High Capacity Image Steganography based on Discrete Wavelet Transform and Singular Value Decomposition

Mansi S. Subhedar
Research Scholar
Department of Electronics & Telecommunication
B.D.College of Engineering & Technology
Sevagram, Wardha - 442102
Maharashtra, India
mansi_subhedar@rediffmail.com

Vijay H. Mankar
Department of Electronics & Telecommunication
Government College of Polytechnic
Nagpur - 440001
Maharashtra, India
vhmankar@gmail.com

ABSTRACT

Steganography plays very significant role in the field of information hiding for secret communication. It is a covert communication to hide secret data in cover media (e.g. text, audio, video, image etc). Security, high embedding capacity and imperceptibility are the key points to design an efficient steganographic algorithm. We propose a novel technique to embed secret information in cover image based on discrete wavelet transform (DWT) and singular value decomposition (SVD). The algorithm modifies singular values of HH band of cover image by that of secret image. Singular values possess intrinsic algebraic properties and exhibit good stability that enables us to hide secret information without degrading the perceptual quality. Furthermore, experimental results show robustness against various image processing and geometric attacks.

Keywords

Image steganography, discrete wavelet transform, singular value decomposition, image quality

1. INTRODUCTION

Information security is a challenging task due to widespread use and growth of internet and multimedia usage. Transmission and reception of secret information is carried out frequently over public communication channels. Due to weakness of human visual system (HVS) and cheaper options available for image storage, communication & processing, image steganography has become popular way of secret communication. The word steganography has been derived from two Greek words, 'stegos' means cover and 'grafia' means writing, defining it as "covered writing". The concept of steganography is usually modelled by the prisoner's problem [15] and is one of the branches of information hiding. The traditional way of information security includes encryption of secret information i.e. cryptography, a method of secret writing. The main aim of cryptography is to hide the information whereas steganography aims at hiding the existence of the secret message [9] - [16]. Images have been extensively used as means for hiding secret information as they possess high degree of redundancy. Any small perturbation in image will not alter the visual quality much and therefore it will not draw eavesdropper's attention to suspect about hidden information embedded in image [4]. Steganography may be used for both legal and illegal purpose i.e. common man may use it to convey some important private information while terrorist may use it to exchange some terroristic data. Watermarking is another branch of information hiding; though looks similar to steganography, it works on different grounds. In case of watermarking, the goal of user is to embed the watermark so that ownership can be proved where as in steganography it's to hide the information so that one can not detect it. In watermarking, the goal of attacker is to remove the data whereas in steganography it's to detect the data. Steganography is used for secret communication, whereas watermarking find applications like content protection, copyright management, content authentication and tamper detection. Security, embedding capacity and imperceptibility are the major requirements to be considered while designing the algorithm for steganography [8]. Regarding the terminology used here, the term cover image is used to describe the image designated to carry secret information; embedded data is known as payload. Secret image is the secret information to be embedded in cover. Stego image is the image generated after embedding process and extracted image is the image retrieved at receiver side from stego image.

In this paper, we developed DWT-SVD based image steganography in which secret information is embedded in singular values of HH band obtained by DWT decomposition of cover. It has been proved that the developed embedding mechanism holds high degree of imperceptibility and is capable of withstanding against geometric attacks and various distortions. The organization of the paper is as follows: section 2 gives basic working principle of image steganography and related work. Section 3 illustrates discrete wavelet transform. Section 4 explains significance of singular value

ICTCS'14, November 14-16 2014, Udaipur, Rajasthan, India
Copyright 2014 ACM 978-1-4503-3216-3/14/11 $15.00 http://dx.doi.org/10.1145/2677855.2677918

