Indian Journal of Science and Technology, *Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102118, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A New Pixel Value Based Steganography Method for Data Security

V. Thanikaiselvan[1*], Shounak Shastri[1], Shaik Ahmad[1] and S Subashanthini[2]

[1]School of Electronics Engineering, VIT University,Vellore, Tamil Nadu, India; thanikaiselvan@vit.ac.in, shounak.mangeshkalika2015@vit.ac.in, shak.ahmad2015@vit.ac.in
[2]School of Information Technology, VIT University, Vellore, Tamil Nadu, India; subashanthini@vit.ac.in

Abstract:

Objective: This paper proposes a new data hiding method to improve the security for data hiding. **Method:** This method first maps the cover image into a 1D pixel sequence and then divides it into non-overlapping blocks containing two successive pixels for embedding. It then calculates the difference between the two pixel values for the blocks. It then compares the difference with a reference table. The reference table is referred in every iteration for the comparison of pixel value differences and the range it falls in. This leads to the calculation of the number of bits which can be embedded in that particular block. **Findings**: The embedded pixels are then modified and their difference is calculated and compared with the range table. If the difference falls in same range, the embedded pixels are used as modified pixels, and if the difference does not fall in the same range, the pixels are modified such that the difference falls in the appropriate range. Extraction of the data is done in the same way to get the covert data. **Application/Improvements**: Experimental results show that this method enhances embedding rate while preserving the stego image quality.

Keywords: Data Hiding, Embedding Capacity, Imperceptibility, Optimal Pixel Adjustment Process (OPAP), Pixel Value Differencing (PVD), Steganography

1. Introduction

With the advent of digital media and the Internet, new methods have evolved and are being adopted for communication. This has led to an increase in the requirement of digital security and protection of digital data. It has been observed that transfer of digital data has suffered a lot from the lack of digital security through cyber attacks and hacking. This has inspired data security professionals to invent new methods to make the network secure and prevent this type of hacking.

Steganography and cryptography are one of the finest and easiest methods which can be used for protection of digital data. It has also been observed that, both can work together to maximize the protection level or security of the data. Cryptography basically scrambles and twists the data in such a way that it gets turned into a cryptic message while steganography hides the digital data in some other digital file.

In recent years, information security has emerged as one of the biggest concerns for governments, military organizations and corporations. As cybercrimes are on the rise and becoming more and more dangerous for the economy, national security and for management of corporate data, concrete methods for information security are needed not only for a secured network but also to provide security to the transfer of images like blue prints of a company's products and strategic and confidential defence and medical data. This can be achieved by using image steganography. As the data can be encrypted by several algorithms, it is difficult to find them in an image.

Steganography is the art of hiding digital data into an image[1]. Logically, it can be said that, embedding of data may lead to noise in the output results and may distort the pixel value of the existing image. As this slight change is

*Author for correspondence

not noticeable to the human eye, it makes steganography one of the most powerful tools for this purpose.

In[2] proposed a Reversible Data Hiding (RDH) scheme for depth maps using the depth no-synthesis-error model. Existing RDH methods can be used for embedding hidden data in 3D images. However, directly applying these methods to depth maps may cause synthesis errors and lead to visual artefacts in the rendered virtual views. Two new RDH methods based on the depth no-synthesis-error model are given in this paper to embed hidden data in the depth maps of 3D images. The proposed methods can preserve the quality of the condensed virtual view and deliver substantially higher embedding capacity.

In[3] came up with a method of reliably detecting data hidden in Least Significant Bits (LSB) of colour and gray scale Images. A large number of steganographic methods use the method of embedding the secret data in LSBs of coloured cover images and gray scale cover images. This method is found to give an accurate and reliable detection even for algorithms which embed data randomly in both coloured and gray scale images.

LSB based approach has become one of the most popular approach for application of steganography in the spatial domain. However, before the proposition[4], most of the existing approaches use a Pseudo Random Number Generator (PRNG) to choose the embedding positions in the cover image without considering the adjacent pixel correlations in the image content and the length of the secret data.

In[5] proposed a method for efficient RDH in colour images which partitioned payload according to the channel and embedded data adaptively. To make better exploitation of the inter-channel correlation and to improve the embedding process, a new colour image RDH scheme is proposed which is based on channel-dependent payload partition. Methods of adaptive embedding are also exploited in this process. The overall data to be embedded is logically divided and then it is embedded in the channel according to the PEH in such a way that the distortion in the cover image due to embedding is minimized. According to the experimental results of this paper, it is seen that the proposed method can give a better output.

