.Maihoang@telecom-lille.fr
Wadih.Sawaya@telecom-lille.fr, Patrick.Bas@ec-lille.fr

Résumé – Nous proposons de formaliser le problème d'authentification par codes graphiques comme un jeu entre la source légitime et l'adversaire, chaque joueur essayant de sélectionner le meilleur canal d'impression/acquisition pour maximiser/minimiser les performances d'authentification. Il est possible de résoudre ce jeu en utilisant des estimations précises des probabilités de fausse alarme et non détection et en modélisant le canal d'impression-acquisition comme un canal additif Gaussien Généralisé ou Lognomal. L'optimisation s'effectue en considérant deux types de scénarios: la présence d'un adversaire passif (qui possède un canal identique à la source légitime), puis la présence d'un adversaire actif (possédant un canal différent). Elle conduit à une formulation $\min\max$. Les résultats de ce cheminement soulignent plusieurs points: (i) les performances d'authentification sont meilleures pour des distributions denses, (ii) les paramètres optimaux de l'adversaire sont proches de ceux de la source légitime, (iii) la source légitime peut trouver une configuration qui maximise les performances d'authentification.

Abstract – We setup the framework of authentication using graphical codes as a game between the adversary and the legitimate source, each actor trying to select the best print-and-scan channel. It is possible to solve this optimisation process by using reliable false alarm and non-detection probabilities et by modelling the print-and-scan channel by Generalised Gaussian or Lognormal densities. We consider two scenarios: a passive adversary who uses the same manufacturing process than the legitimate source and an active adversary who tries to use the worst print-and-scan channel for authentication, this leads to a $\min\max$ optimisation. This analysis brings several conclusions: (i) the authentication performances are better for denses noises than for sparse ones, (ii) the optimal parameters for adversary are close to the parameters of the legitimate source, (iii) it is possible to find configurations that maximise the authentication performances.

1 Introduction

L'authentification d'objets imprimés, qui consiste à apporter la preuve qu'un objet donné n'est pas une copie, est un sujet d'une importance considérable. Les solutions associées doivent en effet permettre de lutter contre la contrefaçon de différents objets tels que des papiers d'identité, ou encore les médicaments en sécurisant leurs emballages.

Ce type d'authentification peut s'effectuer soit en caractérisant directement les éléments non-clônables de l'objet (les fibres de papier à l'échelle microscopique par exemple [1]), soit en exploitant la dégradation provoquée par l'interaction entre un procédé physique (impression, gravure) et le support. Cette deuxième solution, que nous considérons dans ces travaux, peut s'apparenter à une Fonction Physique Non-Clônable (PUF en anglais) [2] puisque le procédé qui ne peut pas être identiquement reproduit par le contrefacteur, peut alors être utilisé pour l'authentification.

Nous étudions ici le système d'authentification proposé par Picard [3] qui repose sur l'impression d'un code binaire à très haute résolution (2400 ppp sur une imprimante offset). Le système est présenté sur la Figure 1 et se décompose comme suit : la source légitime imprime un code binaire aléatoire x^N généré à partir d'une clé secrète, ce code représentant une matrice de N éléments, sur un document ou un emballage. Le receveur authentifie l'objet en scannant un code pouvant provenir de la source légitime ou de l'adversaire qui aura copié le code ; ce dernier réalisant une copie en observant le code imprimé puis scanné y^N (étape 1 de la Figure 1) et en regénérant un code binaire $\hat{x}^N$ (étape 2). Cette étape de seuillage est indispensable car une imprimante industrielle ne peut imprimer que des entrée binaires (des points). A la suite de ce deuxième procédé d'impression-acquisition, le code copié z^N généré par l'adversaire (étape 3) possède une distribution différente du code imprimé légitime y^N et cette distinction est directement utilisée par le procédé d'authentification (étape 4), détaillée dans la section suivante.

