**Improved Reversible Data Hiding Scheme using Weighted Matrix with Overlapping**

Kwang-Yeol Jung, Dae-Soo Kim, Young-Ju Kim, Kee-Young Yoo\*

School of Computer Science and Engineering

Kyungpook National University

Daegu, South Korea

jasp1234@infosec.knu.ac.kr, stairways@infosec.knu.ac.kr, kyj@knu.ac.kr, yook@knu.ac.kr

\*Corresponding Author

***Abstract*— The purpose of data hiding is hiding existence of the secret data. It should not be detected by adversary or others. Data hiding techniques are applied to widespread area in general digital format such as image, text, audio, video, etc. Jung and Yoo first proposed data hiding through image interpolation using neighbor mean interpolation. Then Lee and Huang presented higher capacity image hiding by interpolating with neighboring pixels. In 2016, Jana proposed high payload reversible data hiding scheme using weighted matrix. His scheme can reversible using weighted matrix. Also his scheme has high-level security by updating weighted matrix each block operation with secret key *k*. But his scheme has low hiding capacity. To improve this problem, we proposed the improved reversible data hiding scheme using weighted matrix with overlapping. Our scheme has more embedding capacity keeping similar PSNR.**

Keywords—Reversible, Data Hiding, Interpolation, Weighted matrix

# **Introduction**

In nowadays, we can encounter so many kinds of digital media due to development of IT technology. With the development, security problems about digital media such as duplication, interception, modification and forgery are also emerged. To prevent the security problems, many cryptosystems [1] are already proposed and are used for keeping secret data secure by encryption. However, an adversary can easily detect the presence of some meaningful data in encrypted data. Data hiding is proposed to solve this detect problem.

The purpose of data hiding is hiding existence of the secret data. It should not be detected by adversary or others. Data hiding techniques are applied to widespread area in general digital format such as image, text, audio, video, etc. In the case of image, there are two kinds of image. The image which used to embed secret data is called cover image and after embedding secret data into cover image, it is called stego image. When sender want send to receiver, sender embeds secret data into cover image first, and then sender sends to receiver the stego image. During the sending in insecure channel, anyone can catch that the stego image has secret data. They can only see normal image like common images. After receiving the stego image, receiver extracts secret data in the stego image. By this way, the secret data can be send in high-level security. It can also uses some encryption methods like DES, AES, RSA, ECC into secret data before embedding to get more security. When receiver receives the stego image, if receiver can not only extract the secret data, but also recover the cover image, we can consider that the stego image is embedded by reversible data hiding method. Reversible data hiding is proposed to solve that receiver can not recover the cover image. Reversible data hiding is used in very wide field, especially it is used in sensitive field such as medical and military field. That fields use the reversible data hiding methods because of its property.

In 2006, the first reversible data hiding scheme was proposed by Ni et al [2]. Their scheme adjusts the pixel values of the cover image. It used the peak point and the zero point pixel values in the cover image to embed secret data. But capacity of their scheme was limited by the most frequent pixel values in the cover image.

After Ni et al.'s scheme, many kinds of reversible data hiding schemes were proposed [3-10]. Jung and Yoo [11] first proposed data hiding through image interpolation using neighbor mean interpolation with payload 2.28 bpp. Then Lee and Huang [12] presented higher capacity image hiding by interpolating with neighboring pixels. In 2016, Jana [13] proposed high payload reversible data hiding scheme using weighted matrix. His scheme can reversible using weighted matrix. Also his scheme has high-level security by updating weighted matrix each block operation with secret key k. But his scheme has low capacity.

In this paper, an improved reversible data hiding scheme using weighted matrix with overlapping is proposed to solve the problems of Jana's scheme. An improved reversible data hiding scheme using weighted matrix with overlapping has more embedding capacity keeping similar peak signal-to-noise ratio(PSNR) than Jana's scheme.

