higher compression ratio of around 100:1 (0.08 bit/pixel), the

Table 1: Coding performance of 512×512 colour image 'Lena' using WT-ABPRLC and JPEG codec

	Compression ratio	PSNR
		dB
WT-ABPRLC	50:1 (0.16 bit/pixel)	35.93
JPEG	50:1 (0.16 bit/pixel)	35.95
WT-ABPRLC	100:1 (0.080 bit/pixel)	34.15
JPEG	99:1 (0.081 bit/pixel)	32.05
WT-ABPRLC	178:1 (0.045 bit/pixel)	32.20
JPEG	166:1 (0.048 bit/pixel)	26.33

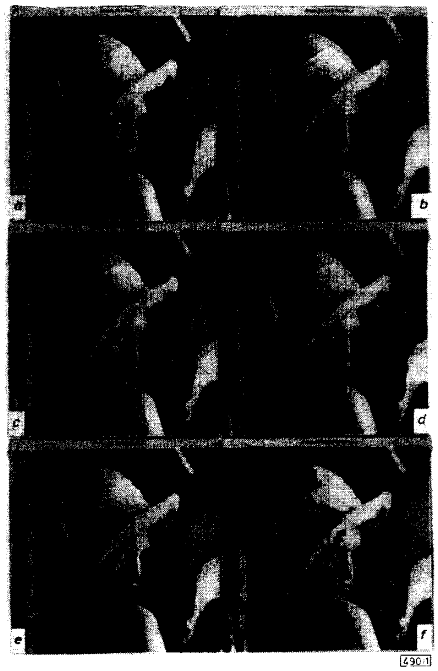

Fig. 1 *Reconstructed 'Lena' image coded at different compression ratios using both codecs*

a Coded using WT-ABPRLC at 50:1 (0.16 bit/pixel), average Y, U, V PSNR=35.93dB
b Coded using JPEG at 50:1 (0.16 bit/pixel), average Y, U, V PSNR=35.95dB
c Coded using WT-ABPRLC at 100:1 (0.08 bit/pixel), average Y, U, V PSNR=34.15dB
d Coded using JPEG at 99:1 (0.081 bit/pixel), average Y, U, V PSNR=32.05dB
e Coded using WT-ABPRLC at 178:1 (0.045 bit/pixel), average Y, U, V PSNR=32.20dB
f Coded using JPEG at 166:1 (0.048 bit/pixel), average Y, U, V PSNR=26.33dB

shape and edge details of the WT-ABPRLC coded image (Fig. 1*c*, 34.15dB) are still preserved and give quite acceptable quality. In the JPEG reconstructed image (Fig. 1*d*, 32.05dB), a 'blocking effect' is noticeable. When the compression ratio is increased to 178:1 (0.045 bit/pixel), the WT-ABPRLC still gives a reasonably acceptable image (Fig. 1*e*, 32.20dB), despite the noise that is concentrated around the edges. At a compression of 166:1 (0.048 bit/pixel), the JPEG reconstruction (Fig. 1*f*, 26.33dB) gives a very blocky image. It is worth noting that the colours in the JPEG reconstruction (Fig. 1*f*) are totally different from those in the original.

This Letter has presented a very simple and effective adaptive image coding scheme which requires no training, no storage of codebooks and produces good quality and compression performance. Compared to the JPEG codec, results show that the new WT-ABPRLC codec gives better quality at high compression ratios. Compared to other hybrid WT based methods such as using VQ or other sophisticated algorithms, this method is much simpler to implement.

Acknowledgment: The authors would like to acknowledge the portable video research group (PVRG), for the use of the PVRG-JPEG 1.1 software package.

