2D Bar-Codes for Authentication: A Security Approach

Cléo Baras, François Cayre

2D BAR-CODES FOR AUTHENTICATION: A SECURITY APPROACH

Cléo Baras and François Cayre

GIPSA-Lab
Domaine Universitaire, 11 rue des Mathématiques, BP 46
F-38042 St. Martin d'Hères Cedex, France

ABSTRACT

In this paper, we investigate the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and we take the opponent's point of view. The opponent is assumed to have access to N_c noisy copies of a genuine 2D-BC (noise being due to printing and scanning processes). A simple estimator of the 2D-BC based on copies averages is proposed, letting the opponent print a fake 2D-BC which aims at being declared as genuine by the system detector. Performance of the estimator in terms of error probability at the detector side is then derived with respect to N_c and compared with experimental results on real 2D-BC. It is shown that the opponent can produce a fake that successfully fools the detector with a reasonable number of genuine goods.

1. INTRODUCTION

When making sure a real-world good (such as medicine, wine, textile, ...) is genuine [1], 2D bar-codes (2D-BCs) are an alternative to watermarks. 2D-BCs [2] (also called Data Matrix or Data Grid) are black-and-white visible images encoding a good binary identifier using a (secret) cryptographic key in a pseudo-random way and printed on the goods package. Using an automated detection process based on a scan of the 2D-BC, a correlation score is computed and compared to a pre-determined threshold in order to decide whether the good is genuine or fake.

In this context, an opponent (Eve) aims at producing a fake 2D-BCs declared as genuine by the detector, whereas the goal of the product manufacturer (Bob) is to make such a reproduction difficult or impossible for Eve. Bob will therefore use the production process noises all the more severe as the printed 2D-BCs size is small (around 4 millimeters). He might even deliberately add some noise during his 2D-BC printing process to obtain properties similar to Physical Unclonable Functions [3]. Besides, Eve, unaware of the good binary identifier encoding, has no choice but to try to estimate the original 2D-BC without getting to the good identifier.

In this paper, this problem is tackled with a security approach inspired by works in digital watermarking [4]. We investigate the worst case attack framework from Bob's point of view, described in section 2: 1) the opponent has access to N_c printed (genuine) versions of the same 2D-BC (since he might have bought several genuine goods); 2) he has the same printing device than Bob and arbitrary precision scanning device; and 3) he has no access to the automated detector[1]. A simple estimator of the original 2D-BC is proposed in section 3. In section 4, estimator performance are derived with respect to N_c and compared to experimental results, presented in section 5.

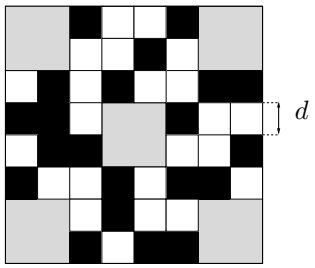

Fig. 1. A 2D-BC with synchronization elements in gray and identification elements over a $\Delta = 255$ dynamic range.

2. PROBLEM STATEMENT

In the sequel, let $\mathcal{M}_L(E)$ denotes the set of square matrices with size $L \times L$ and elements in E.

2.1. 2D-BC construction

After encoding with a secret key, the good binary identifier $\mathbf{b}$ is added to synchronization elements (that won't be taken into account in the sequel) then modulated following an On-and-Off Keying (OOK) modulation with dynamic range Δ (typically $\Delta = 255$). These elements are spread over a matrix $\mathbf{I}_o \in \mathcal{M}_L(\{0, \Delta\})$ forming the black-and-white 2D-BC with $L \times L$ elements equal to 0 or Δ, depicted in figure 1.

This work was supported, in part, by the French ANR Estampille project.

