

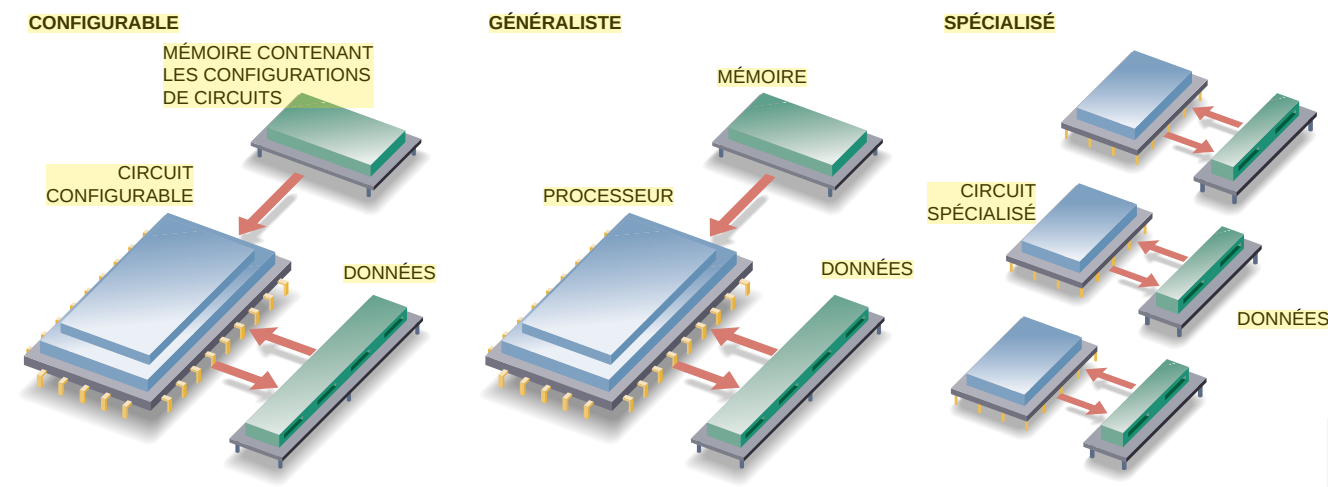
vaux –, on cherche à comparer rapidement l'image avec des milliers de modèles. Certains modèles représentent, par exemple, des véhicules vus de face ou de côté. Chaque image contient des milliers d'éléments (pixels), et la cible peut se trouver en n'importe quel point de l'image. Pour reconnaître des cibles assez rapidement, l'ordinateur doit effectuer plusieurs milliards d'opérations par seconde, car chaque pixel de l'image d'entrée doit être comparé à chacun des pixels des nombreux modèles.

Nous avons ainsi construit un système de reconnaissance dont l'électronique modifiable permet des économies substantielles de matériel en se modifiant lors de la comparaison

avec chaque modèle : comme de nombreux pixels d'un modèle ne contribuent pas à l'identification (voir la figure 4), le circuit configurable les omet simplement lors de ses calculs. Un système classique ne peut pas alléger sa tâche de façon similaire, car les pixels à ignorer diffèrent selon les modèles. On tire encore un meilleur parti des machines configurables en programmant les circuits afin qu'ils utilisent les similarités entre les modèles. Ainsi les circuits modifiables peuvent comparer en parallèle l'image d'entrée à tout un ensemble de modèles, en n'utilisant qu'une unité de comparaison pour chaque pixel dont la valeur est la même pour les modèles de cet ensemble. Par exemple, au lieu que huit

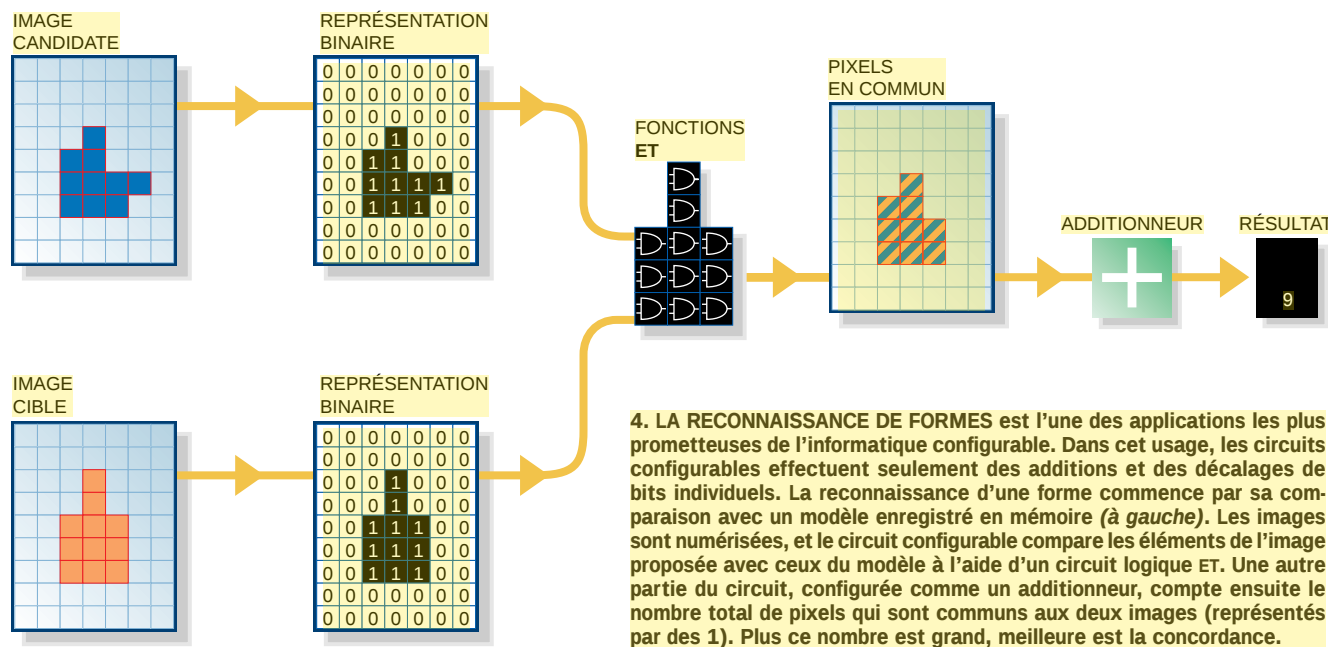
circuits distincts traitent le même pixel pour huit modèles différents, un seul circuit traite le pixel.

