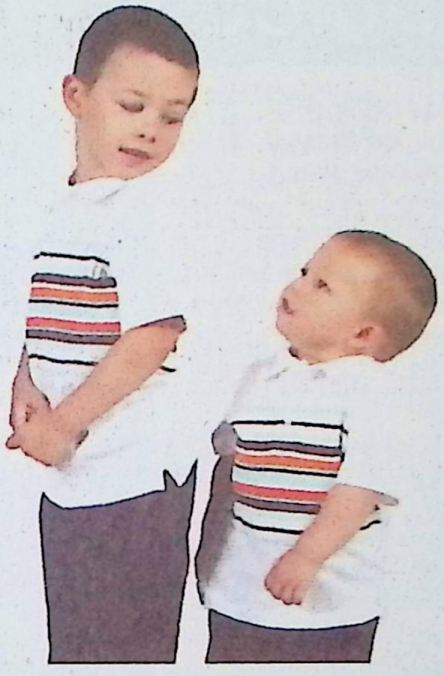
# Mothers See Their Youngest as Shorter Than They Are

Many parents say when their second child is born that their first child suddenly appears to have grown overnight. Now, researchers reporting in the Cell Press journal *Current Biology* on December 16 have an explanation: until the birth of the new child, those parents were subject to a "baby illusion," routinely misperceiving their youngest child as smaller (and younger) than he or she really was.

Researchers at Swinburne University of Technology in Australia made the discovery first by asking 747 mothers if they remembered experiencing a sudden shift in their first child's size after the birth of a new infant. The researchers found that 70% of the mothers did.

To further explore that perceptual shift, the researchers asked mothers to estimate the height of one of their young children (aged 2 to 6) by marking a blank wall. When the researchers compared those height estimations to the child's real height, they found something very interesting: mothers significantly underestimated the height of their youngest child by 7.5 cm on average. In contrast, height estimates for the eldest child were almost accurate.

The findings are a useful reminder of just how



filtered our own perceptions of the world around us can be. Researchers concluded that in many cases, we cannot rust the accuracy of our perceptions.

# Inkblots Improve Security of Online Passwords

Carnegie Mellon University computer scientists have developed a new password system that incorporates inkblots to provide an extra measure of protection when, as so often occurs, lists of passwords get stolen from websites.

This new type of password, dubbed a GOTCHA (Generating panOptic Turing Tests to Tell Computers and Humans Apart), would be suitable for protecting high-value accounts, such as bank accounts, medical records and other sensitive information.



The GOTCHA password system developed at Carnegie Mellon University incorporates randomly generated inkblots (Courtesy: Carnegie Mellon University)

To create a GOTCHA, a user chooses a password and a computer then generates several random, multi-colored inkblots. The user describes each inkblot with a text phrase. These phrases are then stored in a random order along with the password. When the user returns to the site and signs in with the password, the inkblots are displayed again along with the list of descriptive phrases; the user then matches each phrase with the appropriate inkblot.

These puzzles would prove significant when security breaches of websites result in the loss of millions of user passwords -- a common occurrence that has plagued such companies as LinkedIn, Sony and Gawker. These passwords are stored as cryptographic hash functions, in which passwords of any length are converted into strings of bits of uniform length. A thief can't readily decipher these hashes, but can mount what's called an automated offline dictionary attack. Computers today can evaluate as many as 250 million possible hash values every second.