Information Hiding Model Based on Channel Construction of Orthogonal Basis

Bao Kangsheng, Hefei No.6 High School, China

ABSTRACT

Secret information communication model based on channel construction of orthogonal basis can implement secret information hiding and recovery without a key. The orthogonal basis is constructed by the media carrier’s self-correlation. Carrier and secret information channels are constructed independently. And it has good properties of avoiding detection. The experiments show that the model with proper carrier components and threshold of secret information coding has the capacity of secret information and robustness. And the secret information capacity and anti-noise capability can be improved by compressed and error correcting or checking codes.

KEYWORDS

Channel, Coding, Independent, Information Hiding, No-Key, Orthogonal Basis

INTRODUCTION

With the development of cryptography, computer and other technologies, information hiding has become a hot issue in information security research. Especially, pure ciphertext communication tends to attract the attention of non-cooperative recipients. The main forms of expression are as follows: To take some multimedia information as the carrier, such as image, video, voice and so on. To superimpose the secret information on the multimedia information in some way, so as to reduce the sensitivity of the non-cooperative recipient to the secret information and improve the performance of anti-steganography analysis without prior knowledge. In this kind of research, multimedia carrier does not have the significance of information transmission, but only the hidden function of secret information (Wang, 2011; Sun, 2016). According to the change method of secret information to multimedia carrier, this research direction is mainly divided into two categories:

1) The secret information is superimposed directly on the multimedia carrier, and most of the carriers of this kind of methods are images. Usually, the secret information is realized by changing the characteristics of the image according to a certain algorithm or law. (Mehmet, Gaurav, Ahmet & Eli, 2005) use the hiding information to change the gray distribution of the whole image. (Qin, Chang & Chen, 2013) use the hiding information to change the smoothing conditions of the edge region. (Wu & Huang, 2012) use similar method that use the hiding information to change the gray of image. It may be common to use secret information absolute or difference to change the gray distribution of the whole or redundant region of the image, and so on. (Wang, Sun & Li, 2019) is a recently method to complete the transmission of secret information by using interpolation algorithm with the change of image gray value. This method expands the information capacity to a certain extent.
2) The carrier of this kind of methods is more diverse, which superimpose the secret information indirectly on the multimedia carrier. For example, the multimedia carrier is changed in the transform domain by changing the coefficient of the transform domain with the secret information, such as Fourier, wavelet and other transform domain methods (Vaishnavi & Subashini, 2015; Islam & Laskar, 2017). (Wu & Wu, 2016) hided the secret information in areas where the human ear is less concerned and the degree of redundancy is higher, using different domains corresponding to different scales of wavelet bases in voice.

Among them, method 1) often need secret key to explain the algorithm and law of changing carrier with secret information. Although the methods and algorithms to realize covert communication are relatively simple, and the secret information can be solved completely, the transmission problem of secret key (including the design of secret key, transmission mode, etc.) must be considered in the construction of covert communication. At the same time, the secret information should be reasonably designed to change the threshold control of the multimedia carrier, otherwise it will make a great change to the carrier, and the ability of anti-steganography analysis is weak. The central idea of method 2) is to disperse the secret information into the carrier. And the security of the secret information is improved compared with 1). But the mapping method of the transform domain makes it more difficult for the receiver to recover secret information. Therefore, the research of covert communication basically focuses on two aspects:

1) No key or special key;
2) Seeking the balance between less change of multimedia carrier and undistorted recovery of secret information.

With two aspects, the information hiding model is constructed by orthogonal basis. And the orthogonal basis is get by media carrier’s orthogonal decomposition basis. The orthogonal decomposition basis constructs two independent channels for carrier and secret information. Because the basis decided by carrier, it matches 1). And the secret information is scattered over the carrier, without changing special characters of carrier. So the secret information cannot be easily detect. By orthogonal basis get from carrier’s self-correlation, the secret information is not confined to the same type with carrier. For example, if carrier is image, the secret information’s type is image too. The capacity of the secret information is evaluated by type and encode. So the model get better flexibility.

