A Coverless Information Hiding Algorithm Based on Grayscale Gradient Co-occurrence Matrix

Jianbin Wu¹, Yiwen Liu¹, Zhenwei Dai², Ziyang Kang¹, Saman Rahbar³ and Yanke Jia¹

¹College of Physics Science and Technology, Central China Normal University, Wuhan 430070, People’s Republic of China; ²College of Engineering, University of Saskatchewan, Saskatoon, Canada SK S7N 5A9; ³Department of Computer and Science, University of Saskatchewan, Saskatoon, Canada SK S7N 5C9

ABSTRACT

In this paper, a coverless information hiding algorithm is introduced. In which, the grayscale gradient co-occurrence matrix is used to encode images and the mapping relationship between the images and the random numbers is used to express the payload information. There are three steps for this algorithm. Firstly, the grayscale gradient co-occurrence matrix of cover image is calculated, in accordance with which a descriptor is introduced. Secondly, the descriptor is quantized into a binary sequence to construct a mapping relationship between the cover image and the binary random numbers. Finally, the binary secret information sequence is divided into many segments, and the correct images corresponding to those segments are selected from the image database according to the mapping relationship. Moreover, the secret information is encrypted by Turbo encoder to improve the security. The experimental results show that the proposed algorithm has a good tolerance towards JPEG compression attack and low-pass filter attack. This promising algorithm which can be applied into remote sensing satellites leads an applied value in covert communication with high-security.

KEYWORDS

Coverless information hiding; Grayscale gradient co-occurrence matrix; Image coding; Information security; Robustness; Steganography; Zero steganography

1. INTRODUCTION

Nowadays, the satellite technology succeeds in long-range communication with the large cover area. Strengthening the security of satellite communication system is of great significance to the confidential communication at national defense and military levels. At present, the secure transmission of important data on the satellites mainly relies on encryption technology, which directly converts the original signal into meaningless cipher text through encryption keys and encryption functions. However, this technology results in the existence of the covert communication, which may attract the attention of the adversaries. If the covert communication is imperceptible to be detected, the security of the technology will be greatly improved. Due to the increasing demand on the communication security, information hiding technology has been shaping up. Different from the cryptography technology, information hiding technology utilizes the multimedia information as hosts to implement the concealment of digital signals.

In this paper, we introduce a coverless information hiding algorithm based on coding the feature descriptor of remote sensing images. First, the grayscale-gradient co-occurrence matrix (GGCM) of an image is calculated by using a modified extraction algorithm. Then the GGCM is processed and characterized to establish an index relationship between images and random binary sequences without modification on the original image. Last, a mapping library of many-to-one correspondences between carrier images and secret messages is built to ensure the image-based coverless information hiding. By the way, the secret message is encoded to improve the security by using Turbo encoder.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 presents the proposed method in details. Section 4 shows the results of the experiments and analysis. The last section makes a conclusion of the full text.

2. RELATED WORK

Cryptography conceals the content of the messages secretly while steganography aims at hiding the existence of messages. According to the ways of hiding, the existing image steganography methods can be classified into two categories: spatial domain based and transform domain based. One of the most common methods of spatial domain is to replace the least significant bits (LSB) with secret data [1]. Reference [2] proposed a data hiding method based on pixel value difference (PVD),...
least significant bit (LSB) substitution, PVD shift, and modification of prediction error (MPE). Steganography in the transform domain is used to modify the statistical feature of the cover image for achieving data hiding [3]. Many transform domain methods are proposed to hide data into DCT (Discrete Cosine Transform) domain [4], DFT (Discrete Fourier Domain) domain [5], and DWT (Discrete Wavelet Domain) domain [6]. Reference [7] proposed a novel multi-watermarking scheme in DWT domain based on hybrid multi-bit multiplicative rules controlled by secret keys. Reference [8] proposed a method which combines the signal processing, cryptography and steganography to enhance the security of secret information. Reference [9] proposed a novel method which joints traditional data hiding and compression scheme to enhance the information hiding. In addition, some researchers applied the steganography technology in field of satellite communication, embedding low-speed data into the images transferred by the high-speed transmission system [10,11].