[1] This framework is closely connected to the well-known sensitivity attack in digital watermarking already studied in [5]

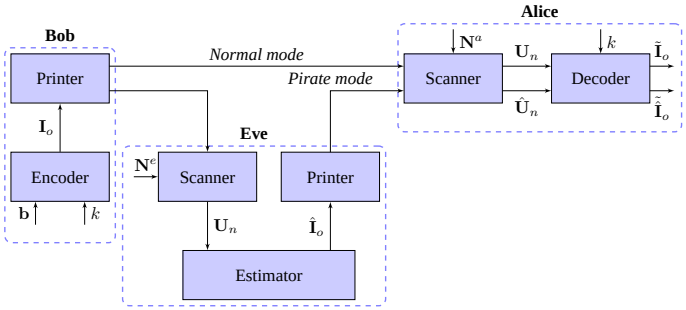

Fig. 2. Description of the authentication system.

2.2. The authentication and counterfeiting processes

Figure 2 gives a brief sketch of our setup. In normal mode, the product manufacturer Bob prints 2D-BCs on goods with a small printing area $d \times d$ (typically d is around 4 millimeters). Then Alice, authorized to use the automated detector, scans them to check whether they are genuine or not. The n-th print and scan operation will be denoted as the function $\mathcal{P}_n$.

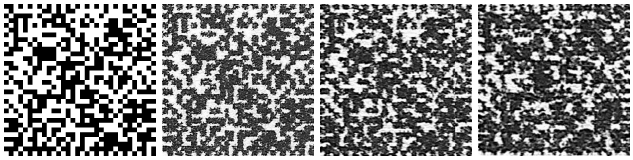

Fig. 3. Acquisition examples of a 2D-BC, printed with a HP PhotoSmart C7200 and scanned at 1200dpi. From left to right: original 2D-BC, $d = 8mm$, $d = 6mm$, $d = 4mm$.

Since print and scan operations occur in the analog realm, distortions on 2D-BC are incurred so that Alice's detector takes a decision on the acquired 2D-BC $\mathbf{U}_n = \mathcal{P}_n(\mathbf{I}_o)$. The reader may have a look at figure 3 to better figure out what kind of artefacts are at stake. Distortions (varying from a print and scan operation to another) include:

- noise $\mathbf{N}_n^a$ due (for instance) to ink dispersion in the paper or inhomogeneous lighting conditions during scan acquisition: the acquired 2D-BC elements $\mathbf{U}_n(i,j)$ are then in the $[0, \Delta]$ range (white and black elements going to gray);

- resampling inherent to the print and scan process and taking into account varying speed of the scanning device during acquisition: each elements of $\mathbf{U}_n$ is spread over a $S \times S$ area , so that $\mathbf{U}_n \in \mathcal{M}_M([0, \Delta])$ with $M = SL$. To put it simply (*hypothesis 1*), $\mathbf{U}_n$ can be viewed as the encoding of $\mathbf{I}_o$ using a repetition code with S repetitions, so that: $\mathbf{U}_n(Si + s, Sj + t) \approx \mathbf{I}_o(i,j)$ with $0 \leq s, t < S$. In practice, S is not necessarily an integer.

Eve, as an opponent having an arbitrary precision scanning device, has access to the N_c 2D-BCs $\mathbf{U}_n$ printed by Bob, each collected with a noise $\mathbf{N}_n^e$. She proceeds to the original 2D-BC estimation, denoted as $\hat{\mathbf{I}}_o \in \mathcal{M}_L(\{0, \Delta\})$, then prints it on fake products. Finally, her fake 2D-BC $\hat{\mathbf{I}}_o$, when submitted to Alice's detector, will suffer print and scan distortions (with noise $\mathbf{N}_n^a$) equivalent to those of $\mathbf{I}_o$ in the normal mode.

2.3. Authentication system performance

Alice's detector will have to decide between the two hypotheses: $\mathcal{H}_f$ when the content is fake and $\mathcal{H}_g$ when the content is genuine. End-to-end performance are related to the well-known false-alarm and false-detection probabilities (resp. p_{fa} and p_{fd}), relying on a decision threshold τ delimiting the boundary between fake and genuine contents. p_{fa} and p_{fd} depend on various parameters (encoding techniques, identifier encryption parameters...) that Eve might be unaware of. Therefore, Eve must be able to reproduce the whole 2D-BC $\mathbf{I}_o$ as accurately as possible, without getting to the original good identifier $\mathbf{b}$. As a consequence, performance can be evaluated with the error probability in the decoding of the original 2D-BC $\mathbf{I}_o$ respectively when Alice scans a genuine 2D-BC emanating from Bob, denoted by $p^d_{e|\mathcal{H}_g}$ then a fake 2D-BC emanating from Eve, denoted by $p^d_{e|\mathcal{H}_f}$ and related to the performance of Eve's estimator.