**CHANNEL CONSTRUCTION OF ORTHOGONAL BASIS BASED ON MULTIMEDIA INFORMATION**

On the basis of studying the two key problems of the covert communication, the paper proposes a covert communication model based on channel construction of orthogonal basis. Two independent channels of the multimedia and the secret information are constructed through the orthogonal basis. The orthogonal basis is determined by the orthogonal decomposition component of the multimedia information. So the relationship between the carrier and the secret information is not required by the intervention of the external secret key. At the same time, the secret information is dispersed into the carrier, not a specific change of multimedia characteristics of a certain kind of parameters. So the secret information change carrier is flexible, controllable, and not easy to be detected. Therefore, the secret information is no longer confined to the homologous form of the carrier, such as the carrier is an image, and the secret information is also an image, which can be represented by other types. The capacity of the information can be determined by the form and coding of the secret information. And the adaptability is stronger.
Fundamental Model

The basic construction model of this paper is shown in Figure 1. Functions and requirements of encryption module at sender are as follows:

1) In the absence of secret key, $S$ changes $C$ and $D$ is output. ($S$ stands for the hid information or secret information. $C$ stands for the carrier. $D$ stands for the result of steganography.);
2) The conventional multimedia feature analysis method is used to analyse $D$ and $C$, and the difference between them is within a small range. The aim is $D$ closet to $C$.

Functions and requirements of decryption module at receiver are as follows:

1) $D$ is transmitted through channel. Because it is added by $N$($N$ stands for noise), $D'$ is received. $S_{out}$ is extracted $D'$ from without prior knowledge.
2) The aim is that there is little difference between $S_{out}$ and $S$ under certain signal-to-noise ratio (SNR).

Steganography Process

Make $C_{arb}$ the original multimedia carrier, and the steganography process is as follows:

Step 1) Standardize $C_{arb}$ to get $\tilde{C}_{arb}$, and find its self-correlation matrix $R_c$, i.e.

$$R_c = E[\tilde{C}_{arb} \tilde{C}_{arb}^T]$$

Step 2) Find the eigenvalue $\lambda_{R_c}$ and eigenvector $\Phi_{arb}$ of $R_c$. Where, $\Phi_{arb}$ is an orthogonal matrix of order $b$, i.e., $\Phi_{arb}^T\Phi_{arb} = I_{arb}$, $I_{arb}$ is an identity matrix of order $b$.

Step 3) According to the principle of orthogonal decomposition,

$$C_{arb} = H_c \Phi_{arb}$$

can be obtained after mapping. Where, $\lambda_i \epsilon \lambda_{R_c}$ and $H_{arb} \epsilon H_c$ correspond one to one.
Step 4) Set the threshold $\lambda_{\text{threshold}}$, keep $H_{c_i} e_{c_i}$, which is corresponding to $\lambda_i > \lambda_{\text{threshold}}$, and complete the multimedia reconstruction, namely

$$C'_{\text{axb}} = \begin{bmatrix} H_{c_1} & H_{c_2} & \cdots & H_{c_d} & 0 & \cdots & 0 \end{bmatrix} \Phi_{\text{bxb}} = H_{e} \Phi_{\text{bxb}}$$

(3)

Step 5) Build secret information $S = S_1 S_2 \ldots S_e$ \(\frac{0}{b-d-e}\), where $S_i \in [S_{\text{max}}, S_{\text{min}}]$, $(S_{\text{max}}$ and $S_{\text{min}}$ are the upper and lower bounds of the encoded values respectively), to solve $S'$.

$$S' = \begin{bmatrix} d & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix} \Phi_{\text{bxb}} = H_{s'} \Phi_{\text{bxb}}$$

(4)

Step 6) To solve $D$.

$$D = C' + S'$$

(5)

Reduction Process

As Fig.1, $D$ is transmitted by “channel”. And $D$ is added by noise and changed to $D'$. So the receiver receives $D'_{\text{axb}}$, and the decryption process is as follows:

Step 1) Standardize to get $D'_{\text{axb}}$, and find its autocorrelation matrix $R_{D'}$, the same as step 1) of 1.2.

Step 2) Find the eigenvalues $\lambda_{D'}$ and eigenvector $\Phi_{D'}$ of $R_{D'}$, the same as step 2) of 1.2.