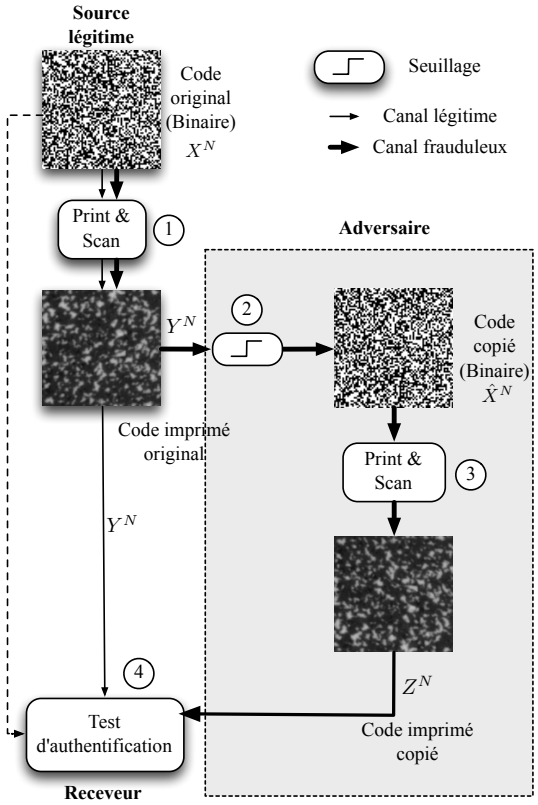

FIGURE 1 – Authentification utilisant des codes graphiques.

2 Modèles pour l'authentification

2.1 Principe du système d'authentification

Le receveur légitime observe un code en niveaux de gris o^N et nous supposons que la séquence observée $(O^N \mid x^N)$ (conditionnée par le secret binaire x^N) est indépendante et identiquement distribuée (i.i.d.). Sous ces hypothèses nous pouvons utiliser le test de Neyman Pearson, défini par :

$$L = \log \frac{P(o^N \mid x^N, H_1)}{P(o^N \mid x^N, H_0)} \underset{H0}{\overset{H1}{\gtrless}} \lambda. \tag{1}$$

où H_0, associée à la distribution $P(O \mid x, H_0)$, représente l'hypothèse que la séquence observée provienne de la source originale, et H_1, associée à la distribution $P(O \mid x, H_1)$, représente l'hypothèse que la séquence observée est un faux. D'un point de vue pratique, $P(O \mid x, H_0)$ modélise le procédé d'impression-acquisition de la partie légitime alors que $P(O \mid x, H_1)$ modélise la concaténation des procédés d'impression-acquisition légitimes et frauduleux.

2.2 Expression asymptotique des performances

Avant de présenter le jeu de l'optimisation en section 3, nous rappelons les résultats de [4] qui proposent une méthode permettant d'obtenir une approximation précise des probabilités d'erreur de type I (α, la probabilité de détecter un code authentique comme étant une copie), et de type II (β, la probabilité de détecter une copie comme authentique). Au lieu d'utiliser l'approximation Gaussienne de L qui n'est pas fiable lorsque le seuil λ de (1) est loin de $\mathbb{E}[L]$, nous utilisons la borne de Chernoff [5]. Pour des séquence aléatoires i.i.d., la distribution de la variable aléatoire $L = \sum_i \ell(O_i \mid x_i)$ dépend de l'origine du code observé (H_0 ou H_1), et pour tout réel s, la fonction génératrice des moments semi-invariante pour chaque $\ell(O_i \mid x_i)$ est définie par $\mu_\ell(s; H_j) = \sum_{x=0,1} \mu_{\ell/x}(s; H_j) = \sum_{x=0,1} \log E_{O|x,H_j}\left[e^{s\ell(O|x)}\right]$.

Les erreurs de type I et II, peuvent alors être précisément approchées pour un N suffisamment grand (avec approximativement $N/2$ points noirs) :

$$\begin{aligned} \alpha &= \Pr(L \geq \lambda \mid H_0), \\ &\underset{N\to\infty}{\to} \frac{1}{\tilde{s}_0\sqrt{N\pi\mu''_\ell(\tilde{s}_0; H_0)}} e^{\frac{N}{2}\left[\mu_\ell(\tilde{s}_0; H_0) - \tilde{s}_0\mu'_\ell(\tilde{s}_0\,; H_0)\right]}. \end{aligned} \tag{2}$$

et

$$\begin{aligned} \beta &= \Pr(L \leq \lambda \mid H_1), \\ &\underset{N\to\infty}{\to} \frac{1}{|\tilde{s}_1|\sqrt{N\pi\mu''_\ell((\tilde{s}_1; H_1)}} e^{\frac{N}{2}\left[\mu_\ell(\tilde{s}_1; H_1) - \tilde{s}_1\mu'_\ell(\tilde{s}_1\,; H_1)\right]}. \end{aligned} \tag{3}$$

où $\mu'_\ell(\tilde{s}_j; H_j)$ et $\mu''_\ell(\tilde{s}_j; H_j)$ représentent respectivement les dérivées premières et secondes de $\mu_\ell(s; H_j)$ à la valeur $\tilde{s}_j$ telle que $\frac{N}{2}\mu'_\ell(\tilde{s}_j; H_j) = \lambda$.