Steganography, in general, is the process of embedding the secret information into the cover media, including images, texts, audio, video and so on, which can be described as follows [12]:

\[
\text{cover image} + \text{secret data} \xrightarrow{\text{embedding algorithm}} \text{stego image}
\]  

(1)

In this way, an image is chosen to be a cover image, and the secret information is embedded into this image by a specific embedding algorithm. This inevitably changes the original image itself and leaves some traces of modifications. In addition, related anti-steganalysis algorithms based on statistical analysis can detect the existence of secret information. Reference [13] proposed a steganalysis method aimed at HUGO steganography, which can detect the stego-images reliably, and extract the embedded message as well. Reference [14] proposed a general steganalysis feature selection method based on decision rough set \(\alpha\)-positive region reduction, improving the efficiency of steganalysis algorithm. Overall, steganalysis technique is a great threat for these traditional steganography methods.

To avoid modifying the original image, zero-steganography proposed by [12] establish a relationship between the cover image and the secret data by using the logistic map to generate a chaotic matrix, and the stego-keys among the cover image, chaotic matrix and secret data. Reference [15] proposed a zero-watermarking like steganography with an information extraction file generated, which is indispensable for the receiver to recover the secret message. Reference [16] proposed a zero-steganography algorithm based on chaotic sequence and DCT transform, using the DC components of the cover image DCT transform coefficients to represent the secret message, with a related document.

A mathematical model for a basic zero-steganography, which is presented in the followed equation, is used for constructing a functional relationship \(F\) between the cover image and secret data to obtain the corresponding stego-key.

\[
F(\text{cover image}, \text{secret data}) = \text{stego key}
\]  

(2)

Zero steganography indeed has a good imperceptibility; however, it produces some auxiliary data, such as stego-keys, the extraction files or other related documents, which must be transmitted through another channel. Moreover, there are some security risks that attacks or cryptanalysis on the auxiliary data caused by the adversaries cannot be avoided. In terms of satellite data communication, additional secure channels are occupied to transmit the auxiliary data, resulting in a waste of resources.

Rather than the traditional information hiding method that embeds the secret data into a specified image, the coverless information hiding method without other carriers was proposed by Zhou et al. [17]. In this method, a cover image can be driven by the secret information and yield an encryption vector, so that the secret message is transmitted without any modification. Besides, the process of the coverless information hiding method does not generate any auxiliary information, which saves the signal channel resources.

From the above analysis, there are three advantages of the coverless information hiding method [18]: no embedding, no additional message, and anti-steganalysis. The main idea of the coverless information hiding method is to construct the mapping relationship between the information contained in the image itself and the secret information. The mapping relationship \(M\) between the cover image and secret data is shown as follows:

\[
M : \text{cover image} \xrightarrow{\text{yields}} \text{secret data}
\]  

(3)

Reference [18] established the correspondence between the Chinese vocabulary and cover image by using the coverless information hiding method. Reference [19] proposed the IEBVER (image-entropy-based visual expression of random) algorithm, which uses the entropy of
each image block and quantifies the eigenvalues of the entropy matrix to express the random numbers. Reference [20] utilizes the MSIM (molecular structure images of material) to achieve coverless information hiding. Reference [21] proposed a coverless image steganography based on DCT and LDA (Latent Dirichlet Allocation). Reference [22] introduced a dynamic content selection framework (DCSF) for coverless information hiding. Reference [23] proposed a coverless steganography method by leveraging a generative model. Besides, the progress in the technology of data sharing and cloud computing [24–26] has indeed facilitated the coverless information hiding.

3. PROPOSED METHOD

The frame diagram of the proposed method is illustrated in Figure 1. A complete image database is constructed through this process, in which the grayscale gradient co-occurrence matrix (GGCM) of an image is employed to carry out the image feature coding. At the sending end, the secret information is processed through Turbo coding, increasing the security of the covert information. For obtaining the correct images corresponding to binary sequences, the sender searches the image from the database and then sends those images out to the receiver through the open channel. Similarly, at the receiving end, the information expressed by the cover image is extracted and then decoded by using Turbo to recover the secret information.

3.1 Establishment of Image Database Using GGCM

An image consists of many features like brightness, colour, entropy and so on. A binary sequence can be expressed through coding and quantizing those features of the image. The GGCM, namely the grayscale gradient co-occurrence matrix, has been proved to be a powerful approach for image texture analysis, describing the distribution of each point in an image at grayscale and gradient scale, and showing the spatial relationship between each point and its neighboring points. Given $h(i, j)$ is an element of GGCM, the value of which is defined as the total number of pixels, in the condition of the gray value $i$ and the gradient value $j$ in the normalized gray image $F(i, j)$ and the normalized gradient image $G(i, j)$.