Step 3) The same as step 3) of 1.2, to solve $H_{D'}$.

Step 4) For $S_i \in [S_{\text{max}}, S_{\text{min}}]$, obtain $[H_i H_{D'}] e [S_{\text{max}}, S_{\text{min}}]$ to set $H_{s'}$, which is $(b-d) \times (b-d)$. Then

$$S'_{\text{out}} = H_{s'} \begin{bmatrix} 1 \ldots 1 \end{bmatrix}_{b-d}$$

(6)

CHANNEL PERFORMANCE OF ORTHOGONAL BASIS BASED ON MULTIMEDIA INFORMATION

For the model constructed in 1, whether the receiver $S_{\text{out}}$ can restore $S$ under certain conditions is a problem that needs to be verified.
Proof of Reasonableness

1) Noiseless situation

That is \( N_{axb} = 0 \), then \( D'_{axb} = D_{axb} \).

Obtain \( D' = C' + S' = (H_{C'} + H_{D'}) \Phi_{axb} \) according to (5).

Because the encryption module at the sender uses principal component analysis (PCA) to solve the orthogonal basis \( \Phi_{axb} \) of the original multimedia, in the process of steganography, it does not change \( \Phi_{axb} \), but only changes the characterization coefficient, so let \( H_{C'} + H_{D'} + H_D \), then \( D' = H_D \Phi_{axb} = H_D \Phi_{axb} \).

Therefore, according to the solution process of 1.3 and the uniqueness of PCA’s solution, \( S_{out} = S \) can be obtained.

2) Noisy situation

That is \( N_{axb} \neq 0 \), then \( D'_{axb} = D_{axb} + N_{axb} \).

If \( N_{axb} \) is independent of \( C_{axb} \) and is Gaussian white noise, process \( N_{axb} \) by PCA and \( N_{axb} = H_{N} \Psi_{axb} \). Obtain

\[
D' = H_{D'} \Phi_{axb} + H_{N} \Psi_{axb} \tag{7}
\]

At this time, the orthogonal representation basis of \( D'_{axb} \) after PCA processing on the receiver will be deflected and no longer be \( \Phi_{axb} \), and the second term of (10) must be eliminated.

Because \( N_{axb} \) is Gaussian white noise, the orthogonal array \( \Lambda_{axb} \) can be constructed, let \( \Psi_{axb} \Lambda_{axb} = 0 \).

Substituted into (10), then

\[
D'' = D'_{axb} + H_{D'} \Phi_{axb} \tag{8}
\]

As a result of \( \Phi_{axb} \Lambda_{axb} \left( \Phi_{axb} \Lambda_{axb} \right)^T = I_{axb} \), \( D'' = H_D \left( \Phi_{axb} \Lambda_{axb} \right) \) can be obtained after processing \( D'' \) by PCA. Therefore, \( S_{out} \) is extracted from \( D'' \) at the receiver, which is consistent with the noise-free environment, and the evidence is obtained.

It is necessary to make an explanation that the certainty of \( H_D \) is very important when the receiver is processing \( D'_{axb} \), and because of the diagonal nature of \( S' \), the solving target is to fit and construct the orthogonal array \( \Lambda_{axb} \), let \( \Psi_{axb} \Lambda_{axb} = 0 \) and make \( H_D \), have the diagonal matrix of the largest subarray.

Because \( N_{axb} = H_{N} \Lambda_{axb} \) and \( \Lambda_{axb} \) is obtained from the correlation matrix of \( N_{axb} \), make \( N_{axb} = \left[ N_1, N_2, \ldots, N_k \right] \), where \( N_i \in N_{axb} \) obeys normal distribution \( N(0, \sigma_i) \), according to (1) (2) (3), it can be obtained that
\[
\Lambda_{bxb} = \begin{bmatrix}
1 & b_{12} & \cdots & b_{1n} \\
\vdots & \vdots & \ddots & \vdots \\
1 & b_{n1} & \cdots & 1
\end{bmatrix}
\]

And because \( \Lambda_{bxb} \) is obtained from \( N_{xb} \), then \( \sigma_1 = \sigma_2 = \cdots = \sigma_b = 1 \) and

\[
b_j = \frac{E[N_i N_j^T]}{\sigma_i \sigma_j}
\]

Fitting steps:

Step 1) According to multimedia transmission environment and SNR, set range \( \sigma_i \) and make the initial value be \( \sigma_1 = \sigma_2 = \cdots = \sigma_b = 1 \).