20 December 1994
Electronics Letters Online No: 19940259

K.H. Goh, J.J. Soraghan and T.S. Durrani (*Department of Electronic and Electrical Engineering, Signal Processing Division, University of Strathclyde, 204 George Street, Glasgow G1 1XW, United Kingdom*)

References

1 ANTONINI, M., BARLAUD, M., and MATHIEU, P.: 'Image coding using lattice vector quantization of wavelet coefficients'. IEEE ICASSP, Toronto, Canada, 1991, **4**, pp. 2273–2276
2 ANTONINI, M., BARLAUD, M., MATHIEU, P., and DAUBECHIES, I.: 'Image coding using wavelet transform', *IEEE Trans.*, 1992, **IP-1**, (2), pp. 205–220
3 SHAPIRO, J.: 'A embedded wavelet hierarchical image coder'. IEEE ICASSP, San Francisco, CA, 1992, **IV**, pp. 657–660
4 LEWIS, A.S., and KNOWLES, G.: 'Image compression using the 2-D wavelet transform', *IEEE Trans.*, 1992, **IP-1**, (2), pp. 244–250

New digital signature scheme based on discrete logarithm

L. Harn

Indexing terms: Cryptography, Data privacy

A new digital signature scheme based on the discrete logarithm is presented. The advantages of this scheme over the ElGamal signature scheme are that it simplifies the signature generation process, it speeds up the signature verification process, it has a broadband subliminal channel to allow any secret information to be concealed in the signature and the secret information can only be recovered by the insiders with the secret key shared with the signer, and it can provide an efficient multisignature.

Introduction: In 1985, ElGamal [1] proposed the original digital signature scheme based on the discrete logarithm problem. A modification of the ElGamal signature was proposed by Agnew *et al.* [2] in 1990. Instead solving $m = xr + ks \bmod p - 1$, the signer solves the congruence $m = xs + kr \bmod p - 1$. The signature (r, s) is verified by checking the quation $\alpha^m = y^s r^r \bmod p$. The advantage of this modified scheme over the ElGamal scheme is that to compute the signature by solving the congruence for s, the signer only needs to compute x^{-1} In $\mathbf{Z}^*_{p-1}$ once, instead of computing k^{-1} in $\mathbf{Z}^*_{p-1}$ for every signature, where x is the secret key for the signer and k is an integer randomly selected by the signer for signing every message.

To shorten the length of the signature and to speed up the signature generation/verification process, in 1989, Schnorr [3] proposed an efficient signature scheme for smart card application, and in 1991, the NIST proposed the digital signature algorithm [4] (DSA) for the digital signature standard. These two schemes were developed based on the original ElGamal signature scheme.

In 1985, Simmons [5] demonstrated that it is possible to conceal secret information in the ElGamal digital signature and the secret information can only be recovered by the insider with the secret key shared with the signer. Possible applications of such subliminal channel can be found in [6]. Two 'narrowband' subliminal channels [7] in the DSA were found in 1993. Most recently, Simmons [6] has shown that the 'broadband' subliminal channel also exists in the DSA. We would like to point out that a similar 'broadband' subliminal channel also exists in the Schnorr digital signature scheme (DSS). The DSA and Schnorr DSS use modulus p for which $p - 1$ has one large prime factor q. It is very difficult to establish a 'broadband' subliminal channel in the ElGamal signature, especially for modulus p for which $p - 1$ has several factors [6].

In this Letter, we would like to propose a new digital signature scheme based on the ElGamal scheme. The advantages of this scheme over the ElGamal signature scheme are that it simplifies the signature generation process, it speeds up the signature verification process, it has a 'broadband' subliminal channel to allow any secret information to be concealed in the signature and the modulus can be any prime number, and it can provide an efficient multisignature.

Our proposed signature scheme: This scheme was due to the original ElGamal signature scheme. We start with a large prime p, and a primitive element α of GF(p), which are publicly known. A one-way function f also needs to be made public.