2.3 Processus d'impression-acquisition

Nous proposons d'utiliser dans ces travaux deux familles de distribution pour modéliser le procédé d'impression-acquisition, mais cette méthodologie générale ne dépend pas intrinsèquement du modèle. La première est la distribution Gaussienne Généralisée (GG), elle a été choisie car elle peut modéliser des distributions à la fois denses ou parcimonieuses. La seconde est la distribution lognormale, déjà utilisée dans un contexte d'authentification par codes graphiques par Baras et Cayre [6] car modélisant fidèlement l'impression laser.

La distribution modélisant la chaine d'impression-acquisition, c'est à dire la combinaison de l'imprimante et du scanner, peut s'écrire comme :

- pour la distribution GG :

$$p(v \mid x) = \frac{b}{2a\Gamma(1/b)} e^{-(|v-m(x)|/a)^b}, \tag{4}$$

où $\Gamma(\cdot)$ est la fonction Gamma, $m(x)$ la moyenne et le paramètre a peut être calculé pour une variance donnée $\sigma^2(x) = \mathrm{var}[V \mid x]$ par :

$$a = \sqrt{\sigma(x)\Gamma(1/b)/\Gamma(3/b)}. \tag{5}$$

Le paramètre b permet de contrôler la parcimonie de la distribution, par exemple pour $b = 1$ la distribution est Laplacienne, pour $b = 2$ la distribution est Gaussienne, et pour $b \to +\infty$ la

distribution tend vers la loi uniforme.

- Pour la distribution Lognormale :

$$p(v \mid x) = \frac{1}{vs(x)\sqrt{2\pi}} e^{-\frac{(\log v - m(x))^2}{2s^2(x)}}, \tag{6}$$

ce qui revient à écrire que $\log(V \mid x)$ est une distribution Gaussienne de moyenne $m(x)$ et de variance $s^2(x)$. Le mode de la distribution est $M(x) = e^{m(x)-s^2(x)}$, et la variance est donnée par $\sigma^2(x) = (e^{s^2(x)} - 1)e^{2m(x)+s(x)^2}$.

Afin de fournir des valeurs entre $[0, \ldots, 255]$ reflétant une acquisition en niveaux de gris, les distributions (4) et (6) sont quantifiées puis tronquées. Chaque canal dépend alors de 4 paramètres, deux par types de points (noir ou blanc).

3 Optimisation du canal

Ce problème d'authentification peut être vu comme un jeu où l'objectif de la source légitime est de maximiser les performances d'authentification, ce qui signifie que pour une probabilité de fausse alarme α donnée, elle utilisera le canal qui minimise la probabilité de non-détection β.
D'un point de vue pratique, cela signifie que le canal peut être modifié en choisissant une qualité de papier donnée, une densité d'encre donnée et en utilisant une résolution d'impression donnée. Par exemple si la source légitime cherche à réduire la variance du bruit du processus, elle peut choisir de dupliquer des points, au contraire si elle cherche à augmenter la variance, elle peut utiliser un papier de moins bonne qualité. Il est important de rappeler que puisque l'imprimante doit utiliser des entrées binaires, l'adversaire effectuera de-facto des erreurs de décodage en estimant $\hat{X}$.

Nous analysons deux scénarios décrits ci-dessous :

1) La source légitime et l'adversaire ont des chaines d'impression-acquisition identiques. Dans ce cas précis, la source légitime cherchera le canal $\mathcal{C}$ tel que pour un α donné, le receveur obtiendra une probabilité β^* telle que :

$$\beta^* = \min_{\mathcal{C}} \beta(\alpha). \tag{7}$$

Dans ce cas, l'adversaire sera défini comme passif.

2) Dans un deuxième scénario, l'adversaire peut modifier son canal d'impression-acquisition $\mathcal{C}_o$, ce qui revient à modifier un ou plusieurs paramètres modélisant sa configuration. L'adversaire va donc chercher à maximiser la probabilité de non détection β en choisissant le canal $\mathcal{C}_o$ adéquate alors que la source légitime adoptera le canal $\mathcal{C}_m$ minimisant β. Nous obtenons un jeu min-max où le β^* optimal est la solution de

$$\beta^* = \min_{\mathcal{C}_m} \max_{\mathcal{C}_o} \beta(\alpha). \tag{8}$$

Dans ce cas-ci l'adversaire est actif puisqu'il adapte sa stratégie afin de dégrader les performances d'authentification.

