ATLANTIS PRESS
Advances in Engineering Research (AER), volume 61
International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2017)

Encrypted Image Steganographic Scheme based on Pixel Valued Differencing

Yu Liu [a], Bailong Yang, Wenqiang Zhao and Zhihua Yuan
Xi'an High - Tech Research Institute, China
[a]lauyu_18@163.com

Keywords: Information Hiding, Chaotic Scrambling, PVD, Hidden Capacity, Peak Signal - To – Noise-Ratio.

Abstract. Aiming at the problem of low hidden capacity and poor imperceptibility of the existing image information hiding algorithm in encrypted domain, an improved encrypted domain information hiding algorithm based on PVD (Pixel Valued Differencing) is proposed. The algorithm combines PVD algorithm, the logistic sequence is used to scramble the encrypted plaintext image, then the pixels in the encrypted image are paired, and the secret information is embedded according to the characteristic of the difference between the pixels. At the same time, the steganographic key is introduced to reduce the modification range of the pixel while keeping the hidden capacity. Experiments show that the algorithm has large hidden capacity, and under different embedding conditions, the imperceptibility of the improved algorithm is improved to some extent compared with the original PVD algorithm.

1. Introduction

With the rapid development of information security, information hiding as a key technology has attracted more and more attention from researchers. As the characteristics of clear image carrier, wide channels and easy operation, information hiding of the mainstream carrier. The plain text information hiding algorithm usually adds the secret information as the noise to the redundant space of the published image. It requires that the noise cannot be detected and avoid the secret attack and achieve the effect of stealing the cliff.

In practical applications, the publisher of the carrier image and the embedder of the secret information may not be the same, and the information transporter does not want the content of the carrier image to be acquired. This requires the information hiding while encrypting the contents of the carrier image, Text information concealment scheme arises at the historic moment. This kind of algorithm converts plaintext image into ciphertext image through various encryption techniques and combines the ciphertext image characteristics to hide information. In [1], the ciphertext image is first segmented, and the 3-layer LSB of the partial pixels is inverted to embed the 1-bit secret information. The receiving end carries out secret extraction and carrier recovery by searching for each block. However, this algorithm has limited capacity. Based on the above problems, the literature [2] using edge matching technology and literature [1] different smoothness calculation function has been improved to a large extent to enhance the hidden capacity and accurate extraction of secret information.

In the light of the idea of image smoothness, [3] calculates the block smoothness of the image blocks and classifies them separately. At the same time, with the help of the histogram modification, the proposed algorithm reverses the hidden information hiding algorithm. Better image quality, while achieving zero error. But because of the introduction of more auxiliary information, which restricts the security of the algorithm. In [4], the data is encrypted using LWE public key cryptography, and the redundancy space generated by LWE encryption algorithm allows users to embed hidden information in ciphertext. As the algorithm does not include the carrier characteristics of the principle, this program can be adapted to the ciphertext domain text, audio, images and any other carrier. It is worth mentioning that the above two schemes are separable ciphertext domain reversible information hiding scheme, that is, the secret extraction process is not sequential, the receiver can extract information according to different permissions, only have a steganographic key can be extracted Secret information without decrypting the

carrier image, only has the encryption key can decrypt the carrier image but cannot extract secret information. Greatly enhance the practicality of the algorithm. [5] proposed a block-based image reversible information hiding scheme, but the texture image processing results are not satisfactory. In [6], the pseudo-random selection set embedding multi-bit information in the image block is defined, but the hidden capacity needs to be improved.

In this paper, an encrypted domain information hiding scheme based on PVD is proposed based on the idea of pixel value difference.

2. PVD algorithm

PVD (pixel value difference) algorithm is an adaptive steganographic algorithm proposed by Wu and Tsai in 2003. The algorithm embeds secret information according to the difference of adjacent pixel pairs. The gray value space of [0,255] is divided into six subintervals: [0, 7], [8, 15], [16, 31], [32, 63], [64,127] and [128,255]. And determines the number of the secret information that the pair of pixels can bear by the difference between the pixels and the gray value sub-interval. The corresponding amount of secret information is used to generate a decision difference value for modifying the pair of pixels, and the pixel value is modified to complete the embedding of the secret information, and the extraction process is similar to the embedding process.