In this scheme, each signer selects a random exponent z from GF(p) as his private key. Suppose A randomly selects a number, z_A, from $[1, p - 1]$ with $\gcd(z_A, p - 1) = 1$; then A computes

$$y_A = \alpha^{z_A} \mod p$$

as A's public key. Assume A wants to sign the message m. A randomly selects a number k from $[1, p - 1]$ and computes

$$r = \alpha^k \mod p$$

A now solves the congruence

$$z_A(m' + r) = k + s \mod p - 1$$

or

$$s = z_A(m' + r) - k \mod p - 1 \qquad (1)$$

for integer s, where $0 \le s \le p - 2$, and $m' = f(m)$. The signature for message m is then the ordered pair $\{r, s\}$.

On receiving the set of $\{m, r, s\}$, any user can verify the signature of message m as

$$y_A^{m'+r} = r\alpha^s \mod p \qquad (2)$$

where $m' = f(m)$.

Security: An attacker might try to solve the secret key z_A, based on the linear equation eqn. 1. For the given message and the signature pair, eqn. 1 involves two unknown parameters, z_A and k. For any increment of the message and the corresponding signature pair, the unknown parameter is also increased by one. This attack cannot work successfully.

The attacker might try to forge a signature pair of a given message based on eqn. 2. He might try to randomly select an integer r' first and then compute the corresponding s' based on eqn. 2. Obviously, this difficulty is equivalent to solving the discrete logarithm problem. On the other hand, he might try to randomly select an integer s' first and then compute the corresponding r'. This is also an extremely difficult problem.

Computation: From eqn. 1, the signer needs to solve the congruence in order to determine the signature. There is no need to compute any computational inverse as is required in the ElGamal and the Agnew *et al.* schemes.

From eqn. 2, the verifier needs to compute only two modular exponentiations to verify the signature. Both the ElGamal and the Agnew *et al.* schemes require three modular exponentiations to verify the signature.

Subliminal channel: Suppose that one of the verifiers is the insider with knowledge of the signer's secret key, z_A. The insider can compute k as

$$k = z_A(m' + r) - s \mod p - 1$$

Thus, k can be used as the information to communicate through the subliminal channel. Because there is no condition imposed on k, any information can be encoded in the channel and the encoded information can be extracted easily by the insider with knowledge of the secret key. This new scheme does not need to use the forward search cryptanalytic technique as discussed by Simmons [6] to recover k.

Multisignature: Most recently Harn [8] proposed the first efficient multisignature scheme based on the discrete logarithm. The multisignature scheme allows multiple signers to sign the same message separately and all individual signatures can be combined into a multisignature without any data expansion. We want to show that this new signature scheme proposed in the Letter can also provide digital multisignature.

We assume that there are n signers to sign the same message m.

Generation and verification of individual signature: Each signer u_i randomly selects a number k_i from $[1, p - 1]$ and computes

$$r_i = \alpha^{k_i} \mod p$$

$\{r_i\}$ is broadcast to all signers. Once r_i, $i = 1, 2, \ldots, n$, from all signers are available through the broadcast channel, each signer computes the value r as

$$r = \prod_{i=1}^{n} r_i \mod p$$

Signer u_i uses his secret keys, z_i and k_i, to sign the message m based on the new signature scheme as we proposed previously. u_i solves the equation

$$s_i = z_i(m' + r) - k_i \mod p - 1$$

for integer s_i, where $0 \le s_i \le p-2$ and $m' = f(m)$, and transmits $\{m, s_i\}$ to the clerk. This designated clerk, who takes the responsibility for collecting and verifying each individual signature, will produce a combined multisignature. There is no secret information associated with this designated clerk.

Once the clerk receives the individual signature $\{r_i, s_i\}$ from u_i, he needs to verify the validity of this signature by checking the following equation:

$$y_i^{m'+r} = r_i\alpha^{s_i} \mod p$$

where $m' = f(m)$ and y_i is the public key for u_i. If the above equation holds true, the partial signature $\{r_i, s_i\}$ of message m received from u_i has been verified.