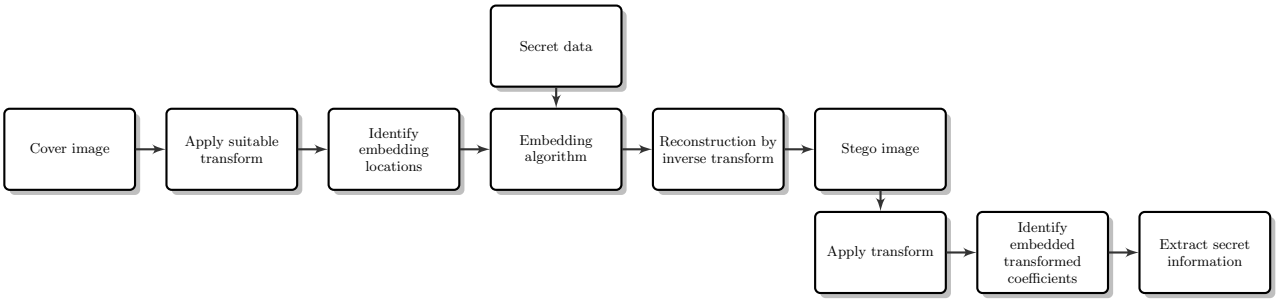


Figure 1: General model of transform domain image steganography

decomposition in image steganography. Section 5 demonstrates the working principle of the proposed algorithm. Section 6 present the experimental results and section 7 concludes the paper.

2. RELATED WORK

Image steganography is a method of covert communication i.e. embedding secret information in cover image. It can be broadly classified into spatial domain and transform domain steganography schemes. In spatial domain, secret information is embedded in pixel values of cover image. These schemes offer simplicity and are easy to implement as pixel values of cover are directly replaced by that secret information. However, they are prone to image processing operations such as scaling, rotation, cropping etc. Any perturbation made may reveal presence of secret information and are therefore not reliable [7]- [12]. On the other side, transform domain techniques achieve better results as they embed secret information in transform coefficients of cover rather than the pixel values directly. Hence, they ensure good imperceptibility and robustness leading to least detectable stego as compared to spatial domain schemes. Transform domain image steganography is the scope of this study. We developed conceptual framework for transform domain image steganography as shown in Fig. 1.

At the transmitter, select the cover and secret information to be embedded. Decompose the cover with the help of suitable transform and obtain transform coefficients. Identify changeable coefficients. Modify the suitable transform coefficients with secret information using desired embedding mechanism and reconstruct the stego image. At the receiver, decompose the stego image. Observe the modified coefficients and extract the hidden information from them. When stego is being passed through insecure channel, it may suffer from undesired attacks and intruder may try to detect or destroy the secret. These attacks can include geometric transformations i.e. arbitrary displacement of some or all the pixels, various distortions like addition of noise etc. The embedding algorithm should be designed in such a way that, it should resist the attacks and remains undetectable.

In order to implement transform domain steganography, a variety of transforms can be used including discrete cosine transform (DCT), discrete wavelet transform (DWT), Hadamard transform, slantlet transform, contourlet transform etc. Choice of transform depends on application and desired capacity requirements. In early days, DCT was more popular due to wide use of JPEG file format on internet. DCT is a block based approach; image is divided into blocks of size 8×8 and then DCT is computed for each block. This approach relies on the assumption that the blocks chosen for obtaining DCT are independent. This unrealistic assumption, makes use of DCT very much limited. With the development of JPEG2000, usage of DWT was explored much and now many other transforms are used in steganography, information hiding and a variety of other image processing applications.

In literature, several DWT based steganography schemes are presented. In [11], DWT based image steganography is presented. Embedding is carried out in HH, HL, LH bands. It has been proved that embedding in diagonal detail coefficients gives better PSNR values. However, PSNR values are very poor suggesting lack of imperceptibility. K. Suresh Babu et al. presented SVD based image steganography in [3]. Secret message is embedded in singular values of cover image. The quantization value is used as secret key and is must to retrieve the payload. Though authors claim high payload capacity, there is much scope for improvement in PSNR and robustness. In [10], K.B. Shivakumar et al. presented block based approach using DWT and integer wavelet transform (IWT). The cover image is divided into blocks of 4×4 each and DWT is applied on each block. In the resulting DWT coefficients, blocks of vertical band of 2×2 each are considered and IWT is applied to get blocks of 1×1 each. The IWT is applied on vertical band of DWT of payload to generate coefficients of payload and are embedded into IWT coefficients of cover image using least significant bit (LSB) replacement method. Error detection and correction coding is also employed. The method seems to be very much complex and hence time consuming. Robustness to attacks is also not justified properly. Abdallah, H.A. et al. proposed steganography scheme based on SVD wherein left singular vectors are used to embed secret information. The authors tried to reduce the embedding errors while maintaining the image fidelity [1]. In [2], combination of DCT and IWT is preferred to embed secret in cover by using Munkres' assignment algorithm. In [5], an idea is proposed by Prabakaran et al.; DWT is performed on both cover and secret image followed by alpha bending operation. Arnold transformation is also employed to scramble secret image.