Récemment, nous avons mis au point un prototype de système de chiffrement utilisant de l'électronique configurable. Sur un circuit, nous avons programmé la norme de chiffrement DES (*Data Encryption Standard*), qui utilise des clés de 56 bits pour coder des blocs de données de 64 bits (en cryptographie, une clé est un nombre utilisé pour chiffrer ou déchiffrer un message confidentiel). Le chiffrement par DES procède en deux étapes : la création de sous-clés et le traitement des données. Lors de la première étape, un ensemble de rotations et de permutations de bits convertit la clé de 56 bits en une série

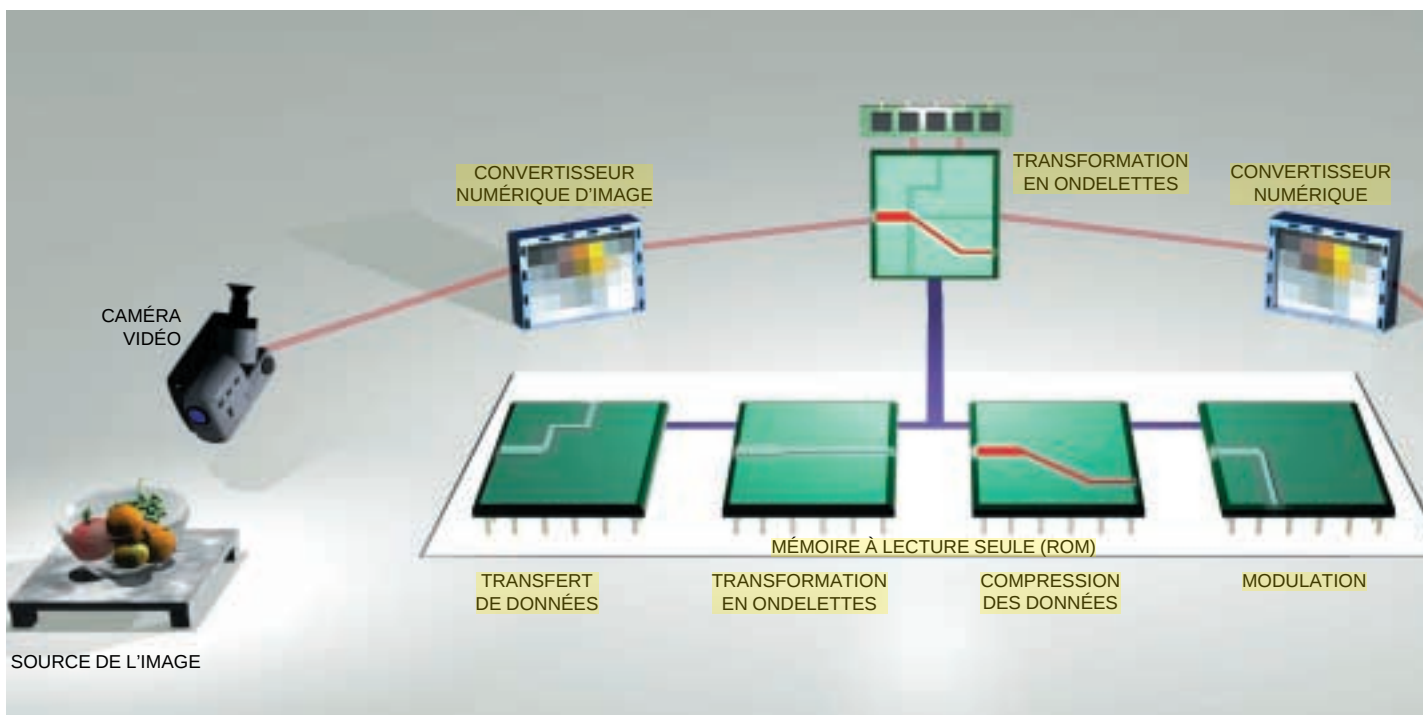


3. LES SYSTÈMES CONFIGURABLES combinent des éléments de calcul généraliste et de circuits spécialisés (ASIC). Les processeurs généralistes fonctionnent avec des circuits fixes qui exécutent les tâches définies par les programmes. Les processeurs