Step 2) Obtain \( D^* \) from (8) and \( H_{D^*} \) from 1.3.

Step 3) Use greedy genetic algorithm according to (Qin, Ding & Gong, 2013), just change \( \sigma_i \) according to its range. The least square method can be used to fit until the diagonal matrix is stable.

Step 4) Obtain \( S_{out} \) from 1.3.

**Model Performance Analysis**

The rationality of the model can be proved by theoretical argumentation in 2.1, and the secret information capacity and robustness of the model should also be considered. From the construction analysis of the model, it can be concluded that the secret information capacity is related to the multimedia carrier. The complex robustness is related to the coding mode of \( S \).

1) Because \( C' \) and \( S \) use the characterization of orthogonal groups obtained by PCA processing of \( C \) together and selective channel is determined by \( \lambda_{threshold} \), the secrecy after encryption is determined by \( \lambda_{threshold} \). At the same time, it decided on \( S_{max} \), then the coding range of \( S \), which determines the secret information capacity.

2) Under ideal conditions, the model can realize \( S_{out} = S \). Especially in many multimedia transmission scenes at present, supplemented by receiving and checking mode, \( N_{xb} \rightarrow 0 \) can be achieved basically, therefore, the basic environment of this module is that of large signal-noise ratio (SNR). In the case of \( a_1 = a_2 = \cdots = a_b = 0 \), SNR is determined by \( \sigma_i \). The computational complexity of \( \Lambda_{bxb} \)’s fitting construction should be reduced accordingly.

3) If \( b \) decreases, the computation of \( \Lambda_{bxb} \) will decrease. At the same time, it results in the reduction of secret information capacity. The computing power of the receiver needs to be weighed, which has something to do with engineering design, so as to determine the value of \( b \), that is, to determine which multimedia carrier to choose.

4) Use appropriate coding method to encode \( S \), the accuracy of \( S_{out} \rightarrow S \) can be obtained by the sacrifice of robustness.
EXPERIMENTAL EVALUATION

According to the performance analysis results of 2.2, 3) and 4) belong to the engineering design and coding design problems, not the model performance, this paper does not discuss 3) and 4). So all the experimental evaluation will use the same multimedia carrier and the same coding method of S to complete the performance test.

Secret Information Capacity Performance

According to the analysis results of 1) in 2.2, the experiment focuses on how to set up $\lambda_{\text{threshold}}$ and $S_{\text{max}}$ for the established multimedia carrier. Under the condition of striving for large secret information capacity, there is no great distortion between $D$ and $C$ by conventional method.

The multimedia carrier is Figure 2, which comes from the grayscale map of the “ring” of the earth. It is released publicly in the major special network of the high-resolution Earth observation system, and image pixels are 891*900.

According to step 1) 2) 3) of 1. 2, $\lambda_{R_C}$, $H_C$ and $\Phi_{900*900}$ are obtained, Figure 3 and Figure 4 shows the obtained $\lambda_{R_C}$ and $|H_C|$. The eigenvalues of the multimedia carrier are up to $7.8817 \times 10^5$ and the minimum value is 0, where the number of 0 is 9, which shows an exponential decline. $|H_C| \in (1000,2000)$.

$\lambda_{\text{threshold}}$ Setup Experiment

1) Experimental data

In this experiment, $C'$ is produced by multimedia reconstruction, and the difference between $C'$ and $C$ is analyzed by conventional multimedia. According to the reality of multimedia, the gray value distribution, texture feature distribution and subjective method are used to evaluate the gap, in which the texture feature distribution is analyzed by LBP method (Local binary patterns).

The gray value distribution and the texture characteristic distribution analysis of the $C$ are shown in Figure 5 and Figure 6.

