Fig. 2 shows the arithmetic complexity of the various block-matching algorithms for the video data 'Talking man'. The video data consists of 41 frames, each frame with size 320 × 240. The dimension of the blocks is N = 8 × 8. The maximum motion in the vertical and horizontal directions is assumed to be ±7. Therefore, for the full-search method, T = 225. To reduce the overhead for performing the DWT, the wavelet used in this Letter is the simple Haar wavelet [4], so no multiplication is required. Other multiplication free unitary transforms such as the Hadamard transform can also be used for the PDS in the algorithm. From Fig. 2, it follows that the algorithm using the PDS in the wavelet domain enjoys less arithmetic complexity than that of the TSA and the full-search method. We also note that our algorithm enjoys the same average distortion as the full-search block-matching algorithm, whereas the TSA method has a higher average distortion. Supposing that a higher average distortion is allowed, then from Fig. 2, it follows that the algorithm performing PDS in the wavelet domain for TSA enjoys the lowest arithmetic complexity. Note that this algorithm has the same average distortion as that of the TSA.

Conclusion: We propose a new fast block-matching algorithm using DWT and PDS techniques. As compared with the full-search block-matching algorithm, the algorithm can reduce the computation time without sacrificing the average distortion for video encoding. Moreover, the algorithm requires less computation time than existing techniques. Simulation results show that the algorithm can be effectively used for the real-time encoding of video data.

© IEE 1997
Electronics Letters Online No: 19970581
Wen-Jyi Hwang, Yeong-Cheng Lu and Yi-Chong Zeng (Department of Electrical Engineering, Chung Yuan Christian University, Chungli, Taiwan, Republic of China)

Geometric approach for blind separation of signals

C.G. Puntonet and A. Prieto

**References**


**Geometric approach for blind separation of signals**

C.G. Puntonet and A. Prieto

**Indexing terms:** Signal processing, Signal detection

The authors suggest an approach to resolve the problem of the blind separation of p ≥ 2 sources. At one instant of time the sources and observations are considered as two vectors, and a simple method for estimating the mixing matrix is proposed for a linear system with bounded sources, where at least one set of orthogonal vectors is generated.

**Introduction:** The problem of separation consists of retrieving the unknown sources, s(t), solely from the observations, e(t), eliminating the effect introduced by the environment [1]. In this Letter, it is assumed that the number of sensors is equal to the number of sources, p, and that the observed signals e(t), (k = 1, 2, ..., p), satisfy

\[ e_k(t) = \sum_{i=1}^{p} a_{ki} \cdot s_i(t) \quad k = 1, 2, ..., p \]  

where \( a_{ki} \) are the coefficients of an unknown and regular A_{pp} matrix (mixing matrix). The signals \( s_i(t), (i = 1, ..., p) \) have a bounded probability density function and are unknown. It is also assumed that \( a_{ij} \neq a_{ji} \) and \( a_{ii} \neq 0 \) (\( i,j = 1, ..., p \)); this is based on the fact that each sensor i is physically nearer to one of the sources i (\( a_{ii} \)) than to others j (\( a_{ij} \)). The literature displays a diversity of approaches with most of them using some kind of statistical analysis [1–3]. We have previously proposed procedures to separate multivalued signals [4] and two analogue signals [5]. It is usual in the blind separation of sources [1, 5] to find a matrix B(t) such that the recovered signals X(t) represent the original sources S(t) transformed as follows:

\[ X(t) = B^{-1}(t) \cdot S(t) = B^{-1}(t) \cdot A(t) \cdot S(t) \]  
\[ B^{-1}(t) \cdot A(t) = D \cdot P \]  

where D is a diagonal matrix and P is a permutation matrix.