Because of the recognition characteristic of the human eye, it is sensitive to the modification of the texture smoothing region. This method makes good use of this feature, and embeds fewer secret bits in the smoothed region with small pixel difference. In texture complex region and edge region the human visual insensitive area embeds more secret information to enhance the embedding rate of the vector image.

PVD algorithm has the characteristics of simple realization and large hidden capacity, and can recover the carrier image without distortion at the same time as the secret information extraction. It is an effective reversible information hiding algorithm. So the advent of, aroused the interest of many researchers. Wang et al. [7] proposed an MF-PVD algorithm [8], which enhanced the imperceptibility of the original algorithm to a certain extent, according to the characteristics of the PVD algorithm which determines the embedding capacity by pixel difference. Hong et al. Proposed a DE-PVD algorithm [9] to further enhance the steganographic capacity.

3. The algorithm proposed in this paper

In this paper, a ciphertext-based information hiding algorithm based on PVD is proposed. The basic idea is to scramble and decrypt the plaintext image, and then to embed the information into the ciphertext image according to the PVD algorithm. In the process of hiding, a steganographic key is used to encrypt the steganographic process while reducing the modification range of the pixel pair. At the same time, the restoration of the carrier image can be realized by the key.

The embedding process of the algorithm is shown in Figure 1:

References are cited in the text just by square brackets [1]. (If square brackets are not available, slashes may be used instead, e.g. /2/.) Two or more references at a time may be put in one set of brackets [3, 4]. The references are to be numbered in the order in which they are cited in the text and are to be listed at the end of the contribution under a heading *References*, see our example below.

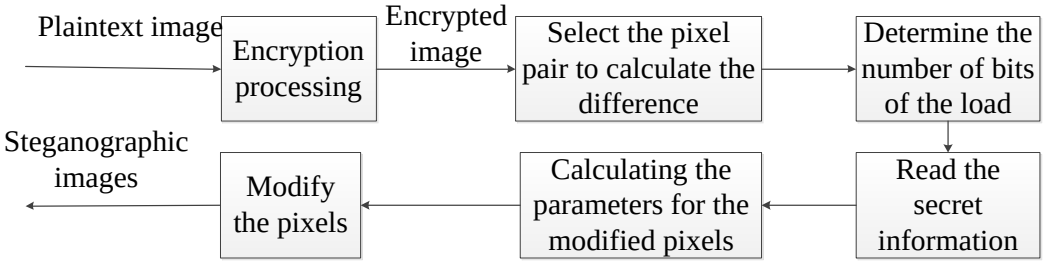

Fig. 1 Algorithm embedding process

3.1 Image encryption preprocessing

Digital image encryption technology and information hiding are closely related technologies, the two complement each other. After years of research, there have been a lot of digital image encryption methods [10]. According to the different scopes can be divided into spatial domain pixel encryption and transform domain coefficient encryption. The spatial domain pixel encryption can be divided into pixel location scrambling encryption and pixel value scrambling encryption, this paper discusses the pixel location scrambling encryption. Common methods are arnold (cat face transformation) scrambling, chaotic sequence of logistic scrambling and so on. Among them, arnold transformation is widely used, with periodic. But the key space is small, the practical application of the cyclical characteristics of the security caused some impact. The logistic chaotic sequence scrambling is an unpredictable, disorderly and aperiodic encryption method. In this paper, the image is encrypted and preprocessed.

Logistic chaotic function is defined as:

$$X_{n+1} = u \cdot X_n \cdot (1 - X_n) \tag{1}$$

Wherein the parameter $u \in (0,4]$, when $X \in (0,1)$, Logistic map is chaotic, and the chaotic sequence generated by the initial value X_0 is aperiodic and nonconvergent.

Logistic chaotic scrambling encryption steps are as follows:

(1) Read the picture, measure its size to $M \times N$, the elements in the figure are scanned in line to form a sequence $K(K_1, K_2, \cdots\cdots K_{M\times N})$ of length $M \times N$

(2) Define the initial Logistic sequence to iterate $M \times N$ times, get $M \times N$ floating point numbers between (0, 1), and make the sequence $L(L_1, L_2, \cdots\cdots L_{M\times N})$ to correspond to the elements in L and K.

(3) The elements of the sequence $L(L_1, L_2, \cdots\cdots L_{M\times N})$ are arranged in ascending order of size to form a new sequence $L'(L_1', L_2', \cdots\cdots L_{M\times N}')$, and the sequence K corresponding thereto undergoes the same permutation to generate the sequence K'

(4) The elements in K' in accordance with each M a row, constitute the size of the $M \times N$ matrix of images, scrambling encryption is completed.