The value of $\lambda_{\text{threshold}}$ is based on the decrease of $\lambda_{R_{\text{max}}}$ per dB unit, that is, $\lambda_{\text{threshold}} = \frac{\lambda_{R_{\text{max}}}}{10^{\frac{\text{dB}}{10}}}$, build $C'$ according to step 4) of 1.2. The result is shown in Figure 7.

The difference between $C'$ and $C$ is analyzed from gray histogram distribution and texture, as shown in Figure 8.

2) Experimental Conclusion

It can be seen from the experimental analysis that, because $C$ may be obtained by a third party in different channels, to ensure the privacy, $C'$ must be analyzed by the attribute of $C$, ensure that the conventional analysis method is adopted, and the difference between $C$ and $C'$ can’t be too large.

From the analysis of Figure 7 and Figure 8, with the decrease of $\lambda_{\text{threshold}}$, the gap between $C$ and $C'$ decreases gradually by using conventional analysis methods. Apart from falling to 9dB, the histogram has a wave of valleys, but there is a big gap between the subjective analysis of the image and other analysis methods. This shows that in the encryption process, the value of $\lambda_{\text{threshold}}$ should be evaluated by various means according to the characteristics of $C$. 
The results show that $C'$ tends to be stable when $\lambda_{\text{threshold}}$ is 31dB smaller than $\lambda_{R_C}$, that is, at least 135 large principal components of $C$ are retained as the transmission channels of $C'$, so the remaining 765 (900-135) components can be used as secret information transmission channels.

$S_{\text{max}}$ Setup Experiment

1) Experimental Data

In this experiment, the value of secret information $S_{\text{max}}$ is investigated. From the original carrier analysis results and Figure 2, $|H_{C\text{imin}}| = 1095.3$ can be obtained. According to the design requirements of step 5) in 1.2, $|S_{\text{max}}| < |H_{i} \cdot H_{C\text{imin}}|$, and the experimental results of 3.1.1, the experimental object is $C'$ which is constructed by $C$ for retaining 135 large principal component channels.
The experiment is based on the criterion that $S_{\text{max}}$ takes $|H_{C_{\text{min}}}|$ according to the decrease of dB unit, that is $S_{\text{max}} = \frac{|H_{C_{\text{min}}}|}{10^{x_{\text{dB}}}/10}$. The encoded value of $S$ is a random value in $[0, S_{\text{max}}]$. Follow step 5) of 1.2 to build $D$, as shown in Figure 9.

The difference between $D$ and $C$ is evaluated by gray value distribution and texture feature distribution, as shown in Figure 10.

2) Experimental Conclusion

From Figure 7 and Figure 8, the overall trend is that the difference between $C$ and $D$ is smaller with the decrease of $S_{\text{max}}$. And because the code selects a random number smaller than $S_{\text{max}}$, there is a certain oscillatory contingency in the single experimental results, which meets the basic requirements of covert transmission adaptability.

According to the results of various analysis, $S_{\text{max}}$ takes the value that goes down 7dB from $|H_{C_{\text{min}}}|$, that is $S_{\text{max}} = 218.5144$ can have a good concealment effect.

Robustness

The robustness of the model determines the adaptive environment of the model. On the basis of 3.1 experiments, the robustness of the model is tested by using basic coding according to the error rate.

Suppose the secret information is $s(t) = \cos \omega t$, and it is encoded according to the natural coding method, as shown in Figure 11. The number of secret information transfers is determined by...
Figure 4. Distribution of component Modules $|H_C|$ corresponding to eigenvalues of Map of the relevant parameters of the forward traffic channel of multimedia

Figure 5. Gray histogram Distribution Map of C

3.1.1, that is (Number of channels required for total orthogonal basis data-$C'$) determines the length of the abscissa of Figure 11. The number of coded bits of the secret information is determined by $S_{\text{max}}$, that is, the lattice number $M$ of the ordinate of Figure 8, and $M_{\text{max}} \ln S_{\text{max}}$. 
Figure 6. Results of LBP Analysis of C

Figure 7. C'
According to the experimental results of 3.1.1, the experimental object is $C'$, which is constructed by $C$ for retaining 135 large principal component channels. According to the experimental results of
3.1.2, make $S_{\text{max}} = 218.5144$, then $M=5$. Then the $S$ in this experiment is 756 5-bit binary coding sequences.