This paper is organized as follows. Section II, the background knowledge is introduced and Jana's scheme is reviewed. Section III, the embedding, extraction and recovery procedures of the proposed method are presented. Section IV, explains experimental results about embedding capacity and PSNR between the proposed scheme and the Jana’s scheme. Finally, Section V concluded this paper.

# **Related Works**

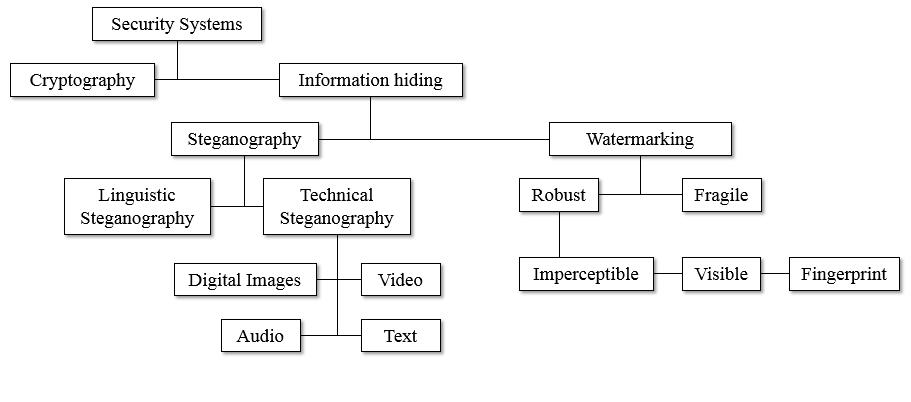


Fig. 1 Category in security system

## Data Hiding

Data hiding is generally categorized into steganography and watermarking. Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data. The carrier can be anything used to transfer information, including, for example, wood or slate tables, hollow heels, images under stamps, tiny photographs, or word arrangements. Digital carriers include e-mail, audio, video messages, disk space, disk partitions, and images.

Steganography and cryptography technics have been used throughout recorded history as means to add elements of secrecy to communication. However, cryptographic techniques scramble a message so that if it is intercepted, it cannot be understood.

Digital watermarking involves information embedding techniques that convey some information about the carrier. Since watermarks are embedded in more significant areas of digital media, watermarking techniques may be applied without fear of image destruction due to lossy compression. In some cases, digital watermarks may be advertised or are visible.

Visible watermarks are not steganography by the definition. The difference between steganography and watermarking is primarily one of intent. Traditional steganography conceals information; watermarks extend information and may be considered attributes of the cover image. Digital watermarks may include information such as copyright, ownership, or license. In steganography, the object being communicated is the cover and the watermarks provide additional information about the cover. Figure 1 shows the category in security system.

## Data Hiding using Weighted Matrix

An integer weighted matrix *W* will be shared by sender and receiver before data communication. The criterion of preferring *W* is that each element of matrix is arbitrarily allotted a value from the combination and each element appears at least once in *W*, where *r* denotes the number of secret bits those will be embedded into each block of cover image . Next, it will embed *r* data bits, say into image block using the following Equation (1).

|  |  |
| --- | --- |
|  | (1) |

where denotes entry-wise multiplication operator and number of blocks. The function represents the modular summation of all the entries of matrix . If d is equal to zero modulo then is intact; otherwise, modify to to satisfy the following Equation (2).

|  |  |
| --- | --- |
|  | (2) |

The receiver can derive by computing . There exists high-risk security vulnerability in special case, because an attacker will be able to estimate the form of weight matrix by using brute-force attack.

## The review of Jana’s scheme

In 2016, Biswapati Jana proposed high payload reversible data hiding scheme using weighted matrix. This scheme can reversible different from presented schemes because of position values. To achieve high capacity, it is computed twelve times sum of entry-wise multiplication on a single block. To improve the security, it is updated weighted matrix twelve times for each block of cover image and is used secret key *k* using update weighted matrix. This scheme interpolates from original image that size of to cover image that size of like Figure 2. Jana’s scheme has high embedding capacity compare with other schemes keeping good PSNR.

