Fig. 1 shows the average PSNR of the Y (luminance) component of the sequence Mobile & Calendar as a function of the switch load when the switch rate was set to 24Mbit/s. Every curve refers to a different coding strategy (MPEG-2 standard, T_{AC} = 2, 4, 8), and transmission (either one or both video layers).

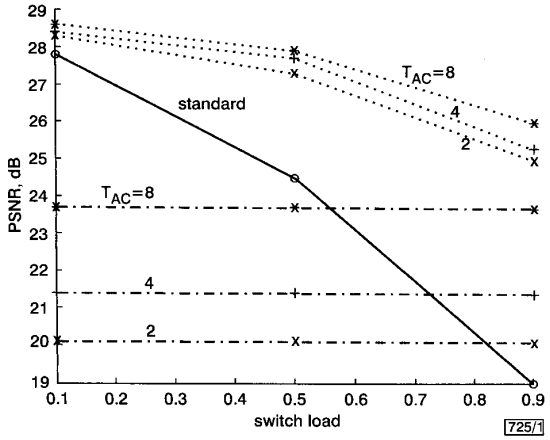

Fig. 1 *Average PSNR of Mobile & Calendar against switch load for double-layer ADP standard MPEG-2 and single-layer ADP*

——— standard MPEG-2
–·–·–· single-layer ADP
····· double-layer ADP

The corresponding cell loss probabilities, for high and low priority cells, are reported in Table 1 for three the switch load values (0.1, 0.5, 0.9) and different coding strategies.

Table 1: Cell loss probability (CLP) for high and low priority cells, for three switch load values (0.1, 0.5, 0.9) and different coding strategies

	High priority cells			Low priority cells		
Load	0.1	0.5	0.9	0.1	0.5	0.9
Standard MPEG-2	0.35×10^{-3}	1.85×10^{-3}	3.1×10^{-3}	0.86×10^{-3}	3.6×10^{-3}	8.1×10^{-3}
Two-layer ADP, $T_{AC}=8$	0	0.27×10^{-3}	0.57×10^{-3}	1.8×10^{-3}	6.2×10^{-3}	1.1×10^{-3}
Two-layer ADP, $T_{AC}=4$	0	0.10×10^{-3}	0.42×10^{-3}	1.3×10^{-3}	5.3×10^{-3}	8.3×10^{-3}
Two-layer ADP, $T_{AC}=2$	0	0.02×10^{-3}	0.19×10^{-3}	1.1×10^{-3}	4.1×10^{-3}	5.9×10^{-3}
One-layer ADP, any T_{AC}	0	0	0	0	0	0

Fig. 1 proves the superiority of the two-layer ADP scheme, especially for high switch load values. The transmission of a single layer can provide good results for load values higher than 0.5. As an example, for critical load conditions (switch load = 0.9) if a single layer with T_{AC} = 8 is transmitted with a switch rate of 24Mbit/s (dotted lines in Fig. 1), sufficient video quality can be obtained (PSNR ≃ 24dB instead of PSNR ≃ 19dB for standard MPEG-2). Also, transmission strategies with T_{AC} = 4 and T_{AC} = 2 outperform standard MPEG-2 for switch loads greater than 0.72 and 0.83, respectively, even if with relatively poor video quality. Moreover, at 24Mbit/s, single-layer ADP provides CLP = 0 both for high and low priority cells and for any value of T_{AC} and switch load (Table 1). Obviously, the absence of cell loss at 24Mbit/s allows the quality of transmission for possible non-video traffic components to be improved.

The same consideration is valid and more evident for lower switch rate values. Extensive experimental results concerning throughput show that the switch behaviour is completely independent of the different transmission strategies supported by the layered video coding based on the ADP scheme. For simpler video sequences, e.g. Tennis Table, the standard MPEG-2 outperforms all one-layer approaches but it performs worse with respect to all two-layer coding strategies. This is due both to the simple motion characteristics of Tennis Table, and to the efficient data partition between high and low priority cells.