There are many significant contributions in field of image steganography in transform domain, though not mentioned here. Each of them tries for the undetectable stego image and robustness to attacks while maintaining high payload capacity.

3. DISCRETE WAVELET TRANSFORM

Discrete wavelet transform is an important tool to compress, transmit and analyse images. Unlike the Fourier transform, whose basis functions are sinusoids, wavelet transforms are based on small waves called wavelets of varying frequency and limited duration. Fourier transform gives frequency domain representation whereas DWT provides time - frequency representation. Multiresolution theory is the basis of wavelet transform i.e. representation and analysis of signals at more than one resolution [13]. DWT decomposition of image results in four subbands. They are called as approximation component (LL), horizontal component (HL), vertical component (LH) and diagonal detail (HH) where the first letter represents whether it is low pass (L) or high pass (H) filtered along the columns (vertical direction) and the second letter represents whether the low pass or high pass filtering is applied along the rows (horizontal direction). The signal is low pass filtered with $H_0(z)$ and $H_1(z)$ indicates high pass filtering that yields detail signal. The transfer functions of the filter are given by,

$$H_o(z) = \frac{1}{2}(1 + (z - 1)) \tag{1}$$

$$G_o(z) = 1 + z \tag{2}$$

$$G_1(z) = \frac{1}{2}(z - 1) \tag{3}$$

$$H_1(z) = \frac{1}{z} - 1 \tag{4}$$

Wavelet transform offers a multiscale and time frequency-localized image representation. The wavelets provide a sparse representation for piecewise smooth signals due to which wavelets are used in many signal processing applications. Advantages of DWT include better energy compaction than DCT without any blocking artefact after coding. It's multiresolution nature makes it suitable for scalable image coding. High resolution subbands help to easily locate edges and texture patterns in an image.

Lowest sub band has the most important and relevant information and the HH subband contains ïňĄne details. It contributes insignificantly to image energy and hence modifications made to this subband while embedding the secret information will not affect the perceptual quality of an image significantly. As, HVS fails to identify these modifications, it is the most suitable embedding location to hide secret information. We have chosen only HH band of cover for embedding purpose.

4. SINGULAR VALUE DECOMPOSITION

SVD is one of the most important analysis tools in linear algebra and is specially used for the analysis of matrices. It is related to the theory of diagonalizing a symmetric matrix in which a matrix can be decomposed into three sub matrices, U, S and V^T. U and V are orthogonal square matrices and S is rectangular diagonal matrix. Any real matrix A can be represented as,

$$A = USV^T \tag{5}$$

$$A = \begin{bmatrix} u_{1,1} & .. & u_{1,N} \\ ... & .. & ... \\ u_{N,1} & ... & u_{N,N} \end{bmatrix} \begin{bmatrix} \sigma_1 & .. & 0 \\ ... & .. & ... \\ 0 & .. & \sigma_N \end{bmatrix} \begin{bmatrix} v_{1,1} & .. & v_{1,N} \\ ... & .. & ... \\ v_{N,1} & ... & v_{N,N} \end{bmatrix}$$

Table 1: Singular Values for Cover Images

Image	Lena	House	Tiffany	Peppers	Jet plane
Max	272	113	293	766	277
Min	0	0	0	0	0

The columns of U are eigen vectors of AA^T; columns of V are eigen vectors of A^TA; D is diagonal matrix that consists of non negative, real values called singular values arranged diagonally in descending order such that $\sigma 1 \geq \sigma 2 \geq \ldots \geq 0$. Singular values can be calculated as square roots of eigen values. Some of the important mathematical properties of SVD include:

1. Size of the SVD matrices is not fixed; it can be square or rectangular.
2. Singular values are unique and the rank of matrix A is equal to the number of it's non zero singular values.
3. Every real matrix A and it's transpose A^T have the same non-zero singular values.
4. Few singular values represent large portion of signal energy.
5. Each singular value represents the luminance of image while the corresponding singular vectors specify the geometry of image.
6. Singular values possess intrinsic algebraic properties and have very good stability.
7. Any small change made to image will not affect it's singular values significantly.