In this paper, we calculate the GGCM of image $F(i, j)$ as follows:

1. Extract the grayscale matrix $F(x, y)$ of the image.
2. Extract the gradient matrix $G(x, y)$ of the image by using the improved Sobel operator [27].
3. Count the number of pixels in the conditions of $F(x, y) = i$ and $G(x, y) = j$.
4. The cumulative number is the value of the element $H(i, j)$ in the GGCM.

The time complexity of the aforementioned algorithm is $O(n^2)$ Figure 2.

In this way, the outermost edge of the gray matrix, which carries on less information, is deliberately omitted.
because the number of dimension in the gradient matrix is one less than that in the grayscale matrix. Thus one can calculate the GGCM though this. For giving an explicit illustration of the 3-D plot, the gradient level (X-axis) is set to 64 and the gray level (Y-axis) is set to 256. For the standard test image, the three-dimensional plot of the GGCM is shown in Figure 3.

To describe the matrix GGCM effectively, a “feature descriptor” is introduced to represent H1 as a binary sequence. First, the 3-D plot is projected to the Y-axis, as H1 shown in Figure 4 (a). Second, the matrix H1 on \([t_1, t_2]\) is extracted to obtain H2, where \(t_1 = 2, t_2 = 63\); in this way, the projection lines corresponding to the highest gradient value, which is 64 and the lowest gradient value, which is 1, are excluded, as shown in Figure 4 (b). Third, the average value of each abscissa in the projection drawing is calculated to obtain matrix H3, as shown in Figure 4 (c). In the interval \([t_3, t_4]\), where \(t_3 = 1, t_4 = 255\), the matrix H3 is intercepted and divided into 17 segments, then the average of all elements in each segment is obtained to get the vector H4, which is the feature descriptor of low distortion.

To generate the binary sequence \(\{a_1, a_2, \ldots, a_n\}\), the quantification criteria are as follows:

\[
\begin{cases} 
  k_i = 1, & \text{if } H4_i \geq H4_{i+1} \\
  k_i = 0, & \text{otherwise}
\end{cases}
\]

where \(1 \leq i \leq n\) (4)

According to this equation, a 16-bit-length binary sequence is denoted by an image. To make full use of a mass of remote sensing images from the satellite, each image is coded into a binary sequence and then stored in a subpool which represents a certain single binary sequence, building a mapping library of many-to-one correspondences between carrier images and secret messages. A complete image database is constructed when all binary sequence is presented by images.

### 3.2 Design for QPP Interleaver in Turbo Code

The Turbo code, which can achieve near-Shannon-limit performance through iterative decoding process, is an impressive forward error correction technique. It is widely used in mobile, deep space and satellite communications. The Turbo encoder is formed by two RSC (recursive systematic convolutional) encoders in parallel concatenation by a random QPP (quadratic permutation polynomial) interleaver, along with the puncturing mechanism. A typical Turbo encoder block diagram is shown as follows Figure 5:

If the polynomial \(F(x) = f_1x + f_2x^2\) can replace the sequence \(\{0, 1, 2, \ldots, N - 1\}\), where \(N \geq 2\), and \(f_1\) and \(f_2\) are nonnegative integers, \(F(x)\) is called QPP based on the integer \(N\). The QPP interleaver is a vital component of the Turbo encoder, which replaces a sequence with \(N\)
symbols, and which converts a series of consecutive burst errors into discrete random errors in the message. Hence, to solve the coefficients of the polynomial is the crux of the matter. Some values of the coefficients for QPP can be calculated through computer-aided search by using the theory [28].

Table 1 gives the appropriate values of the coefficients and the length $k$ of the interleaver.

The operating parameters in this paper are as follows: the interleaving mode for QPP is Pseudo-random; the generator matrix is $[7, 5]$ for RSC1 and $[15, 17]$ for RSC2; the puncture matrix is $P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; the data rate is 0.5; the decoding mode is Log-MAP; the number for iteration is 5.

### 3.3 Process of Sending and Receiving

#### 3.3.1 Process of Sending

Step 1: The secret information is converted into a secret binary sequence $M$ in the first place. The length of the secret binary sequence is $L (L \leq 2^{16})$. Then $M$ is divided into segments of 8-bit-length. Namely $M = \{M_1, M_2, \cdots, M_i, \cdots, M_n\}$. If $M_i$ is less than 8 bits, it will be appended zeros at the end of this segment to reach 8 bits.