Conclusion: Our experimental results prove that the two-layer ADP scheme improves the PSNR of the received video sequence up to 7dB in the presence of packet losses during ATM transmission. Moreover, since the ADP strategy can adapt to the actual network traffic conditions, it is capable of efficiently transmitting video and, more generally, multimedia signals over ATM networks.

21 June 2000
Electronics Letters Online No: 20001211
DOI: 10.1049/el:20001211

A. Garzelli (*DII Dipartimento di Ingegneria dell'Informazione, University of Siena, Via Roma 56, I-53100 Siena, Italy*)

E-mail: andrea.garzelli@dii.unisi.it

References

1 GHANBARI, M.: 'Two-layer coding of video signals for VBR networks', *IEEE J. Sel. Areas Commun.*, 1989, **7**, pp. 771–781
2 GHANBARI, M., and SEFERIDIS, V.: 'Efficient H.261-based two-layer video coded for ATM networks', *IEEE Trans. Circuits Syst. Video Technol.*, 1995, **5**, pp. 171–175
3 SUN, H., KWOK, W., and ZDEPSKI, J.W.: 'Architectures for MPEG compressed bitstream scaling', *IEEE Trans. Circuits Syst. Video Technol.*, 1996, **6**, pp. 191–199
4 ARAVIND, R., CIVANLAR, M.R., and REIBMAN, A.R.: 'Packet loss resilience of MPEG-2 scalable video coding algorithms', *IEEE Trans. Circuits Syst. Video Technol.*, 1996, **6**, pp. 426–435

Short collusion-secure fingerprints based on dual binary Hamming codes

J. Domingo-Ferrer and J. Herrera-Joancomartí

Electronic copyright protection is increasingly dependent on fingerprinting and watermarking techniques. The properties of dual binary Hamming codes are exploited to obtain a fingerprinting scheme secure against collusion of two buyers. The advantage over previous proposals is that collusion security is obtained using well-known and shorter length error correcting codes.

The recent failure of the DVD copy prevention system [1] is just another argument supporting the idea that electronic copyright protection should rather rely on copy detection techniques [2, 3]. The merchant M selling the piece of information (e.g. image) embeds a mark in the copy sold. There are two basic kinds of mark: watermarks and fingerprints. A watermark is an embedded copyright message, whereas one may think of a fingerprint as an embedded copyright message (i.e. something identifying the buyer of the copy).

Whilst buyer collusion is not an issue in watermarking (the marked copies being the same for all buyers), it is a real threat to fingerprinting. Since in fingerprinting the mark is different for every buyer, it makes sense for a set of buyers to collude by comparing their copies and try to locate and delete some mark bits.

In a collusion, two or more different buyers can detect the mark bits by comparison of their copies of the same information item (marking assumption, [4, 5]). After detection, there are two attacking strategies:

Mark bit deletion: The mark bits that differ between buyers are deleted. At mark reconstruction time, M knows where mark bits should be, so he will try to restore deleted mark bits. The probability of correctly restoring a deleted mark bit is 1/2.

Mark bit tweaking: Colluders mix their marked copies in an attempt to tweak some mark bits. This attack is worse than deletion, as M has no way to detect that the bit was tweaked.

Encoding the mark using an error-correcting code (ECC) prior to embedding is an obvious alternative to increase robustness against mark bit deletion and tweaking. However, if the number of bits tweaked (or incorrectly restored from deletion) is greater than the maximum number of errors that the ECC can correct, then mark reconstruction will fail.

In [4, 5], collusion-secure fingerprinting was introduced. Rather than using standard ECCS, a new type of codes called c-secure codes were introduced in that proposal to resist collusions of up to c buyers. With N possible buyers, a code with length $O(N^3 \log N/\varepsilon)$ is needed to be able to identify a member of a c-collusion with probability at least $1 - \varepsilon$. For the case $c = O(\log N)$, the authors propose composition of two codes to reduce to a codeword length $\log^{O(1)}(N)$.

In this Letter, we will show that collusion security for $c = 2$ buyers can be achieved using dual binary Hamming codes, which are well known and have a shorter wordlength than c-secure codes. Part of the ideas below were informally discussed in [6] for the special case of image protection. For N buyers, the codeword length of our proposal is only N and the same technique described in [4, 5] can be used to reduce to length $\log^{O(1)}(N)$. Given the danger inherent to piracy, the size of collusions tends to be small, so achieving protection against collusions of size two is not pointless.

