Research and Implementation of Reversible Information Hiding Technology for Gray Image Based on Wavelet Transform

Shaomin Xie, Tingping Fan, Jing Huang

School of Computer Engineering, Guilin University of Electronic Technology, Guangxi, Beihai, 536000, China

Keywords: Wavelet transform; Gray image; Reversible information; Hiding technology

Abstract: For a gray image, it is not difficult to modify the values of some pixels purposefully with the guidance of a certain strategy to hide a certain amount of information. Information hiding technology shifts the focus of information security from simply encrypting secret information to how to make the embedding of secret information imperceptible. The standardization of information security is relatively backward, high-end talents and their plaques are scarce, while the competition among low-end talents is fierce, and the task of Internet security management is extremely arduous. In this paper, the reversible information hiding technology of gray image is studied based on wavelet transform, and it is verified by experiments that the wavelet transform proposed in this paper uses these characteristics to obtain higher visual quality and peak signal-to-noise ratio of watermark image. In order to achieve this goal, the embedding process always chooses to embed data in the subband of the first-stage integer wavelet transform. This not only makes illegal attackers spend energy to get all the contents needed to recover confidential information, but also makes the owners of confidential information contain each other and improve the confidentiality of information.

1. Introduction

With the rapid development of the Internet, the transmission and exchange of information has become increasingly simple and fast. People can freely send files or chat using email, WeChat, QQ, and other application tools [1]. They can also easily modify original files, and even use the network to carry out illegal actions. It can be seen that the Internet is also a double-edged sword, with many conveniences often accompanied by some information security risks. Currently, the main technologies include secure channel, encryption technology, and information hiding. Secure channel refers to the establishment of a private physical or virtual private network by both communication parties, which cannot be accessed by others [2]. The advantages of this method are high security, while the disadvantages are high cost and poor expansion function. Gray scale images have large data redundancy and sufficient logical redundancy space to hide information, and are often used as carriers of secret data.

For a grayscale image, it is not difficult to purposefully modify the values of some pixels under the guidance of a certain strategy to hide a certain amount of information. Information hiding technology has shifted the focus of information security from simply encrypting secret information to making it difficult to detect the embedding of secret information. Obviously, compared to information encryption, information hiding technology is more secure. The number of grayscale images is countless, and there is a large amount of redundancy in grayscale images themselves. At the same time, it is difficult for the human eye to detect small changes in the image, so grayscale images become a major carrier of information hiding [3]. Encryption technology is currently widely used, with the advantage of simple implementation, while the disadvantage is that the chaotic state of the ciphertext also indicates the existence of confidential information and is vulnerable to attacks. The standardization of information security is relatively lagging behind, lacking corresponding theoretical guidance, and the contradiction between the demand and supply of information security professionals is prominent. While high-end talents and their talents are scarce, the competition for middle and low-end talents is fierce. The task of Internet security management is extremely arduous

  DOI: 10.25236/icmmct.2023.021

[4-5].

Therefore, this paper proposes a grayscale image fusion algorithm based on wavelet transform and color space transformation, and determines the dynamic fusion weight based on the grayscale standard deviation, gradient factor, and grayscale mean value. After wavelet transform, a series of sub images with different resolutions can be obtained from an image. Subimages with different resolutions correspond to different frequencies. The low-frequency band is the best approximation of the original image, while the high-frequency band is only the detailed information of the image. Embedding confidential information into another type of public multimedia information for transmission, utilizing the visual effects of public media to effectively disguise the presence of confidential information to avoid attacks [6]. According to different needs, different image coefficients are obtained to obtain different image features.

2. Basic knowledge of reversible information hiding in gray image

2.1. Information hiding technology

Nowadays, in many practical applications, information hiding and information encryption are combined, that is to say, the attacker must first judge whether there is ciphertext information in the carrier, and then extract ciphertext from it and decrypt it to get plaintext. There can be no mistakes in these links, otherwise the secret information will not be obtained, which shows that the combination of the two is more reasonable and safer [7]. Information hiding, or data hiding, is a more general term, which includes a wider range of embedding information in carrier content. Hiding can make information imperceptible or keep the existence of secret information. Such as digital watermarking and steganography. Steganography is a common form of covert communication, and the existence of messages is hidden. The carrier form of information hiding can be any kind of digital media, such as image, sound, video and text, but the most mature information hiding carrier is digital image. In order to strengthen concealment! Encryption mechanisms are usually also introduced. The structure of an information hiding system with encryption mechanism is shown in Figure 1.

