REVERSIBLE DATA HIDING TECHNIQUES AND ITS APPLICATION IN INFORMATION SECURITY

Phuoc-Hung Vo*

Abstract – Reversible data hiding is widely recognized as one of the most employed methods for copyright protection and data security. This technique involves embedding a unique piece of information, commonly known as a watermark or secret data, without being detected by human or machine visual systems. Moreover, the original image is completely restored after embedded information is extracted by the recipient. Reversible data hiding technique has many significant applications, such as camouflage in communication to protect confidential information or embedding information into photos to protect digital image content.

Keywords: reversible data hiding, steganography, watermarking.

I. INTRODUCTION

With the explosion of information technology and science and technology development, humanity is entering a new era, the era of digital transformation. In recent years, a vast amount of information involving the fields of economy, culture, society, education, and military has been digitalized, stored in the cloud, and distributed through the system network. Although the Internet is considered a means of communication due to its convenience for exchanging information on demand, the Internet environment also gives people numerous risks. When the digital transformation is going in-depth, more digital information is remotely communicated via the network, especially private information that attracts the attention of illegal users aiming to steal, fake, and change intentional information content.

Today, more than ever, the strong development of informatics criminals with available tools online has been working around the world. It is also a critical matter that restricts the economic and social development of countries if there is no effective solution to prevent that wave.

Information safety and security become an important guarantee for economic and social development in the fields of communication, storage, content policies, and data authentication. The method of ensuring information security is also known as information security and network security techniques. This technique is designed to protect information against attacks. Currently, the two techniques to ensure the safety of information are information encryption (cryptography) and information hiding (steganography). Information encryption is a technique that stops hackers from understanding the content of the plaintext. Information encryption is mostly accessible to applications that protect the safety of information by translating clear information into meaningless forms. Meanwhile, information hiding is the technique of embedding the content of confidential information to be protected into other information so that the hackers do not detect hidden information or embed the content of the information into other information that needs to be told. Thus, the steganography technique not only ensures the secret of information hidden during the transmission process but also protects the content of the object with hidden information. With such technical characteristics and properties, steganography is becoming a new approach in the field of information security. It is used a lot for security applications, camouflage in communication, and information content protection, especially in electronic transactions on the Internet environment, an open network environ-
Figure 1 illustrates the classification of secure communication.

![Fig. 1: Classification of information security techniques](image)

The important benefit of steganography methods over cryptography is that they can hide the existence of secret information. On the other hand, one can easily recognize an encrypted data file by seeing the content even though they cannot infer anything from that. Steganography is a functional approach to protect data since it allows concealing data in a host (cover) without losing its value. Figure 2 demonstrates the steganography system.

![Fig. 2: Steganography system](image)

II. METHODS OF STEGANOGRAPHY AND EFFICIENCY PARAMETERS

A. Methods of steganography

The main objective of the data hiding technique in the image is to keep safe communication in the network environment by inserting information into the image to protect the inserted information or the image itself [1]. In recent years, the technology of hidden information has been widely used in many fields of industry and academia [4–6]. Due to different application purposes and embedded processes, the hiding techniques can be divided into different ways. This classification is based on the image data domain, the ability to recover images or image type.

Existing data concealing methods have a relatively limited embedding capacity (the number of bits that can be hidden in an image). Aiming to increase picture embedding capacity while keeping the peak signal-to-noise ratio (PSNR) below allowable levels, various data concealment strategies have been applied. There are two types of data hiding methods: reversible data hiding (RDH) and non-reversible data hiding (non-RDH). In RDH approaches, the actual cover medium can be restored while extracting the hidden details. In non-RDH methods, the original cover medium is irrevocably corrupted and cannot be recovered later. Military and intelligence communication, private communication, and protecting civilian speeches from attackers all use RDH algorithms. The RDH schemes are very popular in medical image transmission to hide patient reports in the medical image. This provides a way to transmit the medical image text files as a single entity instead of sending them as two different entities. Data hiding techniques include steganography, digital watermarking, and RDH.

B. Efficiency parameters

To evaluate the performance of data hiding schemes, the embedding capacity (payload) which is often measured in bits or bit per pixel (bpp) is estimated by embedding rate with the unit of bits per pixel (bpp). The embedding rate is calculated by the following equation:

\[
bpp = \frac{\text{number of embedded bits}}{\text{number of pixels of cover image}}
\]

The visual quality of the stego-image is evaluated by a peak-signal-to-noise (PSNR) in decibels (dB). PSNR measures the embedding distortion due to data embedding in terms of mean square error (MSE). The similarity between the cover
image and the stego-image given by:

$$PSNR = 10 \times \log_{10}\frac{255^2}{MSE} \tag{2}$$

where MSE is defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{H} \sum_{j=1}^{W} (x_{i,j} - x'_{i,j})^2 \tag{3}$$

with $H$ and $W$ refer to the height and width of the cover image, $x_{i,j}$ and $x'_{i,j}$ refers to the pixels located at the $i$ th row and $j$ th column of original image and stego-image, respectively.