3.1 Résultats

Pour le modèle Gaussien généralisé et le modèle Lognormal, nous supposons que respectivement les moyennes $m(0)$ et $m(1)$ d'une part et les modes $M(0)$ et $M(1)$ d'autre part sont constants (ce qui implique que le procédé d'acquisition a la même calibration pour les deux types de modèles). Nous supposons également que les variances des points noirs et des points blancs sont égales pour chaque canal (respectivement σ_m^2 et σ_o^2 pour le canal de la source légitime et le canal de l'adversaire).

Adversaire passif : Le seul paramètre à trouver pour résoudre l'optimisation (7) est le paramètre σ_m. Les figures 2.a et 2.b représentent respectivement l'évolution de β en fonction de σ_m pour $\alpha = 10^{-6}$ avec $m(0) = 50$, $m(1) = 150$ pour le canal Gaussien, et pour différents modes pour la distribution Lognormale. Nous constatons que pour chaque configuration étudiée, nous pouvons trouver une configuration optimale, et que cette configuration offre une probabilité d'erreur plus faible pour $b = 6$ que pour $b = 2$ ou $b = 1$.

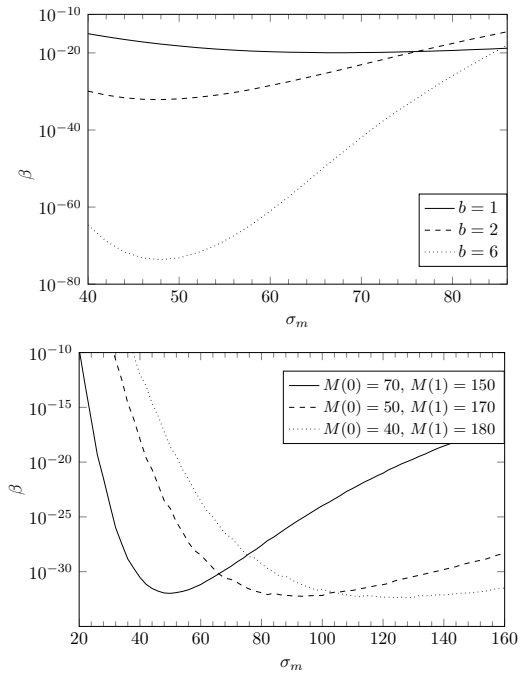

FIGURE 2 – Evolution de la probabilité de non détection en fonction de l'écart type du canal dans le cas d'une GG (haut), et d'une distribution Lognormale (bas). $\alpha = 10^{-6}$.

Adversaire actif : Dans ce scénario, l'adversaire peut choisir sa variance σ_o^2 afin de confondre le receveur en choisissant β maximum. La figure 3.a représente les évolutions de β en fonction de σ_o pour différents σ_m pour un canal Gaussien généralisé. Nous constatons que dans chacun des cas, il est dans l'intérêt de l'adversaire d'optimiser son canal.
Les figures 3.b et 3.c montrent l'évolution de la meilleur stratégie de l'adversaire en fonction de σ_m. En la comparant à la Figure 2, nous constatons que la probabilité de non détection de

l'adversaire peut être multipliée par plusieurs ordres de grandeur pour la distribution GG ($\times 10^6$ pour $b = 1$, $\times 10^5$ pour $b = 2$) et pour la distribution Lognormale ($\times 10^5$ pour chaque mode), mais reste faible lorsque la distribution est proche de l'uniforme ($b = 6$).