Generation of multisignature: Once all individual signatures have been received and verified by the clerk, the multisignature of message m can be generated as $\{r, s\}$, where $s = s_1 + s_2 + \ldots + s_n \mod p - 1$

Verification of multisignature: After receiving the multisignature, $\{r, s\}$, of message m, an outsider needs to use all signers' public key, y, to verify the validity of the multisignature. The public key y associated with all signers is determined as

$$y = \prod_{i=1}^{n} y_i \mod p$$

where y_i is the public key for the signer u_i. The verification procedure is given as

$$y^{m'+r} = r\alpha^s \mod p \qquad \text{where } m' = f(m)$$

If the above equation holds true, the multisignature $\{r, s\}$ has been verified.

 14 December 1993

Electronics Letters Online No: 19940317

L. Harn (*Computer Science Telecommunications Program, University of Missouri, Kansas City, MO 64110, USA*)

References

1 ELGAMAL, T.: 'A public key cryptosystem and signature scheme based on discrete logarithms', *IEEE Trans.*, July 1985, **IT-31**, (4), pp. 469–472
2 AGNEW, G.B., MULLIN, R.C., and VANSTONE, S.A.: 'Improved digital signature scheme based on discrete exponentiation', *Electron. Lett.*, 1990, **26**, (14), pp. 1024–1025
3 SCHNORR, C.P.: 'Efficient identification and signatures for smart cards'. Advances in Cryptology - CRYPTO '89, August 20–24, 1989, Santa Barbara, pp. 239–252, (Springer-Verlag)
4 'The digital signature standard', *Comm. ACM*, 1992, **35**, (7), pp. 36–40
5 SIMMONS, G.J.: 'A secure subliminal channel (?)'. Advances in Cryptology - CRYPTO '85, August 18–22, 1985, Santa Barbara, pp. 33–41, (Springer-Verlag)
6 SIMMONS, G.J.: 'Subliminal communication is easy using the DSA'. Pre-Proc. EUROCRYPT '93, May 24–27, 1993, Lofthus, Norway
7 SIMMONS, G.J.: 'The subliminal channels in the U.S. digital signature algorithm (DSA)'. Proc. 3rd Symp. on State and Progress of Research in Cryptology, Rome. Italy, February 15–16, 1993
8 HARN, L.: 'Efficient digital multisignatures', submitted to EUROCRYPT '94

Single beam photoreflectance microscopy system with electronic feedback

M.B. Suddendorf and M.G. Somekh

Indexing terms: Scanning optical microscopes, Laser beam applications

A new photoreflectance (PR) system which uses only a single optical beam is described. The PR signal is detected at the second harmonic of the modulation frequency, contained in the backreflected light. To reliably measure this small signal, the second harmonic content of the incident beam is reduced by feedback to the modulator.

Modulated photoreflectance [1] is a well established technique for characterisation of semiconductors. The usual implementation [1] uses a relatively high power modulated pump beam, which induces a periodic change in the reflectivity of the sample surface. A low power continuous wave laser is focused onto the same spot as the pump laser, where the intensity of the light reflected from the sample is modulated by the induced photoreflectance. Wagner *et al.* [2] have developed alternative systems, that use a single laser for pump and probe. They split the beam into two separate paths in which intensity modulation at two different frequencies is imposed. The beams are recombined prior to hitting the sample and the photoreflectance signal is detected at the difference between the two modulation frequencies.

The main complication with both system implementations [1, 2] is the need to recombine two optical beams so that they overlap on the sample surface. The focal spots have a diameter of ~1 µm, so that precise alignment and adjustment are necessary. Furthermore, any drift between the two beams gives inconsistent results.

Fig. 1 shows the optical configuration of the single beam system. A frequency doubled Nd-YAG laser (giving ~45mW output power at 532nm), modulated by the acousto-optical (Bragg) cell at a angular frequency ω_m illuminated the sample. The feedback system described in the following paragraphs was employed to reduce the second harmonic output from PD1, so that the photoreflectance signal could be detected at $2\omega_m$ with photodetector PD2.