To evaluate the robustness property of the proposed scheme, bit correlation error (BCR) is used to measure the correction ratio of the extracted watermark.

$$BCR = \sum_{i=1}^{n \times m} \frac{n \times n \times 100}{w_i \oplus w'_i}$$

where $w_i$ and $w'_i$ are the $i$ th binary value of the original watermark and of the extracted watermark, respectively. Notation $\Theta$ indicates an exclusive-OR operator.

III. RELATED WORKS

A. Related works on reversible data hiding

In this section, the research tries to express a high-capacity invertible steganography method using 2-D histogram shifting with EDH [7]. To achieve a balanced relationship between the embedding capacity and the visual quality, our method utilized an embedding direction histogram (EDH) encoded from analyzing the secret data. The EDH plays an important role in shifting 2-D histograms and embedding information. Figure 3 reveals the main processes of the embedding procedure. First, according to the secret data, EDH is generated. Next, based on pre-selected threshold $T$, the left and the right blocks in the DCT domain are considered whether they are similar or not. Then, a 2-D histogram is constructed for embedding the secret data based on the EDH.

Each view of the stereo image is separated into blocks sized $8 \times 8$ and applied DCT transformation. After quantization, the image signal energy focuses on low frequency areas, so the DC coefficient and five first AC coefficients of each block are gathered and calculated to identify whether they are similar or not. The findings of similar block algorithms can be offered as follows:

1. **Input**: $B^l_i$, $B^r_i$, $t$
2. **Output**: $B'^{lm}_i$ or $\emptyset$
   - find out similar block with $B^l_i$ block or $B^r_i$
3. $V^l_i \leftarrow zigzag(B^l_i)$
4. for $B^r_i$ ($i \equiv +k, -3 \leq k \leq +3$)
5. $\{V^r_k \leftarrow zigzag(B^r_k)\}$
6. $Diff_i \leftarrow \sum_{v \geq 0} [V^l_i - V^r_i]$
7. **Endfor**
8. if $\min\{Diff_i\} \leq t$
   - $\emptyset$ threshold $t$
9. return $B'^{lm}_i \leftarrow B^l_i$
10. else return $\emptyset$
11. **Endif**

Based on the similarity of the left and right image blocks, the 2-D histogram is designed to embed information. In addition, research shows that quantization coefficients in the area embedded in two blocks are usually positive integers. Therefore, to ensure the quality of the image after embedding, the process of moving the coefficient to embed information is done in the positive area of the 2-D schema (East-North area). Moreover, according to the proposed solution, when there are many coefficients of two blocks equal to ‘0’, the higher the dip performance. Therefore, the method of proposing to ensure the efficiency of stego-image and highly embedded performance.

B. Related works on reversible watermarking

Reversible watermarking is a technique that is widely used to protect the rightful ownership of digital images. In this section, the article represents a robust hybrid watermarking scheme
based on DCT and SVD for copyright protection of stereo images [8]. Based on the properties of the stereo image, the procedure of reversible watermarking first begins by finding similar blocks, which are based on the coefficients in the frequency domain. Next, the process embeds a watermark image. The watermark image is embedded in the coefficient SVD transformation, which is shown as follows:

```
1: Input: similar blocks $B^l$ and $B^{rim}$, $w (4 \times 4)$, $\sigma$: robustness factor
2: Output: $wB^l$, $wB^{rim}$
3: $B^{det}_DCT \leftarrow DCT(B^l)$
4: $B^{rim}_DCT \leftarrow DCT(B^{rim})$
5: for $(i, j) \leftarrow 0: 3$
6: if $(j < 2)$
7: $A(i, j) \leftarrow B^{det}_DCT(u, v)$ where $(u + v = 7)$
8: else
9: $A(i, j) \leftarrow B^{rim}_DCT(u, v)$ where $(u + v = 7)$
10: Endif
11: Endfor
12: $[U, S, V^T] \leftarrow svd(A)$
13: $wS \leftarrow S + \sigma \cdot w$ \( \sigma \) robustness factor */
14: $[U^*, S^*, V^T] \leftarrow svd(wS)$
15: $wA \leftarrow U^*S^*V^T$
16: for $(u, v) \leftarrow 0: 7$
17: if $(u + v = 7)$
18: $wB^{det}_DCT(u, v) \leftarrow wA(i, j) \forall(i, j = 0: 3, j < 2)$
19: $wB^{rim}_DCT(u, v) \leftarrow wA(i, j) \forall(i, j = 0: 3, j \geq 2)$
20: elseif
21: $wB^{det}_DCT(u, v) \leftarrow B^{det}_DCT(u, v)$
22: $wB^{rim}_DCT(u, v) \leftarrow B^{rim}_DCT(u, v)$
23: endif
24: Endfor
25: $wB^l \leftarrow IDCT(wB^l_DCT)$
26: $wB^{rim} \leftarrow IDCT(wB^{rim}_DCT)$

IV. CONCLUSION

This work discussed the importance of secure communication, especially during image transmission. The paper also discussed the motivation to work in the domain of reversible data hiding. The extension of reversible data hiding called reversible watermarking schemes is also presented. Various well-known reversible data hiding schemes are briefed.

REFERENCES