Step 2: Each segment is coded by Turbo encoder. As a result, the length of each segment becomes 16 bit because of the data rate.

Step 3: Search the correct image randomly from the subpool corresponding to the 16-bit-length segment according to the mapping relationship.

Step 4: Continue step 3 until all of the segments are expressed.
Step 5: Select the right image which is equal to the binary form of \( L \) to represent the length of \( M \). Then, add it to the end of those images.

Step 6: Transmit all images consecutively to the receiving end.

3.3.2 Process of Receiving
At the receiving ending, all images are received one by one. First, the 16-bit-length binary sequence is extracted from each image by using the algorithm mentioned in Section 3.1. Second, the binary sequence of the last image is converted into a decimal number \( L \), which is the length of the binary secret message. Third, each 16-bit-length sequence is decoded into the 8-bit-length binary sequence. Then all 8-bit-length binary sequences are jointed. At last, zeroes should be deleted if there are any of them added to the end of the original sequence, and the number of redundant zeroes is \( L \% 8 \).

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Robustness to Common Attack
Robustness is a rational measurement of the steganography algorithm, representing the ability of resistance to the attacks of an adversary. In the transmission process, the failure of the steganography algorithm is caused by common attacks which are JPEG compression, noise attack, low-pass filter attack and common image processing operations, etc. We will verify the robustness of the algorithm through four experiments in the next chapter.

Bit Error Rate (BER) is introduced to measure the robustness of the algorithm in the communication process. If the binary vector of the original image is \( P = \{p_1, p_2, \ldots, p_n\} \), and \( Q = \{q_1, q_2, \ldots, q_n\} \) represents the binary vector of the image after being attacked, then the BER is defined as follows:

\[
\text{BER} = \frac{e}{n}, \quad e = \sum_{i=1}^{n} p_i \oplus q_i
\]

The BER value is the average of the results for 1000 images.

4.1.1 JPEG Compress
The compression standard for continuos-tone still images (ISO 10918-1), known as JPEG, is the most popular and basic compression format. The JPEG is one of the lossy methods for compression, which allows the loss of information because of the insensitivity at a certain frequency of human vision and is performed on digital images before the transmission between mobile devices [24]. As such, the cover image is likely to be damaged through the transmission if attacked by this kind of compression. In this test, the robustness of the proposed algorithm against JPEG compression attack is measured by bit error rate. The quality factor \( (Q) \) of JPEG compression varies from 1 to 100 with an increment of 5 whereas \( Q = 1 \) represents the highest compression rate and \( Q = 100 \) represents the lowest compression rate. As shown in Figure 6, the abscissa axis represents the compression quality while the ordinate axis represents the bit error rate. Table 2 provides the comparison among the CBD (chaos based DCT steganography) algorithm [29], CBZS (chaos based zero-steganography) algorithm [12], CSD (chaotic sequences and image DCT algorithm) algorithm [16], CIHRIH (coverless information hiding based on robust image hashing) [30] and the proposed algorithm. The result shows the excellent performance of the proposed algorithm with the smallest BER at the same compression quality value.

4.1.2 Noise Attack
Salt & pepper noise, also known as double pulse noise, is caused by the strength of the signal pulse. The position of the noise is random, but the depth of it is fixed. This noise includes salt noise, which belongs to high grayscale noise, and pepper noise, which belongs to low grayscale noise. Generally, two types of noise appear at the same time. The proposed algorithm is analysed for salt & pepper noise,
whose density ranges from 0 to 0.1 with an increment of 0.01. Figure 7 shows the error rate curve of the algorithm with the existence of salt & pepper noise, whose density is represented by the X-axis, and Y-axis represents the BER. Table 3 provides the comparison of the BER among the CIHWE (coverless information hiding without embedding) algorithm [17], CIHRIH (coverless information hiding based on robust image hashing) algorithm [30] and the proposed algorithm when attacked by salt & pepper noise. The result shows the excellent performance of the proposed algorithm with the smallest BER at the same compression quality value.

Additive white Gaussian noise (AWGN) damages the signal through the linear additional white noise, which is a basic interference model. The amplitude of AWGN obeys the Gaussian distribution while the power spectral density obeys the uniform distribution. Mean $\mu$ and variance $\sigma^2$ are two parameters of AWGN. In our test, mean $\mu$ is 0 and variance $\sigma^2$ varies from 0 to 0.1 with a step with 0.01. Figure 8 shows the BER curve of the proposed algorithm with the existence of AWGN attacking.