Set parameters $u = 3.9, X_0 = 0.8$, get lena image after scrambling the encrypted image. The embedding of PVD algorithm makes use of the difference between the pixels. The larger the pixel difference is, the greater the hidden capacity is. In the plaintext, the correlation between each pixel is better, and the difference between adjacent pixels is not ideal. The ciphertext image encrypted by the above process is different from the plain text image, the pixel position is randomly distributed, the image content is invisible, the correlation between the scrambled image pixels is destroyed, the difference between the randomly arranged pixels Large, this time, and the hidden capacity of the algorithm can be further enhanced.

3.2 Secret information embedding and extraction

(1) The gray value space of [0,255] is divided into several different subintervals according to the partition rules in [6], denoted as $S_k = [l_k, r_k]$. This method takes the length of each interval is an integer power of 2, starting from 23 in order progressive. The interval is to determine the load capacity of the pixel pair. References are cited in the text just by square brackets [1].

(2) Load carrier image A, read a pair of pixels (p_i, p_{i+1}), calculate the difference $d_i = |p_i - p_{i+1}|$. While converting the secret information into a binary bit stream B. Determine the difference interval d_i, $d_i \in [l_k, r_k]$, according to the interval length to determine the pixel pair (p_i, p_{i+1}) can load the number of secret bits num_i, the formula is as follows:

$$num_i = \log_2(r_k - l_k + 1) \tag{2}$$

It can be found that each pair of pixels can load 3 to 7 bits of information.

(3) The num_i bit information is sequentially read from the secret bit stream B, converted into the decimal b, and the second difference d_i' is calculated.

$$d_i^{'} = l_k + b \qquad \delta = \left| d_i^{'} - d_i \right| \tag{3}$$

The decision difference values finally used for modifying the pixel values are calculated by d_i and $d_i^{'}$. The size of the δ value directly determines the modification range of the pixel pair, thus affecting the imperceptibility of the algorithm. Therefore, the following strategy is adopted to reduce the δ value.

if $\delta \in \left[2^n, 2^{n+1} \right)$(n=1,2,3,4,5,6,)

$\delta^{'} = \delta - 2^n$

$\lambda = n$

The value of λ corresponds to the pixel pair. The pixel pair is modified using $\delta^{'}$ as the final decision difference. Where λ and $\delta^{'}$ are reserved as steganographic keys for accurate extraction of secret information and restoration of the bearer image. According to the different characteristics of the parameters in accordance with the following rules to complete the modification of the pixel.

$$(p_i^{'}, p_{i+1}^{'}) = \begin{cases} p_i + \lceil \delta^{'}/2 \rceil, p_{i+1} - \lfloor \delta^{'}/2 \rfloor & \text{if} \quad d_i^{'} > d_i \text{ and } p_i \geq p_{i+1} \\ p_i - \lfloor \delta^{'}/2 \rfloor, p_{i+1} + \lceil \delta^{'}/2 \rceil & \text{if} \quad d_i^{'} > d_i \text{ and } p_i < p_{i+1} \\ p_i - \lceil \delta^{'}/2 \rceil, p_{i+1} + \lfloor \delta^{'}/2 \rfloor & \text{if} \quad d_i^{'} \leq d_i \text{ and } p_i \geq p_{i+1} \\ p_i + \lfloor \delta^{'}/2 \rfloor, p_{i+1} - \lceil \delta^{'}/2 \rceil & \text{if} \quad d_i^{'} \leq d_i \text{ and } p_i < p_{i+1} \end{cases}$$

$(p_i^{'}, p_{i+1}^{'})$ is the embedding of new information after the new pixel pairs, repeat steps (1) - (4), you can complete all the secret information embedded. Using all the modified pixel pairs $(p_i^{'}, p_{i+1}^{'})$ reconstruction can be obtained from the embedded image C.

Extraction and recovery process:

(1) Extracting a pair of pixels $(p_i^{'}, p_{i+1}^{'})$ from the embedded image C, while reading the corresponding λ with the pixel pair, computing the difference $d_i^{'} = \left| p_i^{'} - p_{i+1}^{'} \right| + 2^{\lambda}$ while restoring the carrier image by $\delta^{'}$, the recovery strategy is opposite to the embedding process. , At this time to restore the carrier image is the content of the protected ciphertext image, according to the principle of encryption to decrypt the anti-scrambling can be obtained in plaintext image.