Due to extensive mathematical properties mentioned above and stability against certain image processing operations, SVD is the most popular tool that can be used in applications like steganography, watermarking, image compression, recognition systems etc [6]. Table 1 shows the singular values of HH band of cover images used in this paper.

5. PROPOSED WORK

We propose image steganography scheme based on combination of DWT and SVD. As explained in previous sections due to inherent benefits of DWT and algebraic properties of SVD, this scheme results in a high degree of imperceptibility and robustness. The cover image used to embed secret image is first decomposed into four subbands using DWT. As HH band contains the finer details and contributes insignificantly to image energy, alterations made to HH band will not affect the visual quality of cover. Hence, it is opted for embedding secret information.

Any image is basically a matrix of non negative scalar values hence SVD can be applied to process digital image. Before the actual embedding process, coefficients of HH band are further decomposed in a set of uncorrelated coefficients and

then the embedding is carried out. A stepwise approach for embedding and extraction algorithm is presented below:

Embedding algorithm:

1. Obtain one level DWT decomposition of cover image and secret image that results into four subbands.
2. Decompose HH band of cover image and secret image into set of uncorrelated coefficients.
3. Replace the singular values of HH band of cover by that of secret image.
4. Apply inverse DWT to reconstruct stego.

Extraction algorithm:

1. Decompose stego image generated after embedding secret image.
2. Apply SVD.
3. Construct the secret image by combining the singular values with the orthogonal matrices of secret image.

6. EXPERIMENTAL RESULTS

Experiments are carried out to test and analyse the image steganography algorithm in Matlab environment. We have used five gray scale images Lena, House, Tiffany, Peppers, Jetplane of size 512×512 as cover and cameraman image of size 512×512 as the secret. We have verified the algorithm on two different grounds i.e. imperceptibility and robustness. The algorithm performed well in terms of both subjective and objective criteria. Fig. 2 (a) and (b) shows comparison between test image 'Lena' and corresponding stego image generated after embedding secret. The extracted secret image 'cameraman' obtained by extraction algorithm is also shown in Fig. 2 (c).

Stego image should not reveal the presence of secret information. If the quality is deteriorated, it may easily drag the eavesdropper's attention and attacks may be applied either to detect the secret image or to destroy it.

6.1 *Check for Invisibility*

Fig. 3 depicts the histogram match for cover and stego image shown in Fig. 2. A variety of parameters is discussed in literature to judge the image quality. In this paper PSNR, RMSE, MSSIM, FSIM (Feature similarity index) [17] -[14] and normalised cross correlation (NCC) are used to verify the invisibility of stego image. Table 2 shows these values for all the test images.

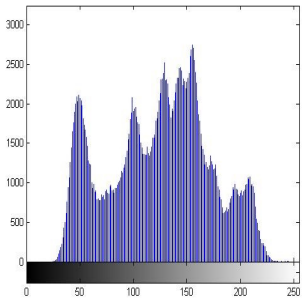
The maximum value obtained for PSNR is 50.55 dB for cover image house and minimum value is 44.66 dB for cover image peppers. The value of NCC is 0.999 and value of FSIM is 1 for all cover images suggesting validity of the proposed method.

(a) Cover Image

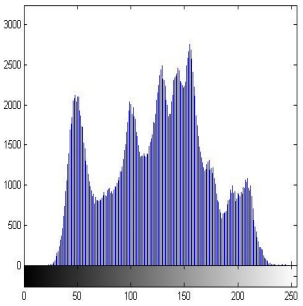
(b) Stego image

(c) Secret Image

Figure 2: (a) Cover image (b) Stego image (c) Extracted secret image



(a)



(b)