### 4.1.3 Low-pass Filter

The low-pass filter removes the high-frequency components in the image. In other words, the filter can blur and smooth the image, and weaken the visible changes at the edges of the object. Some conventional steganography methods embed secret information into the high-frequency region because of the insensitivity of human vision, but those methods cannot resist the low-pass filter attack. In our tests, the cover image is attacked by the mean filter and Gaussian low-pass filter.

The mean filter has the size of $3 \times 3$, $5 \times 5$, $7 \times 7$ and $9 \times 9$, where $3 \times 3$ is the lowest filtering and $9 \times 9$ is the highest. The result is shown as Figure 9, in which the X-axis represents the size of the filter, and the Y-axis represents BER. Table 4 shows different BER of the algorithm CBZS (chaos based zero steganography) [12], SCZS (satellite communication zero steganography algorithm) [31] and CSD (chaotic sequences and image DCT algorithm) [16] when attacked by the mean filter.
There are two parameters of the Gaussian low-pass filter, namely size and Gaussian variance. In our test, the size is the default and the Gaussian variance varies from 0 to 1 with the stepping of 0.1. As shown in Figure 10, the proposed method has robust ability to attacks from Gaussian low-pass filter. Table 5 provides the comparison among the CBD (chaos based DCT steganography) algorithm [29], the CBZS (satellite communication zero steganography algorithm) algorithm [31] and the CSD (chaotic sequences and image DCT algorithm) algorithm [16].

### 4.1.4 Common Image Processing Operation

It is indispensable to carry out robustness analysis when image are attacked by some common image processing operations, which can make negative effects to the result of information hiding. Some kinds of common image processing attacks, which are applied to the cover images, are described below.

In this test, we make comparisons between the RCIS (robust coverless image steganography based on DCT and LDA classification) [21] algorithm and the proposed algorithm. Tables 6 and 7 show the BER of the two algorithms under the attacks of rotation and scaling processing respectively.

### 4.2 Security Analysis

One of the most considerable points for any steganography algorithms is imperceptibility, which can be measured by PSNR (Peak signal-to-noise ratio). For the proposed algorithm, the stego image and cover image are exactly the same; therefore, the stego image has the highest PSNR because of no modifications in the cover image. As a result, existing steganalysis techniques [13,14] fail to detect the secret information. Through the procedure of the covert communication, there is no auxiliary information generated, which reduces the skepticism and suspicion of a latent adversary.

Security is compromised when the covert communication is monitored or broken. For an attacker who wants to acquire the secret information, he or she has to detect the existence of the covert communication and read the hidden massage. According to the analysis above, it is impossible for others to detect the use of steganography and damage a stego-key because there is no additional information. Therefore, the proposed algorithm is of great imperceptibility and security. In addition, this algorithm can be applied to CG (computer graphics) and PG (photographic) [25].
Table 8: Comparison of capacity among the CBD, CBZS, CSD, and the proposed algorithm

| Method        | Capacity(bits/carrier) |
|---------------|------------------------|
| Zhou’s method | 8                      |
| Yuan’s method | 8                      |
| Zheng’s method| 18                     |
| Proposed method| 16                    |

4.3 Capacity Analysis

For \( n \)-bit-length binary encoding of all images in the database, there must be \( 2^n \) images at least corresponding with the binary sequences. If the length of encoding is too long, the image library that satisfies the conditions will be hard to be established; on the contrary, if the length is too short, the image library will be a small one, which is too simple to ensure the secure transmission of covert communication.

It is obvious that the capacity of coverless information hiding is less than tradition image steganography, which is a harsh problem to be solved.

Table 8 provides the comparison among Zhou’s method [17], Yuan’s method [32], Zheng’s method [30] and the proposed method in this paper.

5. CONCLUSION

The proposed method in this paper aims at satellite communication of high-security level, improving the quality of confidential data transmission. Compared with conventional steganography and zero-steganography, the proposed algorithm makes no changes to the cover image and generates no auxiliary data in the process of information hiding. This algorithm, which has been tested in MATLAB 2016b, shows high performance of resisting common image attacks. Therefore, the proposed algorithm is of good robustness and excellent anti-steganalysis. In terms of close and tight monitoring on communication links, this method leads to a strong applied value in the area of covert satellite communication.