**Principles of method:** We define \( F_p(t) \) as a function of the mixed signals \( e_i(t), e_j(t) \) as follows:

\[ F_{ij}(t) = e_i(t) \cdot e_j(t)^{-1} \quad e_j(t) \neq 0 \quad \forall i, j \in \{1, ..., p\} \]  

From eqns. 1 and 3, and assuming the absence of added noise to the signals, it is verified that

\[ F_{ij}(t) = e_i(t) \cdot e_j(t)^{-1} = \left( \sum_{k=1}^{p} a_{ik} \cdot s_k(t) \right) \left( \sum_{k=1}^{p} a_{jk} \cdot s_k(t) \right)^{-1} \quad e_j(t) \neq 0 \quad \forall i, j \in \{1, ..., p\} \]  

This function is continuous in \( \mathbb{R} \times \{1,...,p\} \) with \( i \), being the set of values of \( s_k \) such that \( s_k(i) = 0 \), \( \forall k \in \{1,...,p\} \) with \( n \) being an integer. Thus, the function \( F_p(S): \mathbb{R} - \{0\} \to \mathbb{R} \) is not continuous at the point \( (s_1, ..., s_p) = (0, ..., 0) \). It is easy to verify that the possible extremes, \( F_{ij}^* \), of \( F_p \) are ratio terms \( (a_{i1}/a_{jk}) \), \( k \in \{1, ..., p\} \), as follows:

\[ (\partial F_{ij}/\partial s_k) = 0 \Rightarrow F_{ij}^* = (a_{i1}/a_{jk}) \quad \forall i, j, k \in \{1, ..., p\} \]  

Furthermore, if S is bounded, i.e. \( s_i \in [0, s_{i0}] \) and \( a_{i1}/a_{jk} \) is a minimum of \( F_{ij} \), then \( e_i > e_0 \), \( \forall k \in \{1, ..., p\} \), \( k \neq i \). The minimum value of \( F_{ij} \) is derived as follows:

\[ \lim_{s_i \rightarrow 0, s_i \neq 0} \left( \sum_{k=1}^{p} a_{ik} \cdot s_k \right) \left( \sum_{k=1}^{p} a_{jk} \cdot s_k \right)^{-1} = a_{ii} \cdot a_{ji}^{-1} \]  

Eqn. 6 shows that the minimum \( (a_{i1}/a_{jk}) \) of \( F_p \) is obtained when the following vector S is generated:

\[ S = (0, 0, ..., s_i, ..., 0)^T \quad i \in \{1, ..., p\} \]  

When the vector \( (0, ..., s_i, ..., 0)^T \) is present, the components of vector E are

\[ E = (e_i)^T = (a_{i1} \cdot s_j)^T \quad k \in \{1, ..., p\} \]  

and the maximum component, \( e_i \) of E is \( e_i = a_{i1} \cdot s_k, l \in \{1, ..., p\} \) as \( a_{kl} > a_{ik}, \forall l \neq k \in \{1, ..., p\} \). In this case, \( e_i > e_0, l \in \{1, ..., p\} \). Thus, \( F_{ij}^* \) exactly provides the coefficients of a B matrix when the orthogonal input vector S = (0, ..., s_i, ..., 0)^T appears, and it is then possible to find a general expression to compute a set of coefficients, \( b_{ij} \), as follows:

\[ b_{ij} = \min(e_i \cdot e_j^{-1}) = a_{ij} \cdot a_{ji}^{-1} \quad e_j > 0 \quad \forall i, j, k \in \{1, ..., p\} \]  

**Fig. 1** (a_{ij} and b_{ij}) and \( (e_i, e_j) \) planes, when \( p = 2 \)
By computing $X = B \cdot E$, the reconstructed signals $x_i$ will be $x_i = \lambda s_i n_i$, $i \in \{1, \ldots, p\}$, with $\lambda$ being a constant that depends on the $A$ matrix. Geometrically, suppose we have two sources with bounded values $s_j \in [0, s_j^M]$ and $s_k \in [0, s_k^M]$. At a given time, each pair of values is a point in the $(s_j, s_k)$ plane, and the set of all possible points forms a parallelepiped with vertices $(0, p_i, p_j, p_k, p_m)$, as shown in Fig. 1. The observed signals $e(t), e(t)$ also form a parallelepiped in the $(e_1, e_2)$ plane with vertices $(0, q_1, q_2, q_3)$, where each $S$ vertex maps onto an $E$ vertex; from eqn. 9, the coefficients of the $R_{s_1s_2}$ matrix are the slopes of the parallelepiped. If $p \geq 2$ and $s_i \in [-s_i^M, s_i^M]$, $\forall k \in \{1, \ldots, p\}$, it is possible to transform $S$ into $s_i \in [0, s_i^M], \forall k \in \{1, \ldots, p\}$, by translating the parallelepiped such that one of its vertices is at the origin, and the minimum slope is expressed, from eqns. 1 and 9, as