In[6] came up with a concept of a robust RDH scheme for H.264 without distortion drift. They successfully encoded the secret data using BCH syndrome code prior to hiding the data, so as to improve the robustness. The data is first encoded and then embedded in the 4×4 blocks of the I frame in the quantized Discrete Cosine Transform (DCT) coefficients which have the same directions as that of the intra-frame prediction. The directions of intra-frame prediction are used to avoid the distortion artefacts. It is found that this technique is more robust. In[7] proposed a data hiding scheme based on 9/7 Integer Wavelet Transform (IWT) which adaptively embedded secret data in the LSBs of the IWT coefficients and used a graph theoretical approach to enhance the security of the method.

In[8]Chang et al. proposed a reversible data hiding scheme for secret communication that hides secret information in the compression codes of a cover image, but their scheme has low hiding capacity and introduces extra m bits to reverse the original vector quantization (VQ proposed a RDH technique based on Vector Quantization (VQ) with a higher embedding capacity. In this technique, instead of adding m bits and using only 1/3rd of the VQ indices of the cover image to conceal the secret bits, they proposed using only one bit to distinguish between indices of two clusters. Not only the indices in cluster1 but also those in cluster2 and cluster3 can hide the secret bits. This technique decreases the auxiliary data and improves the hiding capacity.

LSB matching is one of the most conventional as well as efficient data hiding methods. It is seen that the detection of data hidden using LSB matching technique is much more difficult as compared to the simple LSB replacement techniques. In[9] proposed the Exploiting Modification Direction (EMD) method which takes advantage of the different modification directions for hiding the secret data. In this method, 'n' pixels are taken as a single embedding unit, and the digits are embedded in (2n+1) base. In[10] Fuzzy logic with Earth Mover's Distance (FEMD) proposed a novel extraction function by altering the retrieval technique proposed. The alteration makes it possible to utilize eight modification directions for concealing the secret data, restricting the distortions due to embedding into blocks of various sizes and using the Minimum Distortion Embedding (MDE) process. In this way, the proposed scheme can provide different embedding capacities with less distortions compared to some of the recent schemes like those of[11] and[12] proposed a scheme which used pixel value ordering to deliberately introduce an error in the cover image. The histogram of the prediction errors was then modified to embed secret data.

This paper is organized as follows: Section 2 gives an overview of some of the earlier works which are related to this paper. Section 3 gives the explanation of the proposed

algorithm. Section 4 shows the results and gives a short discussion on the results and Section 5 concludes the paper.

2. Background

2.1 Optimal Pixel Adjustment Process

The visual quality of the stego image can be improved by using the Optimal Pixel Adjustment Process (OPAP)[13]. It checks the error between the cover and the stego images and reduces the Mean Square Error (MSE) to improve the visual quality and thus reduce the distortions caused by embedding the secret data. Apart from reducing the computational complexity, it also makes it difficult for the analyst to detect the presence of hidden data.

2.2 Least Significant Bit

In proposed an extension to the LSB matching revisited steganography scheme and came up with a system to choose the embedding areas on the basis of the size of the secret data. The embedding starts with the sharpest regions first. The scheme releases more edge regions adaptively if the secret data to be embedded cannot be accommodated in the available edge regions. This method was evaluated on natural images. Steganalysis tests on the stego images show confirms that the extension significantly enhances the security as compared to other LSB-based methods while maintaining a good visual quality of the stego images.

Firstly, the secret message is adaptively embedded in the sharp edge regions by setting a threshold based on the size of the secret data and the content edge gradients. This adaptive scheme can be extended to other media like audio and video files in the spatial or frequency domains when the amount of secret data to be embedded is less than the maximum embedding capacity.

2.3 Pixel-Value Differencing (PVD) Scheme

The PVD[14] scheme calculates the number of bits that can be inserted in a given pixel block by taking the difference between two consecutive pixels and matching it with a quantization range table. The scheme proposes two tables with different ranges. The first table consists of the ranges [4, 8, 16, 32, 64, 128] and provides a larger capacity but low quality stego images. The second table consists of the ranges [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64] and provides better visual quality of the stego images but a smaller capacity.

The data hiding technique is carried out in three domains, namely spatial domain, compress domain, and frequency domain. The domains specified have their own pros and cons when it comes to the embedding capacity, computation time and the payload capacity. A lot of research is being done to improve the imperceptibility of the hidden data. LSB matching is one of the conventional and most effective steganography methods. It has proven to be much more secure than the simple LSB replacement schemes.