3. EVE'S ESTIMATOR

3.1. Principles

The N_c 2D-BCs $\mathbf{U}_n$ collected by Eve are realizations of the same original 2D-BC $\mathbf{I}_o$. Eve aims at producing $\hat{\mathbf{I}}_o$ estimating $\mathbf{I}_o$ as accurately as possible. A simple estimation will take two steps: a soft output estimation $\hat{\mathbf{I}}_n(i,j)$ of the element value $\mathbf{I}_o(i,j)$ in each of Eve's N_c 2D-BCs using the repetition code; then the combination of these soft values over the N_c contents to produce a hard decision on the 2D-BC element value $\mathbf{I}_o(i,j)$, yielding the fake $\hat{\mathbf{I}}_o$.

Our estimator relies on the hypothesis (*hyp. 2*) that no black element of a 2D-BC should spread more than the half of the surrounding elements as illustrated in figure 4. Indeed, if this hypothesis is violated, then even Alice may well not be able to correctly authenticate the 2D-BC.

3.2. A sliding window estimator

3.2.1. Soft output estimation

The soft output estimation $\hat{\mathbf{I}}_n(i,j)$ of the 2D-BC element $\mathbf{I}_o(i,j)$ (that is spread in $\mathbf{U}_n$ with size of $S \times S$) works as follows: in relation with the hypothesis of section 3.1, a sliding window of size $S/2$ circulates across the $S \times S$ elements $\mathbf{U}_n(Si + s, Sj + t)$ (with s and t varying in $[0; S - 1]$).

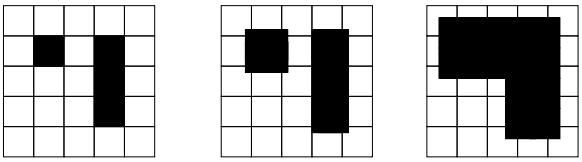

Fig. 4. Left: original 2D-BC elements, to be printed & scanned. Center: printed & scanned elements, respecting our hypothesis. Right: printed & scanned elements that do not respect our hypothesis.

Then, taking the mean value of $\mathbf{U}_n$ at window position $(Si + S/2, Sj + S/2)$ yields:

$$\hat{\mathbf{I}}_n(i,j) = \frac{1}{S^2} \sum_{s=0}^{S-1} \sum_{t=0}^{S-1} \mathbf{U}_n(Si+s, Sj+t). \quad (1)$$

3.2.2. Hard decision

Combining the soft output decisions among the N_c 2D-BCs at element position (i,j) is done by computing the average value of the elements $\hat{\mathbf{I}}_n(i,j)$ over the N_c soft output estimations:

$$\mathbf{W}(i,j) = \frac{1}{N_c} \sum_{n=1}^{N_c} \hat{\mathbf{I}}_n(i,j). \quad (2)$$

Eve's final estimated 2D-BC $\hat{\mathbf{I}}_o$ is then obtained with:

$$\hat{\mathbf{I}}_o(i,j) = \begin{cases} \Delta & \text{if } \mathbf{W}(i,j) \leq \Delta/2 \\ 0 & \text{otherwise} \end{cases}. \quad (3)$$

4. A THEORETICAL STUDY OF THE COUNTERFEITING SCENARIO

In this section, we aim at deriving the decoding performances for both normal and pirate modes of operation, that is the respective error probabilities $p^d_{e|\mathcal{H}_g}$ and $p^d_{e|\mathcal{H}_f}$, related to the print and scan distortions and to the performance of Eve's estimator. For simplicity reasons, we will assume that 0's and Δ's are equiprobably distributed in $\mathbf{I}_o$ (*hyp. 3*).