(2) Determine the difference between the interval $d_i^{'}$ which is calculated for the pixel embedded secret information, that is a decimal number b, $b = d_i^{'} - l_k$ if $d_i^{'} \in [l_k, r_k]$

(3) The number of bits num_i of the secret information is calculated according to Equation 2, and b is converted into num_i -bit binary bits. The above steps are repeated until all the secret bits are extracted, and all the binary bit streams are reconstructed to obtain the secret information.

4. Experimental results and analysis

4.1 Hide capacity analysis

In order to verify the hidden capacity of the algorithm, three representative gray scale images with 512 512 pixels in the standard image library of matlab are used as embedding vectors. Considering the factors that influence the concealment capacity of PVD algorithm, the algorithm of the paper adds the scrambling encryption preprocessing before secret embedding. According to the interval division method in [6], Table 1 calculates the interval between the plaintext and the scrambled encryption of the number of pixel differences.

Table 1. Statistics of pixel difference before and after scrambling encryption

Interval	Peppers		Baboon		Lena	
	Not scrambled	Scrambled	Not scrambled	Scrambled	Not scrambled	Scrambled
[0,7]	96187	10832	54583	12978	99446	12204
[8,15]	24802	10943	32251	13407	19288	12805
[16,31]	7111	19686	27121	24359	8646	21179
[32,63]	2134	33142	14538	40419	3158	37193
[64,127]	687	43913	2575	36021	539	41096
[128,255]	157	12562	10	3894	1	7321

It can be seen, after scrambling encryption, the difference between pixels is amplified, the ability of the pixel to load secret information is enhanced. Respectively, in the literature [6] in the cryptographic domain information hiding algorithm, the original PVD algorithm hidden capacity, compared with the algorithm, as shown in Table 2

Table 2. Each algorithm hides the capacity contrast

Algorithm	Peppers	Baboon	Lena
Algorithm In The Literature[6]	36864	36864	36864
Algorithm In The Literature[8]	407302	457169	409817
Algorithm In This Paper	661191	622070	643531

It can be found that the algorithm has the best hidden capacity compared with the algorithms in [6] and [8]. On the one hand, in [6], the image is divided into several secret information bits by selecting the set, but the embedding rate is only 0.14, and the size of the block is also restricted because of the division of image blocks. The hidden capacity of the algorithm.

In this paper, according to different carrier images with adaptive algorithm to a pair of pixels for the embedded unit, and each pair of pixels can load 3 to 7 secret information, so the hidden capacity is more impressive. On the other hand, this algorithm makes full use of the characteristics of the PVD algorithm, which disrupts the correlation of the pixels in the plaintext and makes the difference of the pixels be fully utilized. Therefore, the algorithm [8] Good hidden capacity.

(If square brackets are not available, slashes may be used instead, e.g. /2/.) Two or more references at a time may be put in one set of brackets [3, 4]. The references are to be numbered in the order in which they are cited in the text and are to be listed at the end of the contribution under a heading References, see our example below.

4.2 Non-Sensibility Analysis

First, the perception of the algorithm is evaluated directly by the human eye senses. A Banboon image is taken as an example to compare the embedded ciphertext image with the original ciphertext image carrier. Embedded, the visual, ciphertext image is difficult to see changes. And decrypts the ciphertext image to obtain the restored carrier image.

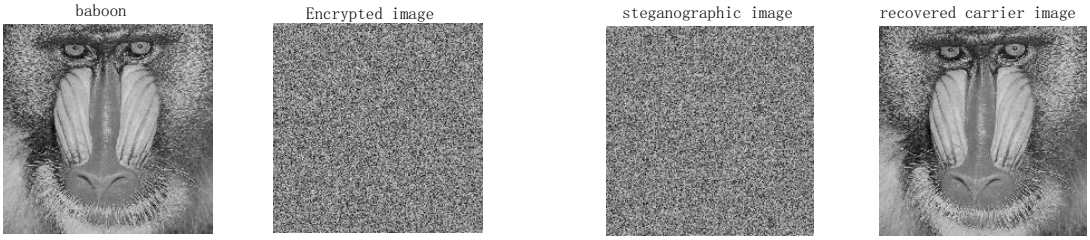

Fig.1 Contrast of Image Steganography and Restoration Effect

A binary watermark image with size of 64 × 64 is chosen as the secret information to test the ability of the algorithm to extract secret information. Figure 2:

Embedded watermark Extract the watermark

Fig. 2 Comparison of embedding and extracting secret information

It can be seen that the ciphertext image, it is difficult to see the changes in image quality, and reverse scrambling after restoration of the original image and steganographic images are no visual difference. Figure 4 also shows that the algorithm can accurately extract secret information.