The effectiveness of a two-buyer collusion depends on the distance between codewords of the ECC used in the mark embedding algorithm. The larger the distance, the more bits will differ between the codewords of colluders, i.e. the easier to tweak a codeword bit. On the other hand, the smaller the distance, the less error-correcting capacity will be obtained from the ECC. Dual binary Hamming codes offer a good tradeoff, because the distance between any two codewords is fixed to half their length. More precisely, a dual binary Hamming code of length $N = 2^n - 1$ consists of N codewords a^1, a^2, ..., a^N (excluding the all-zero codeword) such that the distance $d(a^i, a^k)$ between any two different codewords a^i, a^k is 2^{n-1}. The copy of the ith buyer will be fingerprinted using the word πa^i, where π is a random permutation of the codeword bits. The same π is used for all buyers and is kept hidden from them; use of this permutation was proposed in [4, 5] to prevent a coalition to know which mark bit encodes which bit in the code.

For simplicity, in what follows we will focus on the codeword that identifies a specific buyer once the ECC has been applied. The subsequent permutation to obtain the actual fingerprint is not relevant for our discussion, because it is the same for all buyers. The ECC used will be a dual binary Hamming code H with length $2^n - 1$. The distance between any two codewords in H is then 2^{n-1}, so that up to $2^{n-2} - 1$ errors can be corrected. The following definition introduces some useful notation.

Definition (i): Let a^1, ..., a^c be c codewords of length N (i.e. $a^j = a_1^j a_2^j \cdots a_N^j$). The ith position of the set of codewords a^1, ..., a^c is called invariant position if

$$a_i^j = a_i^k \quad \forall j, k = 1, ..., c$$

We denote by $ivt(a^1, ..., a^c)$ the set of invariant positions of a^1, ..., a^c. Also, we denote by $<a^1, ..., a^c>$ the set of words that can be generated by taking as the first bit one of $a_1{}^1$, ..., $a_1{}^c$, as the second bit one of $a_2{}^1$, ..., $a_2{}^c$ and so on.

For collusions of any size c, the following lemma holds.

Lemma (i): Colluders owning a^1, ..., a^c cannot tweak the bits at positions in $ivt(a^1, ..., a^c)$.

Proof of Lemma (i): According to the marking assumption [4, 5], colluders can tweak a bit only if such a bit differs in their copies. Since bits at invariant positions have all the same value, they cannot be changed.

The following properties of dual binary Hamming codes are stated for later use.

Proposition (i): Let H be a dual binary Hamming code with length $2^n - 1$. Then any three codewords of H have exactly $2^{n-2} - 1$ invariant positions.

Proof of Proposition (i): Let $x, y \in H$ be any pair of codewords. Define $I = ivt(x, y)$ and $\bar{I}$ the positions not in I. We denote by $x_{|I}$ the bits of the word x in the positions in I. Since $d(x, y) = 2^{n-1}$ it follows that $ivt(x, y) = 2^{n-1} - 1$.

By construction, we will prove that given any codeword $z \in H$ and a value $k \leq 2^{n-1} - 1$, if $|ivt(x, y, z)| = k$ then $k = 2^{n-2} - 1$. We have

$$d(x_{|I}, z_{|I}) = d(y_{|I}, z_{|I}) = 2^{n-1} - 1 - k$$

since $x_{|I} = y_{|I}$. Now, x, y and z belong to a dual binary Hamming code with length $2^n - 1$, so $d(x, z) = d(y, z) = 2^{n-1}$; therefore

$$d(x_{|\bar{I}}, z_{|\bar{I}}) = d(y_{|\bar{I}}, z_{|\bar{I}}) = 2^{n-1} - (2^{n-1} - 1 - k) = k + 1$$

But $d(x_{|\bar{I}}, y_{|\bar{I}}) = 2^{n-1}$, so that the only possibility is

$$k + 1 = \frac{2^{n-1}}{2}$$

Otherwise, we would have

$$d(x_{|\bar{I}}, z_{|\bar{I}}) \neq d(y_{|\bar{I}}, z_{|\bar{I}})$$

since if $x_i \neq y_i$ then $z_i = y_i \Rightarrow z_i \neq x_i$ as we work in a binary domain (x_i denotes the ith bit of x). Then

$$k = 2^{n-2} - 1$$

Proposition (ii): Let $x, y \in H$. If $z \in <x, y>\backslash\{x, y\}$, then the correction of z using H cannot yield a codeword different from x and y.