4.1. A naive print and scan model

In view of a theoretical study, the n-th printing and scanning process $\mathcal{P}_n$ can be modeled for the 2D-BC element (i,j) using:

- a noise $\mathbf{N}$: The print and scan noises in the normal mode with Bob and Alice can be viewed as a single accumulated noise $\mathbf{N}^a_n$. Statistical properties of $\mathbf{N}^a_n$ are supposed to be independent from both n and the 2D-BC element (i,j) (*hyp. 4*). Moreover, it can be assumed that Eve has access to the same printing and scanning devices as those used in the normal mode of operation (*hyp. 5*) ; thus statistical properties of $\mathbf{N}^e$ are equal to those of $\mathbf{N}^a$. Both will be denoted as $\mathbf{N}$ and supposed to follow a $\mathcal{N}(0, \sigma^2_{\mathbf{N}})$ distribution (*hyp. 6*);
- a shift parameter α: according to figure 3, the whole process tends to move extremal values 0 and Δ towards $\Delta/2$, making the channel all the more error-prone as the noise level increases. This degradation will be modeled by a shift of extremal levels with a parameter α (*hyp. 7*).

Finally, the acquired 2D-BC $\mathbf{U}_n = \mathcal{P}_n(\mathbf{I}_o)$ is given, for all $0 \leq s,t < S$, by:

$$\begin{aligned} \mathbf{U}_n(Si+s, Sj+t) = \; & \mathbf{I}_o(i,j) + \mathbf{N}(Si+s, Sj+t) \\ & + \begin{cases} \alpha & \text{if } \mathbf{I}_o(i,j) = 0 \\ -\alpha & \text{if } \mathbf{I}_o(i,j) = \Delta \end{cases}. \end{aligned} \quad (4)$$

4.2. Decoding error probability in the normal mode ($\mathcal{H}_g$)

Let the decoder operating on $\mathbf{U}_n = \mathcal{P}_n(\mathbf{I}_o)$ with $\mathbf{I}_o$ emanating from Bob. Due to the model symmetries, the decoding error probability is the probability that the decoded $\tilde{\mathbf{I}}_o(i,j)$ is Δ whereas the original 2D-BC element is $\mathbf{I}_o(i,j) = 0$, that is $p^d_{e|\mathcal{H}_g} = \mathbf{Pr}\left[\mathbf{I}_n(i,j) = \Delta | \mathbf{I}_o(i,j) = 0\right]$.

Alice's detector is assumed to work the same way than Eve's estimator but using the single content $\mathbf{U}_n$ (*hyp. 8*): regarding the 2D-BC element $\mathbf{I}_o(i,j) = 0$, the S^2 observations $\mathbf{U}_n(Si+s, Sj+t)$ are $\mathcal{N}(\alpha, \sigma^2_{\mathbf{N}})$ distributed according to equation (4). Then, the soft estimated value $\tilde{\mathbf{I}}_n(i,j)$ (computed by Alice's detector with equation (1)) follows a $\mathcal{N}(\alpha, \frac{\sigma^2_{\mathbf{N}}}{S^2})$ model. Then, the hard decision on $\tilde{\mathbf{I}}_o(i,j)$ (using $N_c = 1$ in equation (3)) yields:

$$p^d_{e|\mathcal{H}_g} = \mathbf{Pr}\left[\tilde{\mathbf{I}}_n(i,j) > \tfrac{\Delta}{2} | \mathbf{I}_o(i,j) = 0\right] = \frac{1}{2}\text{erfc}\left(\frac{\frac{\Delta}{2} - \alpha}{\sqrt{2}\frac{\sigma_{\mathbf{N}}}{S}}\right) \quad (5)$$

with erfc the complementary error function.

4.3. Decoding error probability in the pirate mode (under $\mathcal{H}_f$)

4.3.1. Estimator performance

We are now interested in Eve's ability to correctly estimate $\mathbf{I}_o$ with respect to the number N_c of printed and scanned versions $\mathbf{U}_n$ she collects, that is the error probability of the estimator $p^e_e(N_c)$, comparing $\hat{\mathbf{I}}_o$ and $\mathbf{I}_o$. Under the same hypotheses than previously, $p^e_e(N_c) = \mathbf{Pr}\left[\hat{\mathbf{I}}_o(i,j) = \Delta | \mathbf{I}_o(i,j) = 0\right]$.