Secondly, PSNR (Peak Signal to Noise Ratio) is used as the quantization standard to evaluate the quality of the image before and after embedding. The PSNR of the steganographic image is tested under the condition of low embedding, medium embedding and high embedding.

Table 3. Comparison of PSNR with low embedded volume

Algorithm	Pepers	Baboon	Lena
Algorithm in the Literature[8]	42.13	38.82	41.45
Algorithm in this Paper	46.22	43.07	47.83

Table 4. Comparison of PSNR with moderate embedding

Algorithm	Peppers	Baboon	Lena
Algorithm in the Literature[8]	40.30	36.79	41.13
Algorithm in this Paper	44.34	40.61	45.28

Table 5. Comparison of PSNR at full embedding

Algorithm	Peppers	Baboon	Lena
Algorithm in the Literature [8]	30.71	31.01	30.59
Algorithm in this Paper	35.60	35.32	34.77

Experimental results show that the improved algorithm can effectively improve the imperceptibility of the algorithm. The PSNR varies with the embedding amount. The more the secret information is embedded, the lower the PSNR is. This is the contradiction between hidden capacity and imperceptibility. The original PVD algorithm calculates the difference directly for the pixel pair after modification, and this algorithm reduces the difference and then acts on the pixel pair, and thus get a better imperceptibility.

5. Summary

In this paper, a cryptographic domain information hiding algorithm based on PVD is proposed. Through the original algorithm, the hidden capacity is positively correlated with the difference of the pixel pair, and the embedding quantity is decided by the interval. Thus expanding the pixel difference so that a pair of pixels can load the secret information is greatly improved, thereby further enhancing the hidden capacity. At the same time, by reducing the decision difference for modifying the pair of pixels, the invisibility of the algorithm is effectively improved while the hidden capacity is kept, and the effectiveness of the algorithm is verified by experiments.

References

[1] De V.C, Delaigle J.F, Macq B.Circular interpretation of bijective ransformations in losslessfor me dia asset management [J].IEEE Transactions on Multimedia, 2003, 5(I):97-105.

[2]HongW, Chen T S, Wu H Y. An improved reversible data hiding in encrypted images usingside ma tch [J]. IEEE Signal Processing Letters, 2012, 19(4); 199-202.
[3] Zheng Shuli, Li Dandan, Hu Donghui, et al. Reversible Information Hiding in Image Cryptosyste m Domain Based on Histogram Modification [J] .Microelectronics and Computer, 2015, 32 (12) 105-109.
[4] Zhang Minqing, KE Yan, SU Tingting Reversible Information Hiding in Ciphertext Domain Base d on LWE[J] Journal of Electronics and Information Technology, 2016, 38 (2): 354-360.
[5] Cheng Hang, WANG Zi-chi, ZHANG Xin-peng. Reversible Information Hiding in Encrypted Do main Based on Image Block Grouping [J]. Journal of Beijing Polytechnic University, 2016, 42 (5): 722-728.
[6] WANG Zi-Chi, ZHANG Yuan, ZHANG Xin-Peng. Reversible Information Hiding Method for E ncoded Images with Multi-bit Embedding [J] .Small Microcomputer System, 2014, 35 (10): 2331-2335.
[7] Da-Chun Wu, Wen-Hsiang Tsai. A steganographic method for images by pixel value differncing[J]. Pattern Recognition Letters, 2003, 24(9-10):1613-1626.
[8] Wang C M, Wu N I, Tsai C S, et al. A high quality steganographic method with pixel-value differ encing and modulus function [J]. Journal of Systems & Software, 2008, 81(1):150-158.
[9] Hong W, Chen T S, Luo C W. Data embedding using pixel value differencing and diamond encod ing with multiple-base notational system [J]. Journal of Systems & Software, 2012, 85(5):1166-11 75.
[10] Shang Yanhong. Digital image encryption technology research [D]. Beijing, North China Univers ity of Technology, 2005