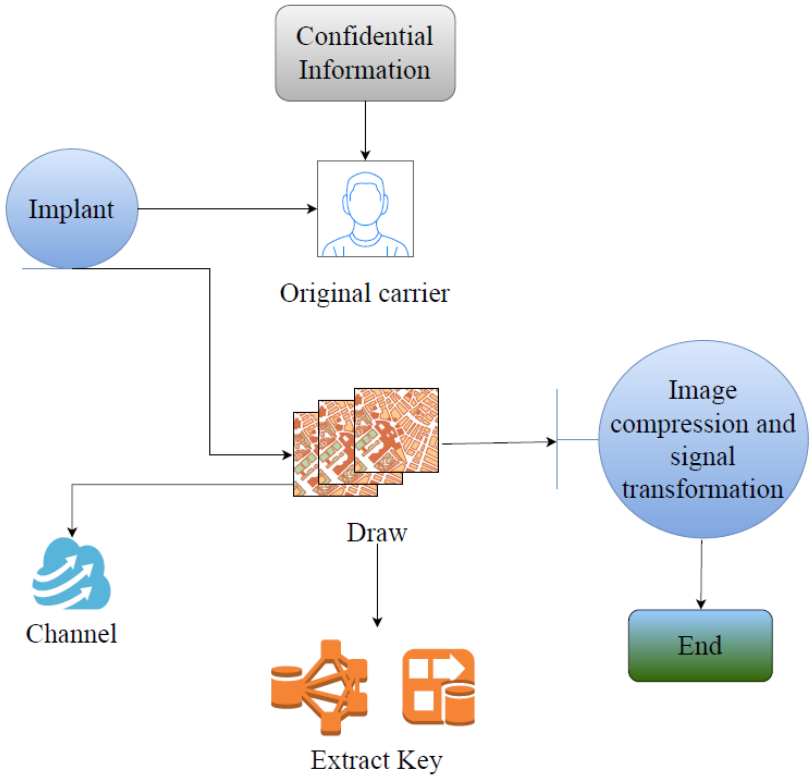

Figure 1 Information Hiding System Structure

Some private information, such as copyright information and serial numbers, is transmitted as

confidential information by the sender using multimedia data such as text, video, images, and audio as carriers. The receiver uses a detector and a key to extract secret information from the encrypted carrier. The required data load may vary significantly depending on the application. For example, copy protection or copy control applications require only a few bits of information, such as a few seconds or minutes of information in audio and video, and only a secret message or name string in an image to implement the function [8]. Generally, covert information is relatively small compared to the carrier, and its modification amount is very small. However, human senses are relatively late and pure, and it is not easy to detect small changes. It should be noted that nowadays, the requirements for imperceptibility have become higher, and some general inspection tools must also ensure that they cannot detect the concealment of hidden information.

2.2. Basic principle of reversible information hiding technology for gray image

Most of the early image information hiding algorithms ignored the integrity of the carrier image, which led to the permanent destruction of the original carrier image. This kind of destruction is not desirable in some situations, so the idea of reversible information hiding is put forward, and the integrity of the original image is also solved. Compared with other characteristics, the misjudgment rate to be achieved depends on the purpose of the strategy in specific applications [9]. In the application of copy control, if a content without watermark is often misjudged, it may lead to serious trouble, so in this case, the misjudgment rate is expected to be infinitely small. The security of information hiding system is very similar to the security of cryptographic system. The algorithm of information embedding is public, and the security is based on key management. Only when you have the key can you extract information. The object that has hidden secret information is called camouflage media. According to different host media, hidden information can be divided into sound information hiding, text information hiding, video information hiding and image information hiding. The hidden information can also be in the form of the above digital media, but they are all treated as bit streams when hidden.

Reversible information hiding can also be called lossless hiding or erasable information hiding, which aims to enable the receiver to obtain the secret information embedded by the sender from the received secret image, and at the same time restore the original carrier image. Because encryption technology can prevent unauthorized reading and writing messages, it can be used in watermarking system to prevent passive attacks and forgery, and can prevent watermark removal attacks. The existence of Mi Lang makes it impossible for the decoding end to obtain the correct watermark information without the correct key even if the watermark algorithm is public. It should be noted that the principle of reversible information hiding requires that gray-scale images need lossless transmission, that is to say, any change to dense gray-scale images will lead to the failure of obtaining secret information and original images [10].

