References

1 ITU Recommendation Standardization Sector, ITU-T Recommendation H.263, 'Video coding for low bitrate communication'. November 1995

2 International Organization for Standardization, ISO/IEC/JTC1/SC29/WG11, 'Description of error resilient code experiments'. Document No. N1327, July 1996

3 Telenor R&D: 'H.263 Video codec test model'. November 1995

Minimum-maximum exclusive mean (MMEM) filter to remove impulse noise from highly corrupted images

Wei-Yu Han and Ja-Chen Lin

Indexing terms: Median filters, Image processing, Digital filters

The minimum-maximum exclusive mean (MMEM) filter is presented to remove impulse noise from highly corrupted images. Simulation results show that even if the occurrence rate of the impulse noise is very high (70%), the restoration performance is still acceptable.

Introduction: The median filter [1] is a traditional method for removing impulse noise. Recently, Russo and Ramponi [2] presented a two-step fuzzy reasoning method for achieving good impulse noise cancellation as well as preserving image detail. Abreu *et al.* [3] also suggested a rank-ordered mean (ROM) filter whose output is the weighted combination of the input signal and ROM. When the noise is < 40%, the ROM filter is effective at suppressing noise and preserving detail. However, through experimental observations, we found that the good performances of these methods [1 – 3] tend to reduce significantly when the occurrence rate of the impulse noise is > 40%. In this Letter we propose an MMEM filter suitable for removing impulse noise, when the percentage of impulse noise is high.

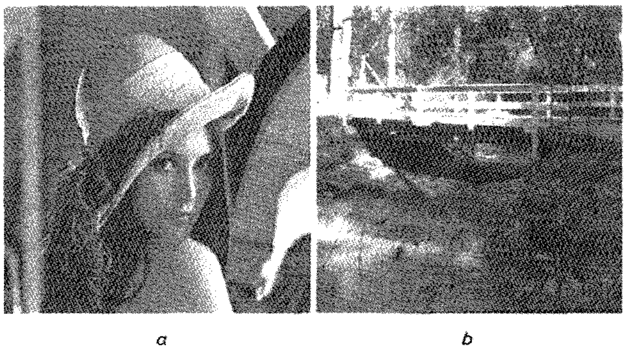

Fig. 1 *Two original images*

a Lena
b Bridge

Proposed MMEM filter: Let $W_n(i, j)$ be a window of size $n \times n$ centred at pixel (i, j). The proposed filter is applied to the original noisy image pixel by pixel to replace the original grey value $g(i, j)$ by the filtered value $\tilde{g}(i, j)$. In other words, for each pixel (i, j) perform the following:

Step 1: $n = 3$

Step 2: Find the maximum and minimum grey values (g_{MAX} and g_{MIN}) within the window $W_n(i, j)$.

Step 3: Discard all pixels $(l, m) \in W_n(i, j)$ whose $\lfloor g(l, m)/4 \rfloor$ equals $\lfloor g_{MIN}/4 \rfloor$ or $\lfloor g_{MAX}/4 \rfloor$. Here $g(l, m)$ is the input grey value at pixel (l, m).

Step 4: If all pixels in the window are discarded and $n = 3$, then set $n = 5$ and go to step 2.

Step 5: Calculate the average (original) grey value of the pixels not discarded, and call this average value *AVG*. (However, if $n = 5$ and if all 25 pixels in the window $W_5(i, j)$ are again discarded, then use the average of the filtered output values of the four neighbouring pixels $\{ \tilde{g}(i-1, j \pm 1),\ \tilde{g}(i-1, j),\ \tilde{g}(i, j-1)\}$ as the *AVG*.)

Step 6: If $|AVG - g(i, j)| > 30$, the filtered output of the pixel (i, j) is $\tilde{g}(i, j) = AVG$; otherwise, $\tilde{g}(i, j) = g(i, j)$, i.e. use the original grey value $g(i, j)$.