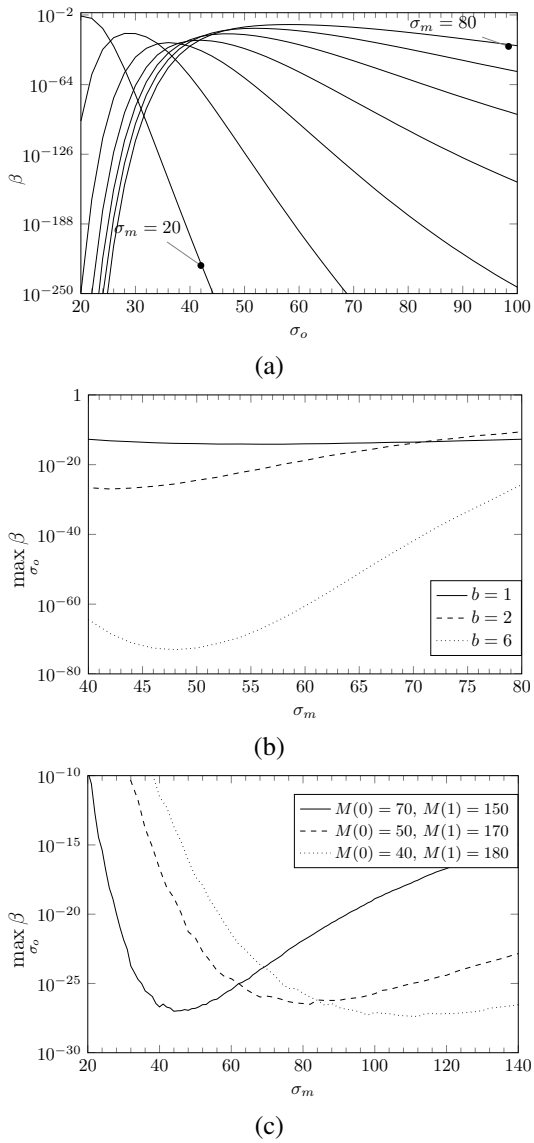

FIGURE 3 – (a) : Evolution de la stratégie de l'adversaire pour la distribution Gaussienne avec un point-selle pour $\sigma_m \approx 30$ et $\sigma_o \approx 40$. (b) et (c) : performance pour l'attaque au pire des cas $\max(\beta)$ par rapport à l'écart type du canal pour une distribution GG (milieu) et Lognormale (bas). $\alpha = 10^{-6}$.

Lorsque l'adversaire est passif, il n'est pas surprenant de constater que dans chacun des cas, β est important lorsque σ_m est faible, i.e. lorsque la chaine d'impression-acquisition est parfaite, car de ce cas l'estimation du code original par l'adversaire est aisée. β est également importante lorsque σ_m est grand, i.e. lorsque la chaine est fortement bruitée, car les codes de la source légitime et de l'adversaire sont ici tous les deux semblables à du bruit. La source légitime devra en conséquence éviter un canal trop, ou trop peu bruité.

Lorsque l'adversaire est actif, le scénario présente un point-selle satisfaisant (8) pour les deux familles de distributions. Cela signifie que même si l'adversaire possède un système d'impression-acquisition parfait, ($\sigma_o \to 0$, $o^N = \hat{x}^N$), ce n'est pas à son avantage de l'utiliser car l'authentification sera possible par simple comparaison entre un code ré-imprimé non-bruité différent du code légitime imprimé y^N.

Nous remarquons également que les paramètres optimaux pour les deux scénarios sont très proches, ce qui veut dire que l'adversaire n'a pas beaucoup de marge de manoeuvre pour choisir son attaque optimale (voir Figures 2 (a) et 3 (b,c)) et pratiquement aucune lorsque la distribution tend vers l'uniforme ($b = 6$). Pour des distributions GG de même variance, les distributions denses permettent d'obtenir des performances plus importantes que les distributions parcimonieuses dans les deux scénarios (voir Figures 2 (a) et 3 (b)).

4 Conclusions

Nous avons proposé de formuler le problème d'authentification par codes binaires d'objets imprimés comme une optimisation entre la source légitime et l'adversaire, chaque acteur essayant de sélectionner le procédé d'impression-acquisition minimisant ou maximisant les performances d'authentification. Ce jeu peut être formulé via l'utilisation de calculs fiables des probabilités d'erreurs, et considérant les canaux comme étant additifs.

Références

[1] T. Haist and H.J. Tiziani. Optical detection of random features for high security applications. *Optics communications*, 147(1-3) :173–179, 1998.

[2] G.E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual Design Automation Conference*, pages 9–14. ACM, 2007.

[3] Justin Picard. Digital authentication with copy-detection patterns. In *Electronic Imaging 2004*, pages 176–183. International Society for Optics and Photonics, 2004.

[4] A-T. Phan Ho, B-A. Hoang Mai, W. Sawaya, and P. Bas. Document Authentication Using Graphical Codes : Impacts of the Channel Model. In *ACM Workshop on Information Hiding and Multimedia Security*, pages ACM 978–1–4503–2081–8/13/06, Montpellier, France, June 2013.

[5] A. Dembo and Z. Ofer. *Large deviations techniques and applications*, volume 38 of *Stochastic Modelling and Applied Probability*. Springer, 2010.

[6] C. Baras and F. Cayre. 2D bar-codes for authentication : A security approach. *Proceedings of EUSIPCO 2012*, 2012.