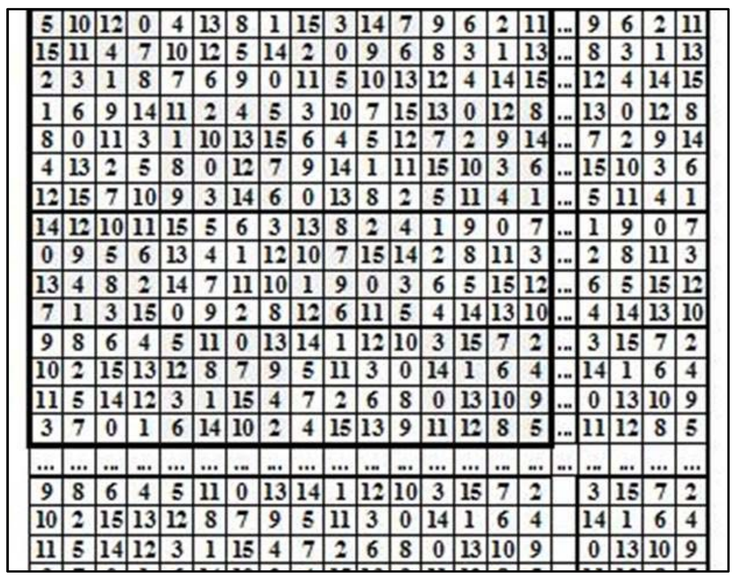
Image Steganography Using Sudoku

Samuel Wagstaff and Vaishnavi Chandrasekaran
Department of Computer Science, Purdue University

Overview

An image sharing scheme that encodes the secret image without altering the image size or requiring any additional information is proposed. The scheme ensures that the fidelity of the revealed secret data is distortion free and also possesses reversible characteristics providing for the retrieval of the host image as well.

The system uses the concept of Sudoku to conceal the shadow with reversibility. Given a secret image, the system derives shadows from the secret image and produces *n* shadow images. Given any *t* out of *n* shadow images along with the corresponding key values, the involved participants can losslessly reconstruct the secret and the original host image.



Shadow Derivation

1. A matrix M of the size of the host image is created consisting of Sudoku grids with the size of 16x16
2. The secret bit stream S is converted into base-16 numeral system digits.
3. An invertible polynomial F(x) is formulated

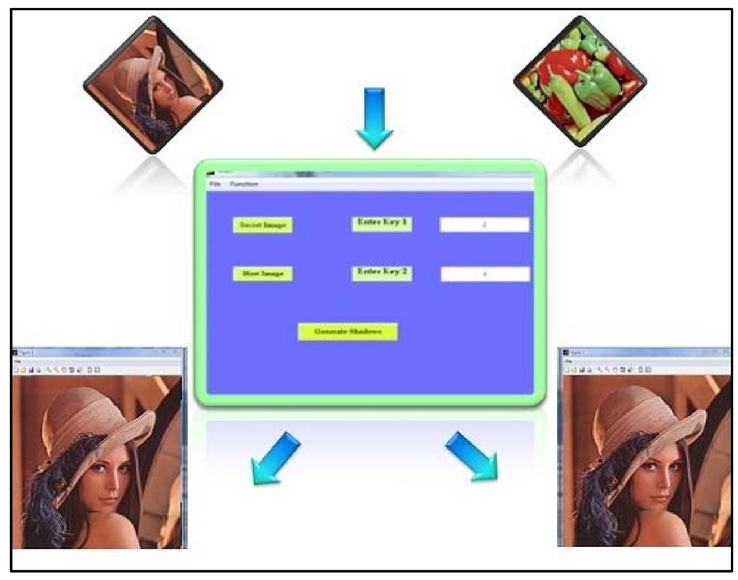
$$F(x)=(m+ s_1x^1 + s_2x^2 + ... + s_{t-1}x^{t-1}) \bmod 16$$

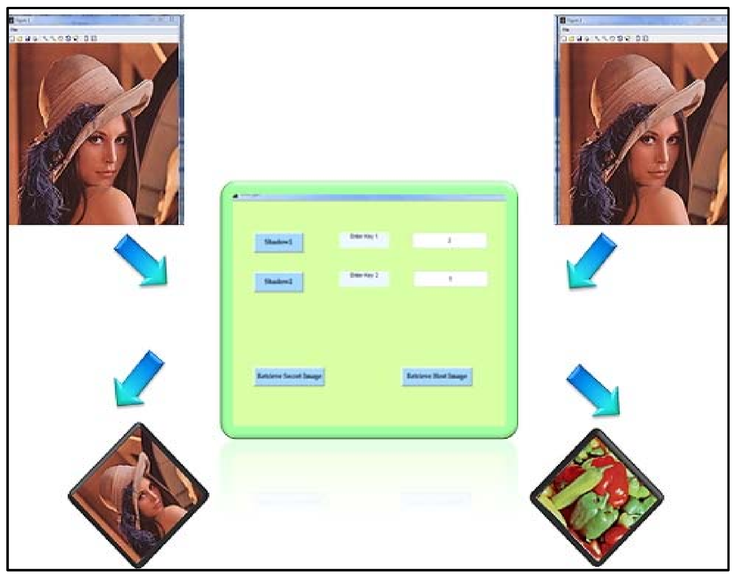
$$m=M(ga,gb)$$

4. *n* shadows are generated by feeding the secret keys K_i into F(x) to obtain y_i

Encryption

1. From the located Sudoku block of the original pair at the matrix, there are 16 digits ranging from 0 to 15.
2. To embed the R values: The new embedded pair (ga_i,gb_i) is obtained by selecting the corresponding shadow in the same Sudoku block as that of (ga, gb).
3. To embed the G values: The new embedded pair (ga_i,gb_i) is obtained by selecting the corresponding shadow in the same Sudoku row as that of (ga, gb).
4. To embed the R values: The new embedded pair (ga_i,gb_i) is obtained by selecting the corresponding shadow in the same Sudoku column as that of (ga, gb).
5. The shadow derivation and camouflage phases are repeated to generate and camouflage all the secret shadows into the host pairs to obtain *n* shadow images, which are distributed along with the keys.





Decryption

1. Given any *t* out of *n* shadow images and the keys from the involved participants, the secret image and the lossless host image can be reconstructed.

2. To extract the (t-1) secret digits and restore the original pixel pair, the polynomial F(x) is derived from the *t* pairs using the Legrange's interpolation formula.