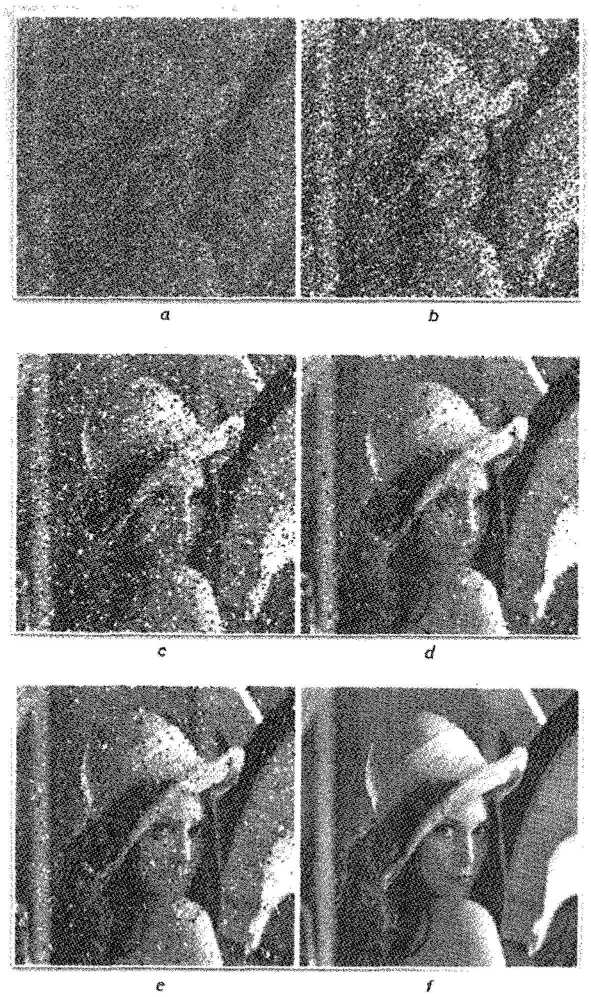

Fig. 2 *Subjective visual qualities of restored images 'Lena' produced by different filters*

a Input noisy image (with 70% noise)
b 3 × 3 median filtered image
c 5 × 5 median filtered image
d fuzzy filtered image
e ROM filtered image
f proposed MMEM filtered image

Simulation results: Nine 512 × 512 'Lena' images corrupted by impulse (salt and pepper) noise with occurrence rate ranging from 10 to 90% were tested. (For the original image 'Lena' see Fig. 1*a*.) The peak signal-to-noise ratio (PSNR) is used as an objective measurement of the restored image quality. For comparison, the median filter [1], fuzzy filter [2] and ROM filter [3] were also implemented in our experiments. The 1296 weighting coefficients for the ROM filter were obtained by recursively computing eqn. 15 of [3] using some training data. From Table 1, it is observed that the PSNR performance of the proposed MMEM filter is often better than that of the other three filters, especially when the noise probabilities are greater than 40%. We may also inspect the restored images to compare the subjective visual qualities. Fig. 2*a* displays the input noisy image whose noise probability is 70%, and Fig. 2*b* – *f* exhibit the filtered images produced by the 3 × 3 median, 5 × 5 median, fuzzy, ROM, and MMEM filters, respectively. From Fig. 2 we can see that except the result processed by our method, other filtered images are still seriously corrupted by impulse noise. Another nine 512 × 512 'Bridge' images corrupted by impulse (salt and pepper) noise with occurrence rate ranging from 10 to 90% were also tested, and the PSNR performance is provided in Table 2.

Table 1: PSNR obtained by different filters for corrupted image 'Lena'

Noise percentage	Median (3×3)	Median (5×5)	Fuzzy [2]	ROM [3]	Our MMEM
	PSNR	PSNR	PSNR	PSNR	PSNR
10	34.25	31.23	37.88	38.98	38.60
20	29.58	30.60	34.19	36.55	36.76
30	23.85	29.72	31.19	33.43	35.41
40	19.18	28.21	28.00	29.88	34.32
50	15.28	24.44	24.97	26.04	32.97
60	12.31	19.09	21.66	21.97	31.76
70	9.95	14.16	18.27	18.12	30.29
80	8.07	10.34	14.72	14.00	28.50
90	6.54	7.42	10.30	9.29	26.09

Table 2: PSNR obtained by different filters for corrupted image 'Bridge'

Noise percentage	Median (3×3)	Median (5×5)	Fuzzy [2]	ROM [3]	Our MMEM
	PSNR	PSNR	PSNR	PSNR	PSNR
10	32.85	28.84	36.78	36.46	37.03
20	28.97	28.34	33.82	34.62	35.54
30	23.34	27.57	30.74	31.87	34.20
40	19.00	26.37	27.65	28.71	33.03
50	15.13	23.29	24.24	24.81	31.70
60	12.25	18.63	20.89	21.04	30.24
70	9.87	13.97	17.61	17.41	28.72
80	7.99	10.25	14.37	13.52	26.77
90	6.48	7.33	10.06	9.14	23.97

Conclusions: In this Letter we propose a minimum-maximum exclusive mean (MMEM) filter which is robust for removing impulse noise. Experimental results show that even if the noise is heavy (70%), the proposed filter can still work properly and the restored image is acceptable.