3. Proposed Scheme

A new steganography method is implemented in this paper to improve the steganographic security of the hidden data. In this method, the cover image is mapped to a 1-D pixel-sequence and then it is split into separate blocks for embedding the secret data. As human eye has limited tolerance when it comes to texture and edge areas than for the smoother areas, and as the difference between the pixel intensities in those areas is larger, the secret bits are embedded in the sharp or edge regions.

Any digit can be inserted by considering the local characteristics of the cover image thus solving the problems which are faced by the existing EMD method. The data is inserted in both pixels of the block. If the difference doesn't fall in the same range after embedding, the second pixel value is adjusted to preserve the imperceptibility. Underflow and Overflow problems can be reduced by this proposed method and henceforth it resolves the detectable artefacts caused by them. The results show that our method improves the embedding rate while preserving the stego image quality.

3.1 Design Approach

3.1.1 Embedding Algorithm

Step 1: An image with size M×N is taken and mage scrambling is done using the Arnold transform. The image is then converted to a 1D sequence.

Step 2: Divide the sequence into non-overlapping (M x N) /2 blocks with two adjacent pixels. Calculate the difference between the adjacent pixel values.

Step 3: Construct a table which consists of the connecting sub-ranges W_j where j=1,2,3…, 6 and $W=\{W_j=[l_j, u_j]\}=\{[0, 7],[8, 15], [16, 31], [32, 63], [64, 127], [128, 255]\}$ for $w_j=u_j-l_j+1$

Step 4: If difference of adjacent pixel pairs (d) belong the range of W_j calculate the value of s_i and k_i where, $s_i=\log_2(w_j)$ and $k_i=\log_2(s_i^2)$

Step 5: Read the next k_i bits from the secret data and convert them to a decimal number (m_i). Now embedding of data is done in both the pixels using embedding function

$$P'(i) = P(i) - \text{mod}\,(P(i), 2^{ki}) + m_i \quad (1)$$

Where P (i) is the original cover pixel while P' (i) is the modified stego pixel value.

Step 6: Difference of modified pixels is being calculated and if difference fall in the same range as earlier calculated one, then the modified pixels will be taken as embedding pixels, if not in the same range as previous, then one pixel is taken and its modification will be done until the difference between the former pixel value and the modified one will fall in the same parameters of range table.

If $d_i<d$

If P'(2i +1) > P'(2i)
P'(2i +1) = P'(2i +1) +1;
If P'(2i +1) < P'(2i)
P'(2i +1) = P'(2i +1) -1;

If $d_i>d$

If P'(2i +1) > P'(2i)
P(2i +1) = P'(2i +1) -1;
If P'(2i +1) < P(2i)
P'(2i +1) = P(2i +1) +1;

(2)

Where d and d_i are the differences between the original and the modified pixel pairs respectively.

Step 7: P'(2i) and P'(2i+1) will be saved in different arrays each of size ((MxN)/2) and when embedding process gets over, the arrays will be combined to get an array of MxN size which will be reshaped to a matrix form so as to get resultant image.

3.1.2 Generation of Secret Data

Using the random bit generator, binary random bits are generated. These bits are later stored in an array format so that it can be used. Each set of generated bits are used only once, and are called secret message. The secret message bits are converted to its decimal value (m_i). The secret message bits are used for embedding and help in determining the payload capacity of the cover image.

3.1.3 Data Extraction Algorithm

Step 1: To extract the embedded message digits, the stego image will be scrambled using the Arnold transform.

Step 2: Convert the image into 1D array and then calculate difference of adjacent pixels. From the w_j division, determine the range in which the difference belongs.

Step 3: If d_i belong the range of W_j calculate the value of s_i and k_{i1} by $s_i=\log_2(w_j)$ and $k_{i1}=\log_2(s_i\text{^}2)$

Step 5: By using k_{i1} , extraction of embedded data will be done as

$$\text{Extracted Data}=\text{mod}\,(\text{pixel value}, 2\text{^}k_{i1}) \quad (3)$$