3. Research on reversible information hiding technology for grayscale images based on wavelet transform

3.1. Wavelet Analysis of Gray Image

Wavelet analysis includes wavelet inverse operations of wavelet decomposition, which are based on the selection of a suitable wavelet function. Because grayscale images do not have channel components. Due to the differences in focus changes between the components of a color image and the channel components of a standard color image, if you want to achieve better fusion of grayscale and color images with different focuses, you need to process the color image channel image [11].

When the grayscale image embedded with the watermark is modified or maliciously attacked by a user, a certain part of the image will usually be damaged or lost, which will also cause a certain part of the embedded watermark image to be damaged or lost. After extracting the damaged watermark image, the watermark image can be restored using Arnold transform. Figure 2 is a block diagram of the structure of grayscale image and wavelet transform fusion. The specific algorithm steps are as follows: first, perform color space conversion on the two source images, and switch

from color space structure to color space structure.

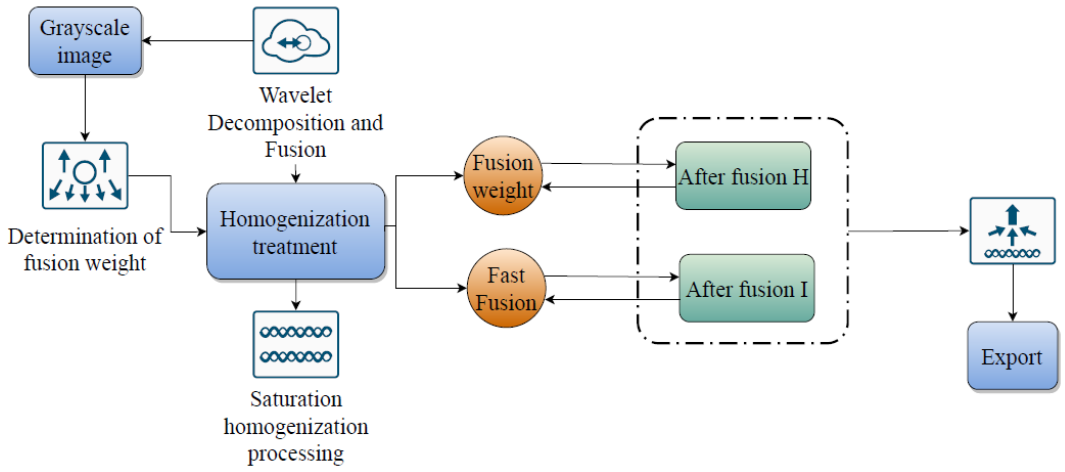

Figure 2 Structural block diagram of grayscale image and wavelet transform fusion

According to the impact of image brightness on saturation in actual photography, the better the ambient light in actual photography, the richer the color category information that can be obtained. These methods have certain advantages in single frame still image fusion, but in complex and dynamic environments, fixed fusion coefficients are obviously not suitable, and the establishment of dynamic fusion coefficients is the key to supporting dynamic fusion. The earliest orthogonal wavelet function with tight support used in wavelet analysis is also the simplest wavelet function. The definition of its scale function for a single rectangular wave within the support domain $t \in [0,1]$ is shown in Equation (1):

$$\varphi(t) = \begin{cases} 1 & 0 \le t \\ 0 & 0 \le 1 \end{cases} \quad (1)$$

The corresponding wavelet function is shown in Equation (2):

$$\psi(t) = \begin{cases} 1 & 0 \le t \\ 0 & 0 \le 1 \end{cases} \quad (2)$$

For an image with a size of $N \times N$, the transformation operation is shown in Equation (3):

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} N, \quad x, y \in \{0,1,2,\cdots N-1\} \quad (3)$$

Wavelet transform can better match characteristics, so we combine characteristics in the wavelet domain to establish a visual threshold model and define a visual masking function. During the process of adding watermark to a grayscale image, we ensure that the amplitude of the watermark added to each wavelet coefficient does not exceed the distortion that this coefficient can mask.

3.2. Experimental analysis

According to the different color information of pixels, gray-scale images can be divided into binary images, gray-scale images and color images. The ultimate users of gray-scale images are human eyes, and the pixel values of two digital images with the same quality perceived by eyes may be very different, which provides a great research space for distortion compression and information hiding of gray-scale images depending on the imperfection of human visual system. Then, there are a lot of redundant information in most images, because except at the edge of the image, the image

In order to reduce the size of the mapping array, the original mapping array can be easily reduced. The watermark information is hidden in the low-frequency component of each block, which is mainly because most of the energy of the original image is taken into account in the low-

frequency scale sub-atlas, and the amplitude of the coefficient is much larger than that of the detail sub-graph, so the perceptual capacity is larger, which is beneficial to the embedding of the watermark. From the data in Table 1, it can be seen that the contrast of the gray-scale image after saturation homogenization after wavelet transform is obviously improved. Image clarity and detail richness have also been significantly improved.

