Have-you-seen...

(Continued from page 1)

Banks want to transfer sums of money without the money being diverted by intruders. The users of an ATM machine want assurance that their transactions are private.

On the other hand, in the case of the (machine readable) zipcode or barcodes, the goal for the code is not to hide information but to speed or track information. Thus, the universal product code serves the dual function of allowing the customer to get out of a supermarket faster, and the store that sold the item to keep inventory on what it sells. This makes it more likely that your favorite store will have your favorite cereal in stock.

The codes used for the information in pictures from Saturn or for the information on a compact disc serve yet another function. These codes are there to correct or detect errors which might occur due to a solar flare during transmission of a picture or due to a speck of dust on the compact disc. (See the example discussed at the right.)

Another recent use of code technology has been in compressing sounds, text (files), and pictures. When television pictures are sent through a cable or a text file is sent electronically from one place to another, the information is represented by a gigantic number of 0's and 1's. Since English has great redundancy and since pictures have a limited number of gray levels, it becomes feasible to use a code that allows faster transmission but that also allows perfect reconstruction of the original.

Finally, codes are being used to synchronize information. Thus, sound and image, recorded separately at a live concert, must be combined for natural viewing.

One of the major tools in the design of new codes for secrecy is the theory of numbers, the subject that the pacifist number theorist G.H. Hardy prided himself for being a researcher in because he felt it could never be put to use. Today number theory is the key to dramatic improvements in what crypt-systems can accomplish. More than ever before the hand-in-hand relationship between mathematics being developed for no specific purpose and applicable mathematics is being demonstrated.

Error-Correction

How can one send a picture back from a distant planet? Imagine that the image to be sent (see box on page 1) has been divided into a grid involving, for simplicity, five rows and five columns. The gray level of each of the 25 cells can now be recorded and a binary code used to represent each gray level.

For simplicity, we have used only two gray levels, black and white. If black is represented by the code word 1 and white by the code word 0, the original image on page 1 can be transmitted as the following sequence of 25 zeros and ones:

0000001110000100111000001

However, if any noise occurs during transmission, which results in zeros and ones being interchanged, the result is that the original image is reconstructed improperly. Richard Hamming pioneered the development of codes to correct errors. A simple example of such a code is to use the code word 111 for black and the code word 000 for white. If no more than one error is made in the transmission of each code word then the code allows accurate restoration of the original image. For example, although a number of errors have been made in transmission, the following sequence can be decoded as the original picture on page 1.

0000001000100000000111111
1100010001000011100010000
1111111010100000001001000 11

The basic idea that Hamming had was that if a code word can not be transformed into another code word by fewer than 2s+1 digit changes, then the code will be able to correct s errors. In our example, the code requires 3 changes to transform one word to another so 1 error can be corrected.

References:

1. *Andrews, E.,* ***Method To Speed Up Compression Of Data,*** *NY Times, Sept. 21, 1991, v.141 p. 16(N).* An account of a recently awarded patent which speeds up the compression of data.
2. *Fisher, L.,* ***Yes, CD Sound Is "Perfect".*** *... NY Times, Oct. 25, 1992, v.142 p. F10(N).* Description of a new data compression technique for audio compact discs.
3. *Fleisschmann, M.,* ***More-accurate CDs;*** *Normile, D.,* ***Dazzling Shows Debut New Audio and Video,*** *Popular Science, (v. 242, no. 2), February 1993, pg. 28-29.* An account of how new advances in compression techniques will make possible better quality sound and images in the near future.
4. *Healey, B.,* ***How To Decipher Those Rather Simple Symbols.*** *NY Times, Jan. 28, 1990, v. 139, p. 22(n).* Bar codes in philately (stamps) column.
5. *Markov, J.,* ***A Public Battle Over Secret Codes,*** *NY Times, May 7, 1992, v. 141 p. C1 (N).* An account of feuding between the government and business over the regulation of encryption techniques.

(Continued on page 9)