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

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

<table>
<thead>
<tr>
<th>Compression ratio</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>WT-ABPRLC</td>
<td>50:1</td>
</tr>
<tr>
<td></td>
<td>(0.16 bit/pixel)</td>
</tr>
<tr>
<td>JPEG</td>
<td>50:1</td>
</tr>
<tr>
<td></td>
<td>(0.16 bit/pixel)</td>
</tr>
<tr>
<td>WT-ABPRLC</td>
<td>100:1</td>
</tr>
<tr>
<td></td>
<td>(0.080 bit/pixel)</td>
</tr>
<tr>
<td>JPEG</td>
<td>99:1</td>
</tr>
<tr>
<td></td>
<td>(0.081 bit/pixel)</td>
</tr>
<tr>
<td>WT-ABPRLC</td>
<td>178:1</td>
</tr>
<tr>
<td></td>
<td>(0.045 bit/pixel)</td>
</tr>
<tr>
<td>JPEG</td>
<td>166:1</td>
</tr>
<tr>
<td></td>
<td>(0.048 bit/pixel)</td>
</tr>
</tbody>
</table>

shape and edge details of the WT-ABPRLC coded image (Fig. 1c, 34.15dB) are still preserved and give quite acceptable quality. In the JPEG reconstructed image (Fig. 1d, 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. 1e, 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. 1f, 26.33dB) gives a very blocky image. It is worth noting that the colours in the JPEG reconstruction (Fig. 1f) 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.

© IEE 1994 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 GI 1XW, United Kingdom)

References

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 embedded 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 multi-signature.

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 \( m = x + ks \mod p - 1 \), the signer solves the congruence \( m = ax + ks \mod p - 1 \). The signature \( (r, s) \) is verified by checking the equation \( os = yr \mod p \). The advantage of this modified scheme over the ElGamal scheme is that to compute the signature by solving the congruence for \( x \), the signer only needs to compute \( x' \mod Z_p \) once, instead of computing \( k' \) in \( Z_p \) 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 [8] 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 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 is due to the original ElGamal signature scheme. We start with a large prime $p$, and a primitive element $a$ of $\mathbb{F}_p^*$. A user chooses $k$ (also needs to be made public).

In this scheme, each signer selects a random exponent $z$ from $\mathbb{Z}_p^*$ as his private key. Suppose $A$ randomly selects a number, $z_A$ from $[1, p - 1]$; then $A$ computes $y_A = a^{z_A} \mod p$ 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

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

$A$ now solves the congruence

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

or

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

for integer $s$, where $0 \leq s < p - 2$, and $m^r = f(m)$. 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

$$y_A^s = r a^s \mod p \quad (2)$$

where $m^r = f(m)$.

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 expositions 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

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

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 cryptoanalytic technique as discussed by Simmons [6] to recover $k$.

Multisignature: Most recently Harn [9] 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

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

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

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

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

for integer $s_i$, where $0 \leq s_i < p - 2$ and $m^r = f(m)$, and transmits $(m, s_i)$ to the cleric. This designated cleric, 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 cleric.

Once the cleric 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:

$$y_i^s = r_i a^s \mod p$$

where $m^r = f(m)$ 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 cleric, 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 keys, $y_i$, 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

$$y^s = r a^s \mod p$$

where $m^r = f(m)$.

If the above equation holds true, the multisignature $(r, s)$ has been verified.

© IEEE 1994 3rd March 1994 Vol. 30 No. 5 397

L. Harn (Computer Science Telecommunications Program, University of Missouri, Kansas City, MO 64110, USA)
Single beam photoreflectance microscopy system with electronic feedback

M.B. Suddendorf and M.G. Somekh

Indexing terms: Scanning optical microscope, 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 reflected light, \( L_0 \), is thus

\[
L_0 = R l_0 + \Delta R l_0^R + \frac{1}{2} m^2 \Delta R l_0^I
\]

where \( R \) is the mean light intensity and \( \Delta R l_0^R \) and \( \Delta R l_0^I \) are the in-phase and quadrature components of the second harmonic content of the modulated beam. These components are then multiplied with \( \cos(2\omega t) \) and \( \sin(2\omega t) \) 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 \( 2\omega_0 \) will have the appropriate amplitude and phase to cancel the \( 2\omega_0 \) from the modulated laser beam. Using the lock-in amplifier in this way effectually 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 \( \times \) 10^4 times the fundamental power.

The difficulty with our approach lies in the fact that the optical second harmonic signal is typically 10^-4 - 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, otherwise, the changes in harmonic content are not swamped (reduction of the optical harmonic to 10^-4 times the fundamental, implies the harmonic in the electrical signal 126dB below the fundamentals). In this Letter an effective feedback method to reduce the second harmonic at PD1 is described.

References