Acknowledgment: This work was supported by the National Science Council, Republic of China, under grant NSC86-2213-E009-108.

© IEE 1997 *12 November 1996*
Electronics Letters Online No: 19970106

Wei-Yu Han and Ja-Chen Lin (*Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 30050, Republic of China*)

Wei-Yu Han: Corresponding author

E-mail: gis81576@cis.nctu.edu.tw

References

1 GONZALES, R.C., and WOODS, R.E.: 'Digital image processing' (Addison-Wesley, 1992)

2 RUSSO, F., and RAMPONI, G.: 'A fuzzy filter for images corrupted by impulse noise', *IEEE Signal Process. Lett.*, 1996, **3**, (6), pp. 168–170

3 ABREU, E., LIGHTSTONE, M., MITRA, S.K., and ARAKAWA, K.: 'A new efficient approach for the removal of impulse noise from highly corrupted images', *IEEE Trans.*, 1996, **IP-5**, (6), pp. 1012–1025

Digital signature for Diffie-Hellman public keys without using a one-way function

L. Harn

Indexing term: Public key cryptography

The author proposes digital signature schemes without using a one-way function to sign Diffie-Hellman public keys. The advantage of this approach is, instead of relying overall security on either the security of the signature scheme or the security of the one-way function, the security of this proposed scheme is based on the discrete logarithm problem.

Introduction: A one-way function is needed in any digital signature scheme. Without using a secure one-way function, a digital signature can be easily forged [1, 2]. There are some well-known one-way hash functions, such as the MD4, MD5, SHA, etc. There exists a major difference of security assumptions between digital signature schemes and one-way functions. The security assumptions of most signature schemes are based on some well-known computational problems, such as the discrete logarithm problem, the factoring problem, etc. However, the security of most one-way hash functions is based on the complexity of analysing an iterated simple function. Since most computational problems are well-known and easy to understand, the security of most signature schemes can withstand quite a long period of time. However, a one-way function may seem very difficult to analyse at the beginning; but it may turn out to be vulnerable to some special attacks later. Thus, in general, the lifetime of one-way functions is shorter than that of signature schemes. For example, recent advancement of cryptanalysis research has found that MD5 is 'at the edge' of risking successful cryptanalytic attack [3]. There are two motivations of proposing signature schemes without using a one-way function. First, instead of relying overall security on the weaker assumption between the signature scheme and the one-way function, the security of our proposed schemes is based on the discrete logarithm problem. Secondly, the overall security can be easily understood and analysed.

Diffie and Hellman [4] proposed the well-known public-key distribution scheme based on the discrete logarithm problem in 1976 to enable two parties to establish a common secret session key based on their exchanged public keys. But their original scheme can only share one common secret key and did not provide authentication for the exchanged public keys. Since them, several key exchange protocols [5, 6] to allow two parties to share multiple secret session keys have been proposed based on the Diffie-Hellman public-key technique. In general, these protocols utilise a digital signature for each distributed public key to provide authentication. Since Diffie-Hellman's public key is obtained by computing an exponential function over GF(p) and the exponential function itself is a well-known one-way function, we propose signature schemes without using any additional one-way function for signing Diffie-Hellman public keys. In addition, since the Diffie-Hellman public key is a random number, our proposed schemes are not suitable for signing any given message.

Digital signature schemes for Diffie-Hellman public keys: Let p be a large prime and α be a primitive number in GF(p). Each user selects a fixed secret key $x \in [1, p{-}1]$ and computes a fixed public key $y = \alpha^x \bmod p$, where y is signed by one authority. $\{p, \alpha, y\}$ are the user public information.

A signature scheme uses a fixed secret key to sign a message and a verifier uses a signer's fixed public key to verify the signature of a message. In this proposed signature scheme, the message itself is a random Diffie-Hellman public key $r = \alpha^k \bmod p \in [1, p{-}1]$ computed by the signer, where k is a secret random integer $k \in [1, p{-}2]$ privately selected by the signer.

Now, we use the following model to describe the signing process. The signer uses his secret keys, x and k, to compute the signature s which satisfies

$$ax = bk + c \bmod \emptyset(p)$$

where (a, b, c) are parameters selected from values (r, s). The verification equation is determined accordingly as

$$y^a = r^b \alpha^c \bmod p$$