Proof of Propostion (ii): Assume that $z \in <x, y>$ exists such that it decodes into a $z' \in H\backslash\{x, y\}$. Since the code H corrects up to $2^{n-2} - 1$ errors, candidates to be z are words with $\leq 2^{n-2} - 1$ errors. But $|ivt(x, y)| = 2^{n-1} - 1$ and $|ivt(x, y, z)| = 2^{n-2} - 1$, so z has at least $(2^{n-1} - 1) - (2^{n-2} - 1) = 2^{n-2}$ errors, which is more than $2^{n-2} - 1$ (the error-correcting capacity of H).

Proposition (iii): Let $x, y \in H$. The probability of obtaining a word $z \in <x, y> \backslash H$ such that z does not uniquely decode into a codeword of H is

$$\epsilon \leq \left(\frac{1}{2}\right)^{2^{n-1}} \cdot 2^n \qquad (1)$$

Proof of Proposition (iii): The only way that z does not uniquely decode is that it contains exactly 2^{n-2} errors.

By Proposition (i), $|ivt(x, y, z)| = 2^{n-2} - 1$. So, from the $2^{n-1} - 1$ invariant positions of x and y, only $2^{n-2} - 1$ correct values will remain in the new word z and thus $(2^{n-1} - 1) - (2^{n-2} - 1) = 2^{n-2}$ will be errors.

Thus, the total amount of errors in z must be in $I = ivt(x, y)$, so $z_{|\bar{I}}$ has to be exactly equal to the corresponding part of a correct codeword in $<x_{|\bar{I}}, y_{|\bar{I}}>$. The probability of this event for a particular codeword is

$$\left(\frac{1}{2}\right)^{2^{n-1}}$$

because $d(x_{|\bar{I}}, y_{|\bar{I}}) = |\bar{I}| = 2^{n-1}$ so that in every position there is exactly one 1 and one 0. Since the total number of codewords in a dual binary Hamming code is 2^n the probability of non-unique decoding is

$$\epsilon \leq \left(\frac{1}{2}\right)^{2^{n-1}} \cdot 2^n$$

We are now in a position to state the main theorem of this Letter. In the vocabulary of [4, 5], the theorem below says that dual binary Hamming codes are 2-frameproof and 2-secure with ε-error. As discussed above, the codeword length is shorter than for c-secure codes.

Theorem (i): If the information to be embedded is encoded using a dual binary Hamming code H of length $N = 2^n - 1$ prior to embedding, then the resulting fingerprinting scheme is secure against collusions of two buyers. An innocent buyer will never be declared guilty (2-frameproofness) and the probability that a participant in a two-buyer collusion can be identified can be made arbitrarily close to 1 (2-security with ε-error).

Proof of Theorem (i): This follows from Propositions (ii) and (iii). Proposition (ii) guarantees that an innocent buyer will never be declared guilty. The probability of identifying one of two colluders is $1 - \varepsilon$, where ε is defined in eqn. 1; as n increases, $1 - \varepsilon$ tends to 1.

Acknowledgment: This work is partly funded by the Spanish CICYT under contract no. TEL98-0699-C02-02.