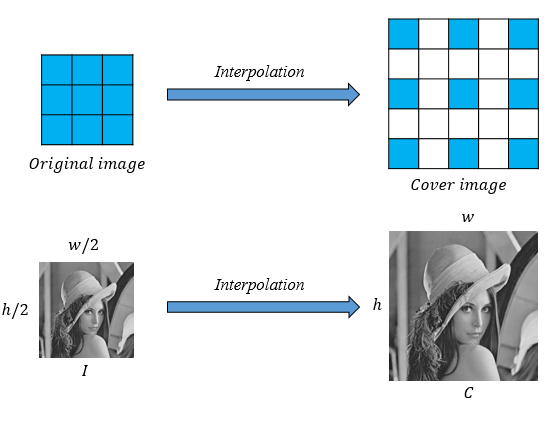


Fig. 2 Interpolation from Original image to Cover image

# **Proposed Scheme**

We proposed new scheme that has more embedding capacity than Jana’s scheme. We used overlapping at neighbor pixels. The proposed scheme used four more interpolated pixels in a block in the cover image. So our scheme can embed 64bits in each block. The proposed scheme consists of the following three phases: (1) Initialization phase, (2) Embedding phase and (3) Extraction phase. Before send the image, initialization phase is performed first. The sender performs embedding phase and the receiver performs extraction phase.

## Initialization Phase

In cover image, if it’s both row value and column value of a block are odd than just follows equation (3).

|  |  |
| --- | --- |
|  | (3) |

If the row value is odd and the column value is even than follows equation (4).

|  |  |
| --- | --- |
|  | (4) |

If the row value is even and the column value is odd than follows equation (5).

|  |  |
| --- | --- |
|  | (5) |

If both the row value and the column value are even than just follows equation (6).

|  |  |
| --- | --- |
|  | (6) |

After that, weighted matrix is filled .

## Embedding Phase

In embedding phase, the sender follows these steps.

1. Select block from the original image.
2. Get *Val* value after compute sum of entry-wise multiplication weighted matrix and original image block like equation (7).

|  |  |
| --- | --- |
|  | (7) |

1. Calculate *pos* value by subtracting *Val* from secret bit value that converted as a decimal.

|  |  |
| --- | --- |
|  | (8) |

1. If is bigger than 8 or smaller than -8, then modify the value should be smaller than 8 and bigger than -8.
2. Add or subtract *pos* value at interpolated location of cover image.
3. Loop continue sixteen times in a block. After sixteen times, updated like equation (9). In the equation, is selected where .

|  |  |
| --- | --- |
|  | (9) |

1. When all the loop is ended, we can get the stego image.

## Extraction Phase

In extraction phase, the receiver follows these steps inverse order because of overlapping blocks.

1. Select block from the original image.
2. Calculate interpolation about *Inpo* value that be made by same equation (3) - (6).
3. Calculate *pos* value by subtracting *Current value* from *Inpo* value.

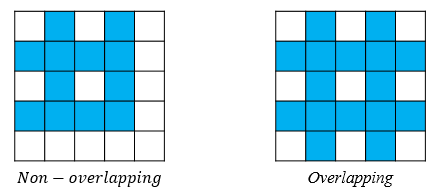


Fig. Comparison of embedded pixels with non-overlapping and overlapping

|  |  |
| --- | --- |
|  | (10) |

1. Go to *pos*-th position and increase or decrease 1 at the original image block position according to the *pos* value in negative or positive.
2. Calculate sum of entry-wise multiplication of the original image block and the weighted matrix.
3. Extract the secret bits by converting *sum* value to binary.
4. Loop continue sixteen times in a block. After sixteen times, updated.

# **Experimental results**

In this chapter, we analyzed the experimental results in respect of the proposed scheme and Jana’s scheme.