ACKNOWLEDGEMENT

Additionally, Yiwen especially thanks to the inimitable care and help by Dr. Sohaib Manzoor.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

FUNDING

This work is supported by the National Natural Science Foundation of China [grant number U1736121].

REFERENCES

1. R. Chandramouli, and N. Memon. “Analysis of LSB based image steganography techniques,” International Conference on Image Processing, 2001. Proceedings IEEE, 2001:1019–1022 vol.3.

2. M. Hussain, A. W. A Wahab, N. Javed, and K. H. Jung, “Recursive information hiding scheme through LSB, PVD shift, and MPE,” IETE Technical Review, Vol. 35, no. 1, pp. 53–3, 8, Feb. 2017.

3. S. Hemalatha, U. D Acharya, A. Renuka, and P. R Kamath “A secure color image steganography in transform domain,” International Journal on Cryptography and Information Security, Vol. 3, no. 1, pp. 17–24, 31 Mar. 2013.

4. H. Noda, M. Niimi, and E. Kawaguchi. “High-performance JPEG steganography using quantization index modulation in DCT domain,” Pattern Recognition Letters, Vol. 27, no. 5, pp. 455–61, Apr. 2006.

5. V. Solachidis, and I. Pitas. “Circularly symmetric watermark embedding in 2-D DFT domain,” IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, Vol. 10, no. 11, pp. 1741–53, 2001.

6. E. Ganic, and A. M. Eskicioglu. “Robust DWT-SVD domain image watermarking: embedding data in all frequencies,” The Workshop on Multimedia & Security DBLP, Vol. 582, pp. 166–74, 2004.

7. J. Wang, S. Lian, and Y. Q. Shi. “Hybrid multiplicative multi-watermarking in DWT domain,” Multidimensional Systems & Signal Processing, Vol. 28, no. 2, pp. 1–20, 2015.

8. R. Ratan, and C. E. Veni Madhavan. “Steganography based information security,” IETE Technical Review, Vol. 19, no. 4, pp. 213–19, July 2002.

9. C. Qin, C. C. Chang, and Y. P. Chiu. “A novel joint data-hiding and compression scheme based on SMVQ and image inpainting,” IEEE Transactions on Image Processing, Vol. 23, no. 3, pp. 969–78, 2014.

10. X. Feng and Q. Zhou. “Information hiding of satellite remote image based on image complexity classification,” Yuhang Xuebao/Journal of Astronautics, Vol. 31, no. 7, pp. 1850–54, July 2010.

11. X. Li and Q. Zhou. “Data hiding transmission method against compression for satellite image based on chaos and slant transform,” Computer Engineering and Design, Vol. 7, p. 006, July 2013.

12. M. Bilal, S. Imtiaz, W. Abdul, S. Ghouzali, and S. Asif. “Chaos based zero-steganography algorithm,” Multimedia
13. X. Luo et al. “Steganalysis of HUGO steganography based on parameter recognition of syndrome-trellis-codes,” Multimedia Tools & Applications, Vol. 75, no. 21, pp. 13557–83, 2016.

14. Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang. “Selection of rich model steganalysis features based on decision rough set α-positive region reduction,” IEEE Transactions on Circuits and Systems for Video Technology, pp. 1–1, 2018. Available: https://ieeexplore.ieee.org/abstract/document/ 8272003

15. H. Ishizuka, I. Echizen, K. Iwamura, and K. Sakurai. “A Zero-Watermarking-Like Steganography and Potential Applications,” 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Aug. 2014

16. J. Wu, X. Fei, and N. Wang. “Zero-steganography algorithm research based on chaotic sequences and image DCT transform,” Electronic Measurement Technology, Mar 2017.

17. Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun. “Coverless image steganography without embedding,” Cloud Computing and Security, ICCCS 2015. Lecture Notes in Computer Science, Vol. 9483, pp. 123–32, 2015.

18. X. Chen, H. Sun, Y. Tobe, Z. Zhou, and X. Sun. “Coverless information hiding method based on the Chinese mathematical expression,” Cloud Computing and Security. ICCCS 2015. Lecture Notes in Computer Science, Vol. 9483, pp. 133–43, 2015.

19. D. Bai, M. Tian, X. Chen, M. Liu, and G. Xie. “Image-entropy-based visual expression of random,” Hunan Daxue Xuebao/Journal of Hunan University Natural Sciences, Vol. 44, no. 4, pp. 139–46, 25 Apr. 2017.