**Experiment on Bit Error Rate (BER)**

Noise is introduced at the noise $N$ of *Figure 1* to evaluate the robustness of the model. Select superimposed Gaussian white noise, SNR interval is $\frac{S}{N} \in [30, 5] dB$, step is 0.5dB. Each SNR corresponds to $\sigma^2 \epsilon (0.5, 10)$, step is 0.5. Repeat 20 times according to (Liu & Temlyakov, 2012) for each test condition. Iterative constraint of genetic algorithms is that the number of iterations is no more than 500 and the maximum modulus error of the output result is less than 0.01. The conditions for each of the following test experiments are the same.

The correlation between BER and SNR is shown in *Figure 12 and Figure 13*. The anti-noise property of the mode can be obtained from the mean value and variance, which can maintain high secret information reduction ability in $\frac{S}{N} \geq 10dB$.

**Experiment on the Ability to Correct Mistakes**

Because the error of a small number of coding bits can be corrected by inserting the supervision code, the adjacent 1 quantitative unit error of the error code is investigated, and the results are shown in *Figure 14*. From the experimental results, it can be concluded that when the SNR is greater than 8dB, the BER of more than 50% is within the range of 1 quantification error, so the optimization of BER of the secret information of the model can be realized by correcting the error coding design.

In order to further test the improvement ability of error correction performance of the model, count the proportion of the wrong one-digit code, the results are shown in *Figure 15*. From the experimental results, if the error - correcting coding performance can correct 1-bit error code, then the better hidden transmission performance can be obtained in the condition that SNR is greater than 7.5dB.
Performance Comparison with Some Method

If the carrier can be gotten from other ways, 1) from research direction in the Introduction will make a slightly bigger difference between carrier and the result of steganography. If the carrier is an image, the difference may be detected easier by gray level distribution, texture. Or there may be some rules in gray and texture change. The model in paper has advantages and is supported by 3.

Transform domain analysis is common in carrier denoising, image enhancement and so on. 2) Research direction in the Introduction will change some components. And it can show a bigger difference in gray level distribution, texture.

Tomas Filler describes the STC(Syndrome-Trellis Codes) steganography method in Tomas Filler (2010) in detail, which is also a classical steganography method at present. And the hid information scatters in carrier without obvious regulation. But it should firstly determine the parity-check matrix H. And like Convolution code, STC has encoding constraint length. In order to avoid being detected easily, it should achieve the result of steganography closest to the original carrier. But this has two targets. The model in paper is easy to complete.
CONCLUSION

In this paper, a new steganography model is constructed by orthogonal basis. And the orthogonal basis is get by carrier itself from the correlation. And the hiding information and carrier share the orthogonal basis. It meets the need of two aspects stated in Introduction.

Carrier uses a small part of the orthogonal basis with a larger component, as PCA (Principal Component Analysis) told. And the hiding information can use the remaining. So it constructs two channels, and one for the carrier, the other for the hiding information. The two channels are physically orthogonal. This model is stated in Chapter 1. And the rationality is proved in Chapter 2.

If the threshold is controlled reasonably, the hiding information scattered in the carrier cannot be detected easily. The experiment is built to test performance of the model stated in Chapter 3. In the experiment, the carrier is a high resolution image. The hiding information is a bit stream which can match any form. The capacity is tested by the typical character of the image. And the noise resistance is also tested in the same experimental subject.

This model provides a new steganography method. And the form of hiding information is not limited to the same form as a carrier. From experiment, the performance can be improved by many aspects. These will be the next research object.

Next research direction:

1) It is pointed out that the genetic algorithm is used in this paper to fit the noise model in 2.1. In the course of the experiment, the genetic algorithm has the excellent potential in the multi-peak solution, but the convergence is slow, and the initial value is set to a certain requirement, so other methods can be considered to complete the work (Yan, Cui & Wang, 2018).