Regarding the 2D-BC element (i,j) when $\mathbf{I}_o(i,j) = 0$, the related S observations $\mathbf{U}_n(Si+s, Sj+t)$ in the n-th collected 2D-BC still follows a $\mathcal{N}(\alpha, \sigma^2_{\mathbf{N}})$ distribution ; thus the soft estimated value $\hat{\mathbf{I}}_n(i,j)$ is still $\mathcal{N}\left(\alpha, \frac{\sigma^2_{\mathbf{N}}}{S^2}\right)$ distributed.

Now, the averaged value $\mathbf{W}(i,j)$ over the N_c values $\hat{\mathbf{I}}_n(i,j)$ follows $\mathcal{N}\left(\alpha, \frac{\sigma_{\mathbf{N}}^2}{S^2 N_c}\right)$, so that the hard decision on $\hat{\mathbf{I}}_o$ yields:

$$p_e^e(N_c) = \mathbf{Pr}\left[\mathbf{W}(i,j) > \tfrac{\Delta}{2} | \mathbf{I}_o(i,j) = 0\right] = \frac{1}{2}\text{erfc}\left(\frac{\frac{\Delta}{2} - \alpha}{\frac{\sqrt{2}\sigma_{\mathbf{N}}}{S\sqrt{N_c}}}\right) \quad (6)$$

4.3.2. *Decoding error probability under $\mathcal{H}_f$*

Alice is now scanning the Eve's fake content $\hat{\mathbf{I}}_o$. The observed 2D-BC $\hat{\mathbf{U}}_n = \mathcal{P}_n(\hat{\mathbf{I}}_o)$ (after print and scan) is subject to the same decoding process as described in section. 4.2. The decoding error probability under $\mathcal{H}_f$ is then the probability that the decoded value $\tilde{\hat{\mathbf{I}}}_o(i,j)$ is Δ whereas the genuine information in $\mathbf{I}_o(i,j)$ is 0. Thus: $p_{e|\mathcal{H}_f}^d = \mathbf{Pr}\left[\tilde{\hat{\mathbf{I}}}_o(i,j) = \Delta | \mathbf{I}_o(i,j) = 0\right]$.

Taking into account 1) the estimated 2D-BC $\hat{\mathbf{I}}_o$, 2) the estimator errors and 3) the symetrical configurations regarding value 0 and Δ, it comes (omitting the indexes (i,j) to ease the reading):

$$\begin{aligned} p_{e|\mathcal{H}_f}^d = \quad & \mathbf{Pr}\left[\tilde{\hat{\mathbf{I}}}_o = \Delta | \hat{\mathbf{I}}_o = \Delta, \mathbf{I}_o = 0\right] \mathbf{Pr}\left[\hat{\mathbf{I}}_o = \Delta | \mathbf{I}_o = 0\right] \\ & + \mathbf{Pr}\left[\tilde{\hat{\mathbf{I}}}_o = \Delta | \hat{\mathbf{I}}_o = 0, \mathbf{I}_o = 0\right] \mathbf{Pr}\left[\hat{\mathbf{I}}_o = \Delta | \mathbf{I}_o = 0\right] \end{aligned} \quad (7)$$

$\mathbf{Pr}\left[\tilde{\hat{\mathbf{I}}}_o = \Delta | \hat{\mathbf{I}}_o = 0, \mathbf{I}_o = 0\right]$ is independent of the genuine 2D-BC and is directly linked to the error probability of the decoder when the submitted content, that is $\hat{\mathbf{I}}_o$, is corrupted by a single printing and scanning operation ; thus it is equal to $p_{e|\mathcal{H}_g}^d$. Moreover, $\mathbf{Pr}\left[\tilde{\hat{\mathbf{I}}}_o = \Delta | \hat{\mathbf{I}}_o = 0, \mathbf{I}_o = 0\right] = (1 - p_{e|\mathcal{H}_g}^d)$. Finally,

$$p_{e|\mathcal{H}_f}^d = 1 - [1 - p_e^e(N_c)]\, p_{e|\mathcal{H}_g}^d + p_e^e(N_c)\left[1 - p_{e|\mathcal{H}_g}^d\right]. \quad (8)$$

It can be noticed that $p_{e|\mathcal{H}_f}^d$ is entirely given by $p_e^e(N_c)$ since $p_{e|\mathcal{H}_g}^d = p_e^e(1)$.