20. Y. Cao, Z. Zhou, X. Sun, and C. Gao. “Coverless information hiding based on the molecular structure images of material,” Computers, Materials & Continua, Vol. 54, no. 2, pp. 197–207, 2018.

21. X. Zhang, F. Peng, and M. Long. “Robust coverless image steganography based on DCT and LDA topic classification,” IEEE Transactions on Multimedia, pp. 1–1, 2018. Available: https://ieeexplore.ieee.org/document/8361834

22. Y. Cao, Z. Zhou, C. Yang, and X. Sun. “Dynamic content selection framework applied to coverless information hiding,” Journal of Internet Technology, Vol. 19, no. 4, pp. 1179–86, 2018.

23. X. Duan, H. Song, C. Qi, and M. K. Khan. “Coverless steganography for digital images based on a generative model,” Computers, Materials & Continua, Vol. 55, no. 3, pp. 483–93, 2018.

24. Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo. “On the fault-tolerant performance for a class of robust image steganography,” Signal Processing, Vol. 146, pp. 99–111, May 2018.

25. J. Wang, T. Li, Y. Shi, S. Lian, and J. Ye. “Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics,” Multimedia Tools and Applications, Vol. 76, no. 22, pp 23721–737, 22 Nov. 2016.

26. J. Li, Y. Zhang, X. Chen, Y. Xiang, and J. Li. “Secure attribute-based data sharing for resource-limited users in cloud computing,” Computers & Security, Vol. 72, pp. 1–12, Jan. 2018.

27. C. Deng, W. Ma and Y. Yin. “An Edge Detection Approach of Image Fusion Based on Improved Sobel Operator,” 2011 4th International Congress on Image and Signal Processing, Oct. 2011.

28. C. Schlegel, and L. Perez. Trellis and Turbo Coding. Chichester: Wiley Blackwell, 2015

29. S. Singh, and T. J. Siddiqui. “A security enhanced robust steganography algorithm for data hiding,” IFCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, no 1, May 2012, vol. 9, no. 3, ser. 1, pp. 131–39, May 2012.

30. S. Zhenget al. “Coverless information hiding based on robust image hashing,” Intelligent Computing Methodologies, IJCIC 2017. Lecture Notes in Computer Science, Vol. 10363, p. 536–47, 2017.

31. D. Bai, X. Chen, and M. Tian. “A satellite communication zero steganography algorithm,” Multimedia Tools and Applications, Vol. 76, no. 24, 10 Dec. 2016, pp. 26447–462, 10 Dec. 2016.

32. C. Yuan, X. Li, Q. Wu, and X. Sun. “Coverless image steganography based on SIFT and BOF,” Journal of Internet Technology, Vol. 18, no. 2, pp. 435–42, 2017.
Authors

Jianbin Wu is a Professor at the College of Physics Science and Technology, Central China Normal University. He received the MSc in Electronic Circuit and System and PhD in Communication and Information System from Wuhan University, in 2003 and 2009, respectively. His research interests include information security, information hiding, radar signal processing and low observable technology.

E-mail: wujianbin@mail.ccnu.edu.cn

Yiwen Liu received her BSc degree in Electronic and Information Engineering from Wuhan University of Science and Technology in 2016. She is currently a Master’s candidate in Information Security at Central China Normal University, Wuhan, China. Her research interests include information hiding and image processing.

Corresponding author. E-mail: even4lev@mails.ccnu.edu.cn

Zhiwei Dai is currently a Master’s student studying in the College of Engineering, University of Saskatchewan, Canada. His research interests include mechanical design, mechanical manufacture and soft robotics.

E-mail: zhd856@mail.usask.ca

Ziyang Kang received his BS degree in Physics from Hubei University of Education in 2016. He is currently a Master’s candidate at Central China Normal University. His research interests include deep learning and information security.

E-mail: ziyangkang666@163.com

Saman Rahbar is a Master’s student and researcher at the department of Computer Science, University of Saskatchewan, Canada. His research interests include: Artificial Intelligence, Machine Learning, Data Analysis and Information Technology.

E-mail: Saman.rahbar@usask.ca

Yanke Jia received her BSc degree in Physics from Zhoukou Normal University in 2015, and MSc in Communication and Information System from Central China Normal University in 2018. Her research interests include information security and information hiding.

E-mail: jiayahke@mails.ccnu.edu.cn