The degree of distortion on an image is measured with *PSNR* (Peak Signal to Noise Ratio). *PSNR* is used as a method for detecting distortion of a cover image in image processing. Define the width and height as the *w* and *h* in the cover image, the *PSNR* is calculated by the following equation.

|  |  |
| --- | --- |
|  | (11) |

*MSE* (Mean Square Error) is obtained by the equation (12).

|  |  |
| --- | --- |
|  | (12) |

The comparison of the proposed scheme and Jana’s scheme is in the below.

|  |  |
| --- | --- |
| scheme | Payload(bpp) |
| Ni et al.’s [2] | 1.11 |
| Jung et al.’s [11] | 0.96 |
| Lee et al.’s [12] | 1.59 |
| Jana’s [13] | 2.96 |
| Proposed | 3.94 |

The maximum number of bits Jana’s scheme can embed is 774,192 bits and that of the proposed scheme is 1,032,256 bits. Therefore, the embedding capacity of the proposed scheme is increased by about 33% compared to Jana’s scheme maintaining similar *PSNR*.

Also the proposed scheme has high *bpp* than existed schemes.

# **Conclusion**

In 2016, Biswapati Jana proposed high payload reversible data hiding scheme using weighted matrix. Jana’s scheme has high capacity than presented schemes. But Jana’s scheme used non-overlapping block operation. So Jana’s scheme has limited embedding capacity. To solve this problem, we proposed an improved reversible data hiding scheme using weighted matrix with overlapping. The purpose of the proposed scheme is getting more embedding capacity keeping similar *PSNR*. In experimental results, the proposed scheme can embed 1,032,256 bits in the stego image while the Jana’s scheme can embed 774,192 bits in the stego image. Both schemes *PSNR* has 36.1dB. The embedding capacity is increased 33% than Jana’s scheme.

To embed more secret bits and to get more high *PSNR*, we will research about more efficient block operation.

##### **Acknowledgment**

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1D1 A1A01060801) and supported by the BK21 Plus project (SW Human Resource Development Program for Supporting Smart Life) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (21A20131600005).

##### **References**

1. M.S. Subhedar, V.H. Mankar. "Current status and key issues in image steganography:A survey." *Computer science review. ScienceDirect* (2014): 95-113.
2. Z. Ni, Y.Q. Shi, N. Ansari, W. Su. "Reversible data hiding." *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, IEEE* 16.3 (2006): 354-362 .
3. W. Bender, D. Gruhl, N. Morimoto, A. Lu. "Techniques for data hiding." *IBM Systems Journal, IBM 35.4 (1996):313-336*.
4. V.M. Potdar, E. Chang. "Gray level modification steganography for secret communication." *Industrial Informatics, IEEE* (2004).
5. D.C. Wu, W.H. Tsai. "A steganographic method for images by pixel value differencing.” *Pattern Recognition Letters, Elsevier* 24.9 (2003): 1613-1626.

B. Chen, G.W. Wornell. "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding." *IEEE Transactions on Information Theory, IEEE* 47.4 (2002): 1423-1443.

C.C. Chang, T.S. Nguyen, C.C. Lin. "A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies." *Journal of Systems and Software, Elsevier* 86.2 (2013): 389-402.

H.C. Wu, H.C. Wang, C.S. Tsai, C.M. Wang. "Reversible image steganographic scheme via predictive coding.” *Displays*, Elsevier 31.1 (2010): 35-43.

Y.M. Behbahani, P. Ghayour, A.H. Farzaneh. "Steganography based on eigen characteristics of quantized DCT matrices.” *Information Technology and Multimedia, IEEE (2011)*.

H.Y. Huang, S.H. Chang. "A 9/7 wavelet-based lossless data hiding." *Computational Intelligence for Multimedia, Signal and Vision Processing*, IEEE (2011).

K.H. Jung, K.Y. Yoo. "Data hiding method using image interpolation." *Computer Standards and Interfaces, Elsevier 31.2* (2009): 465-470.

C.F. Lee, Y.L. Huang. "An efficient image interpolation increasing payload inreversible data hiding.” *Expert Systems with Applications, Elsevier* 39.8 (2012): 6712-6719.

B. Jana. "High payload reversible data hiding scheme using weighted matrix." *Optik, Elsevier 127* (2016): 3347-3358.