spécialisés ont des circuits qui les confinent à des tâches particulières ; la commande par programme est alors réduite. L'ordinateur configurable peut exécuter des commandes logicielles qui modifient ses circuits selon les tâches.



4. LA RECONNAISSANCE DE FORMES est l'une des applications les plus prometteuses de l'informatique configurable. Dans cet usage, les circuits configurables effectuent seulement des additions et des décalages de bits individuels. La reconnaissance d'une forme commence par sa comparaison avec un modèle enregistré en mémoire (à gauche). Les images sont numérisées, et le circuit configurable compare les éléments de l'image proposée avec ceux du modèle à l'aide d'un circuit logique ET. Une autre partie du circuit, configurée comme un additionneur, compte ensuite le nombre total de pixels qui sont communs aux deux images (représentés par des 1). Plus ce nombre est grand, meilleure est la concordance.



5. CE SYSTÈME PROTOTYPE de communication vidéo utilise un unique circuit configurable pour exécuter quatre fonctions qui sont normalement effectuées par des puces distinctes. Une puce mémoire conserve les quatre configurations utiles et les charge successivement dans le processeur configurable. Une première configuration permet d'abord au processeur adaptable d'acquérir des données

vidéo numériques. Puis la puce est rapidement configurée pour mettre l'information vidéo sous une forme comprimée, et modifiée encore pour préparer la transmission. Enfin, les circuits reçoivent la dernière configuration, qui leur permet de moduler et de transmettre l'information vidéo. Dans le récepteur, les quatre configurations sont appliquées dans l'ordre inverse de celui de

Calcul en temps réel

Le concept de système configurable est né simultanément aux États-Unis et en Europe, dès l'introduction des circuits logiques configurables par la Société *Xilinx*, en 1986. Le premier système couplant un microprocesseur à des circuits reconfigurables a été conçu à l'INRIA (Institut national de recherches en informatique et en automatique) en 1987.

Parallèlement, des architectures similaires ont été mises en œuvre dans les « émulateurs » de logique (*QuickTurn* dès 1987, *Hewlett-Packard* plus récemment). Ceux-ci utilisent de très grandes quantités de circuits configurables (plusieurs centaines) pour simuler des circuits intégrés avant leur fabrication. Ces émulateurs de logique, devenus indispensables pour la conception des microprocesseurs modernes, n'ont cependant qu'une seule fonction : simuler de très grands circuits. En revanche, les systèmes reconfigurables proprement dits ont des fonctions aussi diverses que celles du microprocesseur, auquel ils ajoutent des fonctions spécifiques. On a ainsi le meilleur de deux mondes : universalité du logiciel et performances du matériel spécifique à chaque application.

Le système reconfigurable *DECPeRLe1*, réalisé en 1992 au Laboratoire de recherche de la Société *Digital Equipment*, à Paris, pour le prix et le volume d'une station de travail de l'époque, détient encore aujourd'hui sept records absolus de vitesse — toutes techniques confondues, du super ordinateur au circuit intégré sur mesure. Ce système

est le plus performant pour le codage et le décodage par la méthode de chiffrement à clés publiques RSA. Le même système reste le seul à répondre aux besoins d'acquisition et de filtrage de données en temps réel exprimés par le CERN pour son futur accélérateur de particules (LHC). Des performances de calcul en temps réel équivalentes à celles de ce système configurable s'obtiendraient avec un ordinateur classique au prix d'une multiplication par 100 des fréquences d'horloge les plus élevées.

Par leur souplesse et le nombre de connexions potentielles (on peut faire sortir directement des centaines de fils de ces circuits), les systèmes reconfigurables sont d'excellentes interfaces entre les ordinateurs et des dispositifs externes variés. Dans le cas d'une caméra numérique à haute résolution, telle celles de l'astronomie ou de l'imagerie médicale, on y programme à la fois l'interface, le protocole de communication, et aussi les fonctions de filtrage de l'image et l'adaptation du débit des données reçues par l'ordinateur hôte. On obtient ainsi un système d'acquisition optimal, qui peut s'adapter aux évolutions des caméras ou aux besoins d'acquisition par simple reconfiguration. C'est à travers des applications de ce type que les systèmes reconfigurables sont aujourd'hui passés du stade de la recherche à celui de produits industriels.

Jean VUILLEMIN, École normale supérieure
Patrice BERTIN, École des mines de Paris