14 July 2000
Electronics Letters Online No: 20001231
DOI: 10.1049/el:20001231

J. Domingo-Ferrer and J. Herrera-Joancomartí (*Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, ETSE-Autovia de Salou, s/n, E-43006 Tarragona, Catalonia, Spain*)

E-mail: jdomingo@etse.urv.es

References

1 http://www.lemuria.org/DeCSS

2 PETITCOLAS, F.A.P., ANDERSON, R.J., and KUHN, M.G.: 'Attacks on copyright marking systems'. 2nd Int. Workshop Information Hiding, 1998, (Springer-Verlag), Paper LNCS 1525, pp. 219–239

3 PETITCOLAS, F.A.P., ANDERSON, R.J., and KUHN, M.G.: 'Information hiding - a survey', *Proc. IEEE*, 1999, **87**, (7), pp. 1062–1078

4 BONEH, D., and SHAW, J.: 'Collusion-secure fingerprinting for digital data'. Advances in Cryptology- CRYPTO '95, 1995, (Springer-Verlag), Paper LNCS 963, pp. 452–465

5 BONEH, D., and SHAW, J.: 'Collusion-secure fingerprinting for digital data', *IEEE Trans. Inf. Theory*, 1998, **IT-44**, (5), pp. 1897–1905

6 DOMINGO-FERRER, J., and HERRERA-JOANCOMARTÍ, J.: 'Simple collusion-secure fingerprinting schemes for images'. Int. Conf. Information Technology: Coding and Computing - ITCC'2000, IEEE Computer Society, 2000, pp. 128–132

Analytic model of parasitic capacitance attenuation in CMOS devices with hyper-thin oxides

K. Ahmed, E. Ibok and J. Hauser

The parasitic accumulation capacitance attenuation in MOS structures with hyper-thin oxides has been modelled using a distributed RC network. The simple analytic model is in excellent agreement with a two-dimensional numerical simulation and experimental data.

Introduction: Oxides thinner than 20Å have been used as gate dielectrics to fabricate sub-100nm CMOS devices [1, 2]. Estimation of the insulator thickness is essential for the characterisation of these devices. A simple and accurate estimate of t_{ox} can be provided by proper analysis of C-V characteristics in strong accumulation. However, for oxides thinner than 20Å a large direct tunnelling current flows between the gate electrode and silicon substrate [3] and introduces capacitance attenuation in both inversion and accumulation [4 – 7]. The attenuation is a strong function of parasitic series resistance (*Rs*). The value of *Rs* depends on the layout of the capacitor as well as on the contact and sheet resistivity (*SR*) of polysilicon gate and substrate. A typical test structure is shown in Fig. 1. The n^+ regions are used to supply minority carrier to the channel in strong inversion. An ohmic contact to the substrate is provided by the p^+ regions. In inversion capacitance attenuation is believed to be due to the resistance of the inversion layer [4], the source-drain resistance, or the sheet resistivity (*SR*) of the (silicided) polysilcon gate [6]. For the structure shown in Fig. 1, capacitance attenuation in accumulation is believed to be due to the *SR* of the accumulation layer and the contact resistance at the p^+ regions. The contribution of *SR* of the channel to capacitance attenuation becomes larger as the channel length increases for the structure shown in Fig. 1. It was shown that channel lengths of less than 10μm are needed to avoid capacitance attenuation in inversion for sub-20Å oxides [4]. *Owing to differences in channel resistance, tunnelling current and capacitance for inversion and accumulation bias, the capacitance attenuation may be asymmetric. The limit on the channel dimensions for minimum capacitance attenuation in accumulation needs to be estimated.* In this Letter, an analytic model of the terminal gate capacitance for the structure shown in Fig. 1 is derived and used to estimate the limit on test structure dimensions for minimum capacitance attenuation in accumulation.

Model: For the capacitor test structure shown in Fig. 1, substrate contact is provided by a p^+ region for n^+ poly-SiO_2-*p*-Si devices. When the gate is biased in accumulation ($V_g < 0$), a sinusoidal small signal with frequency f is applied to the gate in order to measure the capacitance. In response to the applied test signal, if it is assumed that the introduction (or removal) of holes to (or from) the channel area occurs mainly in the lateral direction, a one-dimensional distributed RC network (shown in Fig. 2) can be used to model, approximately, the small-signal admittance of the structure shown in Fig. 1. Using standard transmission line analysis [8 – 10], it can be shown that the terminal gate capacitance and conductance of the RC network shown in Fig. 2 can be expressed in terms of intrinsic physical circuit model components as:

$$C_g \simeq \frac{G_T}{\omega}\,\mathrm{Im}\left[\frac{\tan\lambda}{\lambda}\right] + C_{go}\,\mathrm{Re}\left[\frac{\tan\lambda}{\lambda}\right] \quad (1)$$

$$G_g \simeq \frac{G_T}{\omega}\,\mathrm{Re}\left[\frac{\tan\lambda}{\lambda}\right] - \omega C_{go}\,\mathrm{Im}\left[\frac{\tan\lambda}{\lambda}\right] \quad (2)$$

with C_{go} is the intrinsic gate capacitance (series combination of oxide capacitance, C_{ox}, and accumulation layer capacitance), and $\lambda = (L_{pp}/2)\sqrt{(G_T r + j\omega C_{go} r)}$, where ω is the angular frequency and L_{pp} is the distance between p^+ substrate contacts (see Fig. 1), r is the *SR* of the accumulation layer, and G_T is tunnelling conductance. The terminal C_g–V_g curve can be calculated using eqn. 1 by generating $C_{go}(V_g)$ using a one-dimensional numerical calculations [6] and $J_g(V_g)$ using a WKB-based simple analytic model [11].

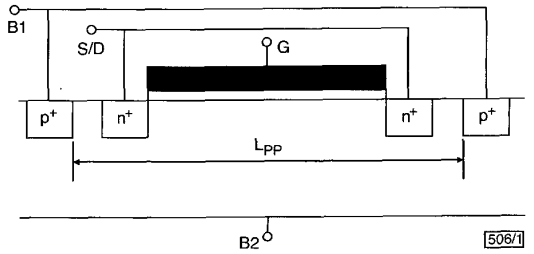

Fig. 1 *Schematic diagram of capacitor test structure used for C-V measurements*

Terminal B1 or B2 can be used for substrate contact

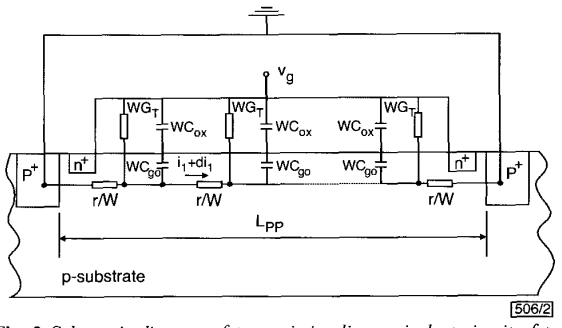

Fig. 2 *Schematic diagram of transmission line equivalent circuit of test structure shown in Fig. 1, terminal B2 used for substrate contact*

Effect of tunnelling current taken into account using tunnelling conductance G_T. C_{go} = intrinsic gate capacitance per unit, and r = accumulation channel sheet resistivity

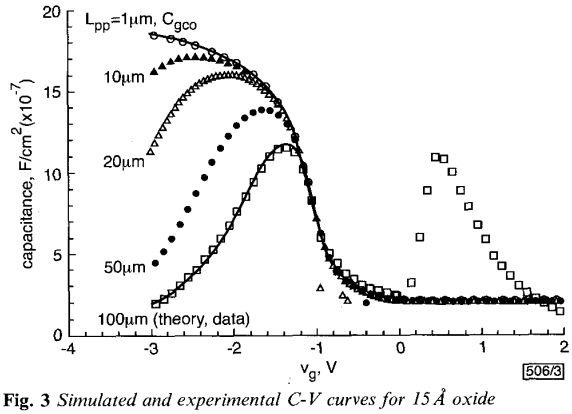

Fig. 3 *Simulated and experimental C-V curves for 15 Å oxide*

Excellent agreement is shown between analytic model of eqn. 1 and theoretical and experimental data of [7] for 100 × 100μm² capacitor. Simulated C-V curves for different values of L_{pp} are also shown
□ data
t_{ox} = 1.5nm
$m_{ox} = 0.5m_o$
ϕ_B = 3.1eV