Table 1 Comparison of saturation before and after homogenization

	Gray Left Blur	Color Right Blur Image	No saturation treatment performed	Saturation homogenization
Gray scale standard deviation	0.3124	0.2135	0.1862	0.1758
Relevance	0.8745	0.8547	0.8867	0.9024
Contrast ratio	0.5133	0.3458	0.3785	0.4024
Uniformity	0.7542	0.7248	0.7862	0.8035

Making full use of the confusion inherent in exposing grayscale images using wavelet transform reduces the attention of attackers, thereby greatly protecting the security of grayscale images. The wavelet coefficients of different subbands have different energies and have different effects on the resulting watermark image and distortion level. The wavelet transform proposed in this paper utilizes these characteristics to obtain higher visual quality and peak signal to noise ratio of the watermark image. To achieve this goal, the embedding process always chooses to embed data in the subbands of the first level integer wavelet transform. This not only makes illegal attackers expend energy to obtain all the content needed to recover confidential information, but also makes the owners of confidential information check each other, improving the confidentiality of information.

4. Conclusions

In this paper, the advantages of blocking and wavelet transform are combined, and the advantages of integer wavelet lifting algorithm are fully utilized. The image is blocked first and then transformed, which is more robust to shearing attacks. The wavelet decomposition of gray image has good frequency division characteristics, and the obtained sub-bands can be well combined with human visual system. For example, the low-frequency sub-band concentrates most of the energy and is an important part of human visual system, and the distribution of coefficient values in the high-frequency sub-band conforms to Laplace distribution, especially the most coefficient values in the high-frequency sub-band concentrate on zero, which is very suitable for embedding watermark by histogram shifting method. Experiments show that the wavelet transform proposed in this paper uses these characteristics to obtain higher visual quality and peak signal-to-noise ratio of watermark images. In order to achieve this goal, the embedding process always chooses to embed data in the subband of the first-stage integer wavelet transform. This not only makes illegal attackers spend energy to get all the contents needed to recover confidential information, but also makes the owners of confidential information contain each other and improve the confidentiality of information. Make full use of the confusion of the public gray-scale image itself, reduce the attacker's attention, thus protecting the security of the gray-scale image to a great extent.

References

[1] Naik K. Pal A K. A Cryptosystem for Lossless/lossy Grayscale images in IWT domain using Chaotic map based Generated key matrices[J]. International Journal of Wavelets Multiresolution and Information Processing, 2021, 16(7):18-31.

[2] Gao F. Infrared and visible image fusion using dual-tree complex wavelet transform and convolutional sparse representation[J]. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 2020, 39(32):58-74.

[3] Ma G. Wang J. Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform[J]. Signal Processing: Image Communication, 2022, 75(20):55-63.

[4] Ma G. Wang J. Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform[J]. Signal Processing. Image Communication: A Publication of the the European Association for Signal Processing, 2019, 48(75):75-87.

[5] Duevedi M. Muttoo S K. An Improved Separable and Reversible Steganography in Encrypted Grayscale Images[J]. International Journal of Information Security and Privacy, 2021, 15(2):1-28.

[6] Kapadia A M. Pandian N. Reversible data hiding methods in integer wavelet transform[J]. International journal of information and computer security, 2020, 12(1):70-89.

[7] Xiong Y Q. An integer wavelet transform based scheme for reversible data hiding in encrypted images[J]. Multidimensional systems and signal processing, 2022, 29(3):11-27.

[8] Ma G. Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform[J]. Signal Processing. Image Communication: A Publication of the the European Association for Signal Processing, 2019, 63(20), 75-89.

[9] Babu S A. Perumal E. Wavelet Based Improved Coding Techniques (WBIC) for grayscale images using lossy compression[J]. International Journal of Pure and Applied Mathematics, 2022, 118(8):51-62.

[10] Savi A G. Prokin M. Rajovi V M. et al. Memory Efficient Hardware Architecture for 5/3 Lifting-Based 2-D Forward Discrete Wavelet Transform[J]. Microprocessors and Microsystems, 2021, 87(17):104176-104197.

[11] Amk A. Pn A. Secured Reversible matrix embedding based on dual image using Integer wavelet and Arnold Transform[J]. Procedia Computer Science, 2019, 165(58):766-773.