2) The more conventional coding method is used to test the performance of the model in 3.2 in this paper, but to some extent, the secret information capacity is limited. Compression coding technology can be used to further improve the secret information capacity (Chen, Liang, Li, Sun, Tan & Li, 2017; Li, Ding, Miao & Xiao, 2017).
3) According to 3.2, on the basis of satisfying the capacity of the secret information, the performance of the error-correcting coding can be introduced to further improve the performance of the model (Lv, 2016).
Figure 15. The relationship between error 1-bit code and total error code
REFERENCES

Chen, H.-Q., Liang, Q., Li, X.-C., Sun, Y.-M., Tan, T.-F., & Li, D.-F. (2017). LDPC decoding algorithm based on generalized threshold function in Rayleigh channel. *Acta Electronica Sinica, 45*(1), 16-21. doi:CNKI: SUN: DZXU.0.2017-01-003

Filler, T. (2010). Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization. *Proc. SPIE, Electronic Imaging, Media Forensics and Security XII.*

Islam, M., & Laskar, R. H. (2017). Geometric distortion correction based robust watermaking scheme in LWT-SVD domain with digital watermark extraction using SVM. *Multimedia Tools and Applications, 77*(11), 14407–14434. doi:10.1007/s11042-017-5035-9

Li, M.-Z., Ding, J., Miao, C.-W., & Xiao, H.-L. (2017). Differential Network coding of symbol multiplication in complex Domain. *Journal of Systems Engineering and Electronics, 40*(5), 1142–1147. doi:10.3969/j.issn.1001-506X.2018.05.28

Liu, E., & Temlyakov, V. N. (2012). The orthogonal super greedy algorithm and applications in compressed sensing. *IEEE Transactions on Information Theory, 58*(4), 2040–2047. doi:10.1109/TIT.2011.2177632

Lv, F.-C. (2016). Secure Communication Scheme based on error Correction Code. Chengdu: University of Electronic Science and Technology of China. doi:CNKI: CDMD:2.1018.708795

Mehmet Utku, C., Gaurav, S., Ahmet Murat, T., & Eli, S. (2005). Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing, 14*(2), 253–266. doi:10.1109/TIP.2004.840686 PMID:15700530

Qin, C., Chang, C.-C., & Chen, Y.-C. (2013). Efficient reversible data hiding for VQ-compressed images based on index mapping mechanism. *Signal Processing, 93*(9), 2687–2695. doi:10.1016/j.sigpro.2013.03.036

Qin, Y.-H., Ding, X.-Q., & Gong, H.-L. (2013). Application of High dimensional feature selection method in near Infrared Spectroscopy Classification. *Hongwai Yu Jiguang Gongcheng, 42*(5), 1355–1359. doi:10.3969/j.issn.1007-2276.2013.05.045

Sun, S. (2016). *Research on the Application and Security of Information hiding*. Xidian University.

Vaishnavi, D., & Subashini, T. S. (2015). Robust and Invisible Image Watermarking in RGB Color space using SVD. *Procedia Computer Science, 46*, 1770–1777. doi:10.1016/j.procs.2015.02.130

Wang, J.-J., Sun, Z.-R., & Li, G.-X. (2019). Large capacity reversible Information hiding algorithm in Parabola interpolation Space of Image. *Tien Tzu Hsueh Pao, 47*(1), 137–144.

Wang, Y. (2011). *Information Hiding Technology and Its Military Application*. National Defense Industry Press.

Wu, H.-T., & Huang, J. (2012). Reversible image watermarking on prediction errors by efficient histogram modification. *Signal Processing, 92*(12), 3000–3009. doi:10.1016/j.sigpro.2012.05.034

Wu, Q.-L., & Wu, M. (2016). A new method of speech information hiding based on wavelet transform. *Dianzi Yu Xinxi Xuebao, 38*(4), 834–840. doi:10.11999/JEIT150856

Yan, N., Cui, C., & Wang, X.-M. (2018). Infrared image enhancement based on Gaussian multimodal fitting and histogram specification. *Journal of Changchun University of Science and Technology (Natural Science Edition), 41*(3), 115-119. doi:CNKI:SUN:CGJM.0.2018-03-025

Bao Kangsheng is affiliated with Heifei No.6 High School. They were born in December of 1978. They have a Master’s in Information Processing. They were awarded special allowance by Anhui.