$$b_{ij} = \min \left[ \frac{a_{ij} s_j + \ldots + a_{ip} s_p}{a_{ij} s_j + \ldots + a_{ip} s_p} \right]$$

(10)

Fig. 2 Correcting slope of parallelepiped

Applying eqn. 10 when $p > 2$, the minimum value of $(e_1/e_2)$ (or minimum slope) may not correspond to $(a_{ij}/a_{ik})$ but rather to another coefficient ratio, as $(a_{ij}/a_{ik}, j \neq l$ (see Fig. 2). If $e_j$ and $e_l$ are the maximum values of $e_l$ and $e_j$, respectively, when a minimum of $(e_1/e_2)$ is obtained, with $e_i > e_l, l \neq j, \forall k \in \{1, \ldots, p\}$, then

$$c_k = \min \left[ e_i \right], i \in \{1, \ldots, p\}$$

(11)

and the following expression is verified:

$$b_{ij} = \min \left[ e_i \right]$$

(12)

where $r$ denotes the number of times that $e_i$ must be subtracted from $e_j$ until $e_i > e_j$. Thus, the correct coefficient ($a_{ij}/a_{ik}$) is computed and the mixing matrix $B$ is obtained.

![Figure 4 Square error of separation](image)

**Simulation results:** The validity of the procedure has been corroborated by a good many simulations. As an example, we include a simulation that uses the same sources reported by Amari et al. [2]: the first source is a uniformly distributed noise, $s_i = \sin(400t) + \cos(30t)$, and $s_i = \sin(500t + 9\cos(40t)$. Matrix $A$ was randomly generated in the interval $[-1, 1]$. With 1000 samples, and from $B$, adaptive processing was performed to reconstruct signals $x_i, x_j$ and $x_k$ as shown in Fig. 3. Fig. 4 shows the square error of each signal, coincident with crosstalk results of $c(1) = 39$dB, $c(2) = -22$dB and $c(3) = 28$dB.

**Conclusions:** The source separation method is based on geometrical considerations and is a very simple approach which does not need the estimation of statistics of any order. Convergence is fast

![Figure 3 Original, mixed and separated sources](image)

depending only on the probability of obtaining at least one point close to each of the parallelepiped edges, which means that orthogonal vectors in the source space must exist. We are currently studying the influence of added noise on the signals and the hardware implementation of the geometrical procedure.

© IEE 1997
Electronics Letters Online No: 19970557
14 March 1997
C.G. Puntonet and A. Prieto (Departamento de Electrónica y Tecnología de Computadoras, Universidad de Granada, 18071-Granada, Spain)
E-mail: carlos@casip.ugr.es

**References**


**Linearly weak keys of RC5**

H.M. Heys

**Indexing term:** Cryptography

The author examines the application of linear cryptanalysis to the RC5 private-key cipher and shows that there are expected to be weak keys for which the attack is applicable to many rounds. It is demonstrated that, for the 12-round nominal RC5 version with a 64-bit block size and a 128-bit key, there are 2^3 weak keys for which only 2^11 known plaintexts are required to break the cipher. There are 2^9 keys for which the cipher is theoretically breakable, requiring 2^25 known plaintexts. The analysis highlights the sensitivity of RC5 security to its key scheduling algorithm.

**Introduction:** RC5 [1] is a class of private-key block ciphers designed to be efficiently implemented in software by using three