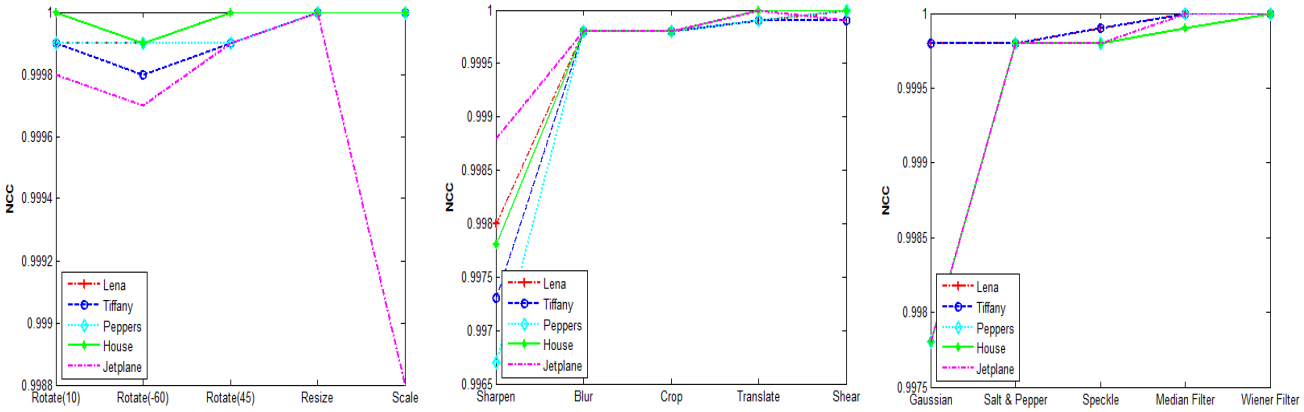
Figure 3: (a)Histogram for Cover-Lena (b) Histogram for Stego

(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 4: a) Stego images under various attacks a) Blur b) Sharpen c) Histogram Equalisation d) Gaussian Noise e) Salt and Pepper Noise f) Speckle Nosie g) Median Filter with 3×3 mask h) Wiener Filter with 5×5 mask



(a) (b) (c)

Figure 5: Performance of proposed scheme under various attacks a) Rotate by 10, -60 and 40, Resize, Scale b) Sharpen, Blur, Crop, Translate, Shear c) Gaussian noise, Salt and Pepper noise, Speckle noise, Wiener filter and median filter

Table 2: Performance parameters for proposed method

Image	PSNR	RMSE	MSSIM	NCC	FSIM
Lena	49.33	0.8706	0.9967	0.9998	1
House	50.55	0.7567	0.9969	0.9999	1
Tiffany	47.32	1.0976	0.9950	0.9993	1
Peppers	44.66	1.4907	0.9868	0.9996	1
Jetplane	53.95	0.5117	0.9993	0.9999	1

Table 3: Comparison of PSNR values for various attacks

Attack	Gaussian Noise	Median Filter	Sharpen	Hist. Equalization	Gaussian Blur
Algorithm in [11]	26.67	28.47	16.17	19.13	26.32
Proposed Scheme	28.79	36.62	22.50	20.66	22.40

6.2 *Robustness to Various Attacks*

Robustness to attacks is one of the major requirements that separates the field of steganography from similar branches of data hiding like cryptography and watermarking. We investigated the performance of the proposed scheme for various global geometric attacks on all the five cover images. Fig. 4 shows the stego image for Lena under various attacks.

Correlation coefficient suggests the degree of similarity between original and extracted secret image. It's value lies between -1 and 1. If two images are exactly identical, the value will be 1; if they are completely opposite, the value will be -1. The value will be 0 if two images are uncorrelated. It can be calculated using Eq.6.

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{i,j}-\mu_c][S_{i,j}-\mu_s]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[(C_{i,j}-\mu_c)^2]}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[(S_{i,j}-\mu_s)^2]}} \quad (6)$$

where $C_{i,j}$ represents cover image, $S_{i,j}$ is the stego image, μ_c & μ_s is the value of mean for cover and stego image respectively.

Stego under attack is used further for extraction purpose. The NCC values between extracted secret and original secret are computed for all cover images and are summarized in Fig. 5. The stego image is resized to 1024×1024 and back to 512×512 using bicubic interpolation. Addition of noise is very common attack in image processing applications. Noise may get added during transmission of stego image through public channel. Here, three different types of noise with various magnitudes are added to stego image. Fig. 5 illustrates the effect on NCC values for Gaussian noise with zero mean and variance of 0.01, Salt and Pepper noise with noise density of 0.01 and speckle noise of density 0.4. The values are found to be in range 0.9998 to 0.9999.

Stego image is rotated by various angles and is used further for extraction of secret. Rotation by 45° results in NCC value very close to 1. Similarly the results are computed for shearing, sharpening, translation etc. The stego image is blurred, cropped and intensity transformed and NCC values are verified and found to be very close to 1. It is evident from Fig. 5 that for almost all cases the value of NCC is near to 1 indicating high degree of robustness.