5. RESULTS

5.1. Results using the proposed theoretical model

Figure 5 depicts Eve's increasing performance in estimating the original 2D-BC when she accumulates several printed and scanned versions of it. Estimator theoretical performances of equation (6) are validated through Bit Error Rate (BER) with Monte-Carlo simulations using 2D-BCs containing 10kbits of information. Moreover, the print and scan channel is modeled using fixed parameters (α and $\sigma_{\mathbf{N}}^2$).

In figure 6, we plot, as a function of the number of 2D-BCs Eve has used, the probability of error at the decoder side when a fake is submitted to the system (cf. equation 8).

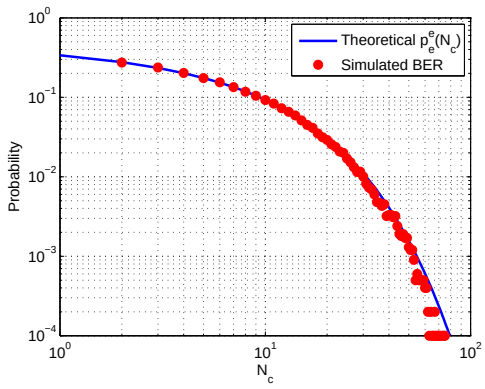

Fig. 5. Error probability of the estimator on the basis of theoretical equation (6) and evaluated with BER through simulations. Parameters: $\alpha = 50$, $\sigma_{\mathbf{N}}^2 = 0,3$, $\Delta = 1$, $S = 4$.

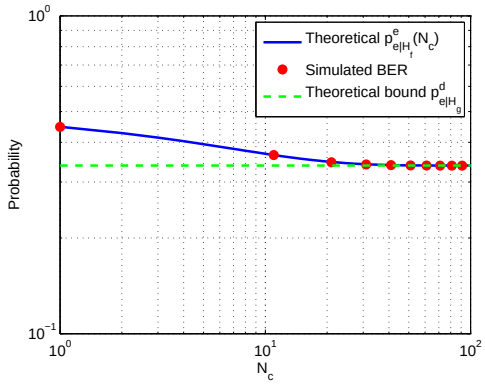

Fig. 6. Decoding error probability using fake contents on the basis of theoretical equation (8) and evaluated with BER through simulation, compared to the decoding error probability using genuine contents (equation (5)). Parameters: $\alpha = 50$, $\sigma_{\mathbf{N}}^2 = 0,3$, $\Delta = 1$, $S = 4$.

Simulated BERs confirm the accuracy of equation 8. It also shows that when the number of collected contents N_c increases, $p_{e|\mathcal{H}_f}^d$ tends to $p_{e|\mathcal{H}_g}^d$ *i.e.* Alice's decoder performance in normal mode. This means that, the fake and the genuine 2D-BCs can no longer be distinguished at the decoder side, since the messages obtained after decoding have the same number of error.

5.2. Results using real 2D-BC

In this section, we use real 2D-BCs, as depicted in figure 3. They contain a realistic amount of information (1kbit) and they were printed and scanned on a HP PhotoSmart C7200.

In figure 7, we accumulate a varying number of scanned 2D-BCs to estimate the original. We are then able to compute the BER to assess the raw estimator performance. Clearly as

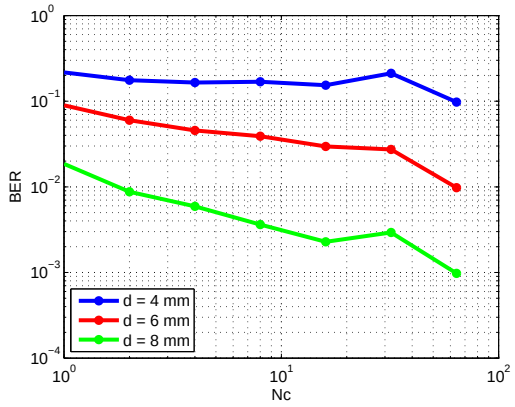

Fig. 7. Estimator performance with real 2D-BC through the estimation of $p^d_{e|\mathcal{H}_f}$ for 3 printing dimensions: $d \in \{4, 6, 8\}$ mm. All 2D-BCs contain 1024 bits and were printed and scanned on a HP PhotoSmart C7200 (scan resolution: 1200dpi).