Let the incident intensity, I_s, on the sample vary sinusoidally, i.e. $I_s = I_0(1 + m\cos(\omega_m t))$, where I_0 is the mean light intensity and m is the index of modulation at the frequency ω_m. The sample reflectivity, R, is given by $R_0 + \Delta R I_s$, where R_0 is the sample intensity reflection coefficient in the absence of optical excitation and ΔR is the photoreflectance coefficient which gives the change in reflectivity divided by the incident intensity, I_s. The intensity of the reflected light, I_r, is thus

$$\begin{aligned} I_r = RI_s = {} & (R_0 I_0 + \Delta R I_0^2 + \frac{1}{2}m^2\Delta R I_0^2) \\ & + (mR_0 I_0 + 2m\Delta R I_0^2)\cos(\omega_m t) \\ & + \frac{1}{2}m^2 \Delta R I_0^2 \cos(2\omega_m t) \end{aligned} \quad (1)$$

The reflected power thus contains a large signal at ω_m and a relatively small signal at $2\omega_m$ which is proportional to the photoreflectance coefficient.

The difficulty with our approach lies in the fact that the optical second harmonic signal is typically $10^3 - 10^5$ times smaller than the fundamental. The amount of second harmonic incident on the sample must therefore be kept to a very low value, so that the changes in harmonic content are not swamped (reduction of the optical harmonic to 10^{-6} times the fundamental, implies the harmonic in the electrical signal 120dB below the fundamental). In this Letter an effective feedback method to reduce the second harmonic at PD1 is described.

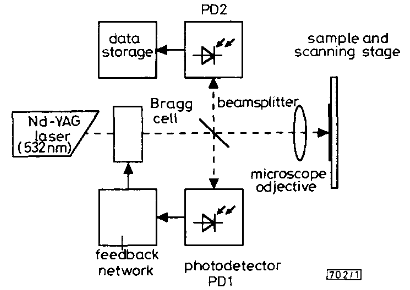

Fig. 1 *Optical system of single probe beam photoreflectance system*

– – – – optical signal
——— electrical signal

The most obvious method of reducing the second harmonic signal is to feed a proportion of the output signal back to the input to cancel the distortions produced in the forward path. The amount of reduction in second harmonic distortion is determined by the loop gain. The implementation of this approach is hampered by bandwidth requirements in the feedback loop much in excess of the actual signal bandwidth [3]. As the loop bandwidth is increased the phase shifts experienced by the higher frequencies reduce the maximum stable loop gain. In our photoreflectance system this would limit the usable beam modulation frequency to impractically low values (tens of Hertz).

It is not necessary, however, for the feedback to act at the modulation frequency but merely to compensate for changes in the harmonic content produced by slow drift. This removes the need for a rapid feedback, and the loop bandwidth becomes independent of the modulation frequency.

To achieve the requirements indicated above, the system shown in Fig. 2 was implemented. The lock-in amplifier outputs, X and Y, are proportional to the in-phase and quadrature components of the second harmonic content of the modulated beam. These components are then multiplied with $\cos(2\omega_m t)$ and $\sin(2\omega_m t)$ signals, derived from the signal source. The output from the summing amplifier reproduces the second harmonic signal input into the lock-in amplifier, averaged over the integration period of the lock-in amplifier. Given the proper adjustment of the lock-in reference phase, the output from the summing amplifier at $2\omega_m$ will have the appropriate amplitude and phase to cancel the $2\omega_m$ from the modulated laser beam. Using the lock-in amplifier in this way effectively inserts a dominant low frequency pole into the open loop transfer function, thus allowing the use of high gains which give excellent suppression of second harmonic content while still retaining large gain and phase margins. The loop gain and hence the approximate reduction in electrical second harmonic signal thus achieved was 60dB, with the effect of reducing the second harmonic power of the modulated light beam measured at PD1 to 2×10^{-6} times the fundamental power.