We also compared the proposed method with results obtained in [?] and [11]. In these papers, the highest value of PSNR for stego image is 39.8441 dB for cover image lily and 30.7849 dB for cover image peppers. Table 3 shows the comparison of proposed scheme with these two methods. Cover image employed is peppers; however secret images used for

embedding in two algorithms differ. In our algorithm, for all the cover images, PSNR value is much higher not only for these two methods but also for many traditional DWT based image steganography schemes.

7. CONCLUSION

In this paper, we proposed hybrid DWT-SVD based image steganography scheme. Due to intrinsic algebraic properties of SVD and very good stability of singular values against image processing operations, use of SVD was preferred. It has been clear from PSNR, RMSE, MSSIM, FSIM and NCC values between cover and stego image that our scheme achieves high imperceptibility. We investigated the performance when stego was subjected to variety of attacks like addition of noise, resizing, scaling, translation, sharpening, blurring, cropping, histogram equalization etc. Attacked stego was further used for extraction purpose and NCC among original and extracted secret was computed. NCC values illustrate that the proposed scheme survived in the presence of these attacks. For almost all attacks, the normalised cross correlation almost equals one and validates the proposed algorithm.

8. REFERENCES

[1] H. Abdallah, M. Hadhoud, and A. Shaalan. An efficient svd image steganographic approach. *International Conference on Computer Engineering & systems,*, pages 257–262, 2009.

[2] R. N. M. A.M.E. Digital image steganography based on assignment algorithm and combination of dct-iwt. *International conference on computational intelligence, communication system and networks*, pages 295–300, 2012.

[3] K. S. Babu, K. B. Raja, U. M. Rao, R. K. A, V. K. R, and L. M. Patnaik. Robust and high capacity image steganography using svd. *IET UK International Conference on Information and Communication Technology in Electrical Sciences*, pages 718–727, 2007.

[4] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt. Digital image steganography: survey and analysis of current methods. *Signal processing*, 90:727–752, 2010.

[5] P. G. and B. R. A modified secure digital image steganography based on discrete wavelet transform. *International conference on computing, electronics and electrical technology*, pages 1096–1100, 2012.

[6] V. Gorodetski, L.J.Popyack, V.Samoilov, and V.A.Skormin. Svd based approach to transparent embedding data into digital images. *Int. Workshop on Mathematical Methods, models and Architecture for Computer Network Security*, 2052:263–374, 2001.

[7] P. V. S. Han and C. E. A survey of digital image watermarking techniques. *Industrial Informatics INDIN 05*, pages 709–716, 2005.

[8] I. J.Cox, M. L.Miller, J. A. Bloom, J. Fridrich, and T. Kalker. Digital watermarking and steganography. *The Morgan Kaufmann Series in Multimedia Information and Systems*, 2008.

[9] N. F. Johnson and S. Katzenbeisser. A survey of steganographic techniques. Artrech House, 2000.

[10] K. S. kumar and K. B. R. Khasim T. Dual transform technique for robust steganography. *IEEE International Conference on Computational Intelligence and Communication Systems*, pages 310–314, 2011.

[11] V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. *IEEE international conference on advance computing*, pages 223–228, 2010.

[12] B. Li, J. He, J. Huang, and Y. Q. Shi. A survey on image steganography and steganalysis. *International Journal of Information Hiding and Multimedia Signal Processing*, 2(2):142–172, 2011.

[13] S. Mallat. A wavelet tour of signal processing. *2nd Edition Academic Press*, 1999.

[14] H. Sheikh, M. Sabir, and A. Bovik. A statistical evaluation of recent full reference image quality assessment algorithms. *IEEE Trans. on Image Processing*, 15(11):3440–3451, 2006.

[15] G. J. Simmons. The prisoner's problem and the subliminal channel. *Advances in Cryptology: Proceedings of CRYPTO'83*, pages 51–67, 1983.

[16] X.Yi. Fast encryption for multimedia. *IEEE Transactions on Consumer Electronics*, 47(1):101–107, 2001.

[17] L. Zhang, L. Zhang, X. Mou, and D. Zhang. Fsim: a feature similarity index for image quality assessment. 20(8):2378–2386, 2011.