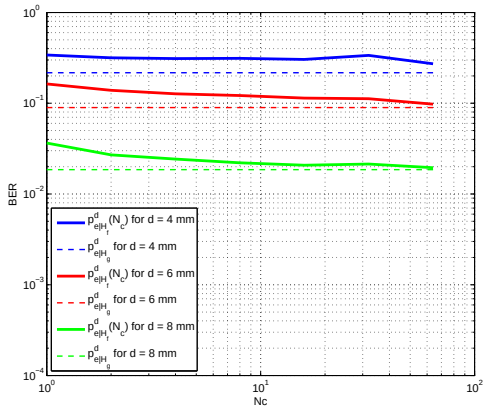

Fig. 8. Overall fake generation performance. When increasing N_c, Eve can ultimately reach Alice's decoder bound on authentic 2D-BCs (dashed lines): a fake can produce the same amount of errors as an authentic 2D-BC, which is good enough for Eve's goal.

expected with theoretical results, Eve can refine her estimation as she has access to more and more 2D-BCs. But the slope of the plots have few in common with these of figure 5 since the print and scan channel model is far from reality.

Plugging the data of the figure 7 into equation 8 (which is independent from the channel model), we can plot the overall fake performance Eve can actually achieve (taking into account errors she might make but compensated by Alice's own errors). The results are given figure 8 where we also plot the bound on Alice's detector (that is the normal mode performance). As expected, the error decoding probability with fake 2D-BC tends to the one for genuine 2D-BC when the number of collected 2D-BC used in Eve's estimated 2D-BC increases; but the number of required contents is greater than expected (with theoretical results).

However, it can be noticed that Eve's goal may not be to estimate perfectly the original 2D-BC. Rather, she might be just as satisfied when she knows Alice's detector will make the same amount of errors given an authentic or a fake 2D-BC. For a bad printing quality, Eve will need a much greater amount of 2D-BCs to achieve Alice's detector bound. However, as the printing quality increases, a fake quickly leads to the same amount of errors as an authentic 2D-BC at Alice's detector side.

6. CONCLUSION

In this paper, we consider a good authentication system using 2D-BCs from the point of view of the opponent. An estimator that he can use to product a fake was proposed and its performance was derived through theoretical results and simulations on real printed and scanned 2D-BCs.

While both the model and the tests conducted on real data agree on the general conclusion that Eve's estimation performance increases when collecting 2D-BCs, the slope of the curves, however, differs greatly. We believe this is due to the fact that our printing and scanning channel model is rather poor.

Future works have two directions: first, improving the opponent estimation ability using for instance (possibly geometrical) channel equalization or a 2D extension of the Viterbi decoder by solving the problem of the complexity of the aforementioned decoder and second, elaborating the product manufacturer counterattack, that is adapting an additional noise to his printing process to efficiently disturb the opponent estimation.

7. REFERENCES

[1] J.-M. Bobee, "How technology can help to fight counterfeits?," *STP Pharma Pratiques*, vol. 19, no. 1, 2009.

[2] J. Picard, "Digital authentication with copy-detection patterns," in *Proc. IS&T Optical Security and Counterfeit Deterrence Techniques V*, 2004, pp. 176–183.

[3] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," in *Science*, september 2002, pp. 2026–2030.

[4] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," in *IEEE Trans. Signal Processing*, 2005, vol. 53, pp. 3976–3987.

[5] P. Comesana, L. Perez-Freire, and F. Perez-Gonzalez, "Blind newton sensitivity attack," *IEEE Proceedings of Information Security*, vol. 153, no. 3, pp. 115 – 125, 2006.