STEGANOGRAPHY: APPLICATIONS OF SINGULAR VALUE DECOMPOSITION

Olin College of Engineering, Spring 2015

David Abrahams, Annabel Consilvio, Hannah Fowler

BACKGROUND OF STEGANOGRAPHY:

Steganography is the process of concealing a message, image, or file in another message image, or file. Whereas cryptography involves sending information through clearly encrypted messages, information sent through steganography is imperceptible. Information is sent through making small changes to the original file, invisible to anyone not looking for an encrypted message.

UNDERSTANDING SVD

Singular value decomposition is the factorization of a matrix into two eigenvalue matrices and a corresponding eigenvector matrix. Decomposing matrices has applications in fitting of data, matrix approximation, data embedding, and other fields. The following is an qexample of how we can SVD the matrix.

1. Take matrix *A* of size *m x n*
2. Find its transpose A^T of size *n x m*
3. Define an *n x n* matrix *V* whose columns are orthonormal eigenvectors of A^TA, in order of descending eigenvalue from left to right
4. Define matrix *U* whose columns are composed by the following:
   - a. $u_i = \frac{Av_i}{\sqrt{\lambda_i}}$
   - b. Ensure that the each column is an orthonormal eigenvector of AA^T
5. Define the *m x n* matrix Σ, composed of the nonzero eigenvalues, λ_i, placed diagonally in descending order.
6. $A = U\Sigma V^T$ should be true

$$A = U\Sigma V^T$$

A matrix such that each column is an eigenvector of AA^T. The dominant eigenvector is the first column.

A matrix consisting of the squareroot of the eigenvalues along the diagonal in decreasing value.

A matrix such that each column is an eigenvector of A^TA. The dominant eigenvector is the first column.

USING SVD FOR STEGANOGRAPHY

EMBEDDING

1. Operate on bits of message to make them signed. i.e., *m* = 0110101 -> *p* = -1 1 1 -1 1 -1 1
2. Divide the image into *r* blocks, where each block's pixel values are embedded into matrix *A*.
3. Decompose *A* into $A = U\Sigma V^T$
4. Keep the first column of *U* the same
5. Embed the signs of *p* into the second column of *U* by making the elements $\hat{u}_{i,j} = p_r|u_{i,j}|$
6. Set the final element of column 2 of *U* to the value that makes columns 1 and 2 orthogonal.
7. Proceed embedding signs into subsequent columns, ensuring all columns remain orthogonal (we do not embed signs into the final two elements of column 3, the final three elements of column 4, etc.)
8. Create the new image out of blocks defined by $\hat{A} = \hat{U}\Sigma V^T$

EXTRACTING

To extract a message, one must first divide the image into a known number of blocks. For each block, compute the SVD such that $A=U\Sigma V^T$.Looking at the signs of each element of each column, we can interpret the binary message. For example, if the column is $u2$ =(3 -4 15 38 7 -46 9 6)^T, then the binary message is 011101.

1. Divide the image into n blocks
2. Compute singular value decomposition $A = U\Sigma V^T$
3. For example: $u_2 = (\ 3 \quad -4 \quad 15 \quad 38 \quad 7 \quad -46 \quad 9 \quad 6\ )^T$

EXAMPLE

Original Image:

Embeded Image:

Original Message:

a. **"Singular value decomposition is amazing! Just like Sarah"**

Recovered Message:

a. **"]S 4i 7n 3g :u 6l 0a 9r ;v 0a 6l :u 2e 2d 2e 1c 7o 6m 8p 7o 9s 4i :t 4i 7o 7n 4i 9s 0a 6m 0a =z 4i 7n 3g ! %J :u 9s :t 6l 4i 5k 2e]S 0a 9r 0a 4h."**

The difference seen here between the embedded message and the recovered message is caused by using different binary encoders and decoders. This is a common occurance since steganography does not reveal which encoder was originally used.

BEYOND THE BASICS

1. **Columns Protected** - Determines which columns of *U* not to edit, saves most important information
2. **Redundancy -** Number of times message is embedded into the image
3. **Block Size -** Determines number of blocks image is split into, more blocks = smaller message = less distortion

REFERENCES

"Jeremiah Denton, Ex-senator and Vietnam POW Who Blinked "torture" in Morse Code, Dies at 89." *CBSNews*. CBS Interactive, n.d. Web. 29 Apr. 2015.

SarasioMeyer, Daniel. "Steganography and SVD." (2008): n. pag. 2008. Web. 29 Apr. 2015.

"Secret Code in Color Printers Lets Government Track You." *Electronic Frontier Foundation*. N.p., 17 Oct. 2005. Web. 29 Apr. 2015.

Wengerhoff, Daniel, "Using the singular value decomposition for image steganography " (2006). Retrospective Theses and Dissertations. Paper 1388.