3.2 Example

3.2.1 Embedding

- Assume (P(2i), P(2i +1))= (162, 142). Now calculate difference i.e. d=|162-142|=20
- "d" lies in the range [16,31] ; $w_j=u_j-l_j+1$
- $w_j=31-16+1=16$; $s_i=\log_2(w_j)$
- $s_i=\log_2(16)=3.99$; $k_i=\log_2(s_i\text{^}2)$, $k_i=3.99=4$
- $k_i=4$ means we have to embed 4 bits in both pixels
- 4 bits secret data = 0001. Now convert binary into decimal $m_i=1$
- Now embed data in pixel value 162 so new pixel after embedding is $P'(2i) = 162-\text{mod}(162,2\text{^}k_i)+m_i$; P'(2i) = 162-mod(162,16)+1;
- P'(2i) =161; Now embed data in pixel value 142 so new pixel after embedding is $P'(2i+1) = 142-\text{mod}(142,2\text{^}k_i)+m_i$; P'(2i+1)=142-mod(142,16)+1; P'(2i +1)= 129
- After embedding data in the pixel pair (162,142) the pixel pair will be modified to (161,129)
- Now calculate difference of pixel pair (161,129) i.e $d_i=|161-129|=32$
- Difference is not falling in same range as earlier so we have to modified the new pixel value P'(2i +1) until it comes under the same range as earlier

If $d_i<d$

If P'(2i +1) > P'(2i)
P'(2i +1) = P'(2i +1) +1;
If P'(2i +1) < P'(2i)
P'(2i +1) = P'(2i +1) -1;

If d_i>d

If P'(2i +1) > P'(2i)

P(2i +1) = P'(2i +1) -1;

If P'(2i +1) < P(2i)

P'(2i +1) = P(2i +1) +1;

Where d is the difference of original pixel Here d_i>d and P' (2i +1) < P' (2i)

- So P'(2i +1) = P'(2i +1) +1;
- P*(2i +1)=129+1=130;
- Now calculate difference between (161,130) i.e. d_i=31 fall in the range [16,31]
- Hence after embedding pixel pair (162,142) will be modified to (161,130)

3.2.2 *Extraction*

- Embedded pixel pair = (161,130)
- Calculate difference d_e=|161-130|=31
- "d_e" lies in the range [16,31]
- $w_j=u_j-l_j+1$; w_j=31-16+1=16
- $s_{i1}=\log_2(w_j)$; $s_{i1}=\log_2(16)$=3.99
- $k_{i1}=\log_2(s_i\text{^}2)$; k_{i1}=3.99=4
- embedded bits = 4; embedded data = mod(pixel value, $2\text{^}k_{i1}$)
- data=mod(161,16) ; data=1;

4. Experimental Results and Discussions

The experiments in this section were conducted on a personal computer with Windows 7 professional operating system using an Intel i5 processor with 4 GB RAM and MATLAB version 2013a. Eight standard 8-bit grey-scale images of size 512×512 were used to hide the secret data. Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and embedding capacity were considered as evaluation parameters. The mathematical representations of PSNR and MSE are shown in equation. (4) and (5). The secret data to hide was generated from MATLAB's inbuilt random number generator.

$$\mathbf{PSNR} = \mathbf{10}\log_{10}\frac{\mathbf{255}^2}{\mathbf{MSE}} \quad (4)$$

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}([Aij - A'ij)]^2 \quad (5)$$

Where A_{ij}, A'_{ij}, m and n are the pixel intensities of the cover image, stego-image, row size and column size of the images respectively.

In this paper, OPAP was incorporated to improve the performance of the proposed method. Table 1 presents the evaluation parameter values of the proposed method without OPAP and Table 2 presents with OPAP. Figure 1 represents some of the input images used for data hiding along with its stego images. The data is embedded in both pixels of the pixel block. This maintains the difference between the two pixels and thus preserves the visual quality of the stego image.

In the standard EMD method the data is stored in uniformly over the whole image. This produces artefacts in the stego image. The proposed method avoids this by embedding the secret data according to the local characteristics of the cover. This reduces the artefacts caused by the readjusting process for overflow/underflow problem. The PSNR values for the proposed method are high and

Table 1. MSE PSNR and capacity for test images without OPAP

Image	MSE	PSNR (dB)	Capacity (Bits)
Pebbles	14.6064	42.06	409564
Baboon	25.4533	40.1110	403024
Lena	7.3949	45.4791	395220
Messi	12.5139	43.1945	394832
Peppers	3.5168	48.7069	395621
Milk drop	13.6707	42.8105	396533
Cameraman	20.6310	41.0232	397405
Koala	13.4843	42.8701	404592

Table 2. MSE PSNR and Capacity for test images with OPAP

Image	MSE	PSNR (dB)	Capacity(Bits)
Pebbles	7.9889	45.1435	409564
Baboon	3.3677	48.8951	403024
Lena	4.2188	47.9165	395220
Messi	4.2607	47.8736	394832
Peppers	5.1107	47.0836	395621
Milk drop	3.1049	49.2480	396533
Cameraman	7.7615	45.2689	396533
Koala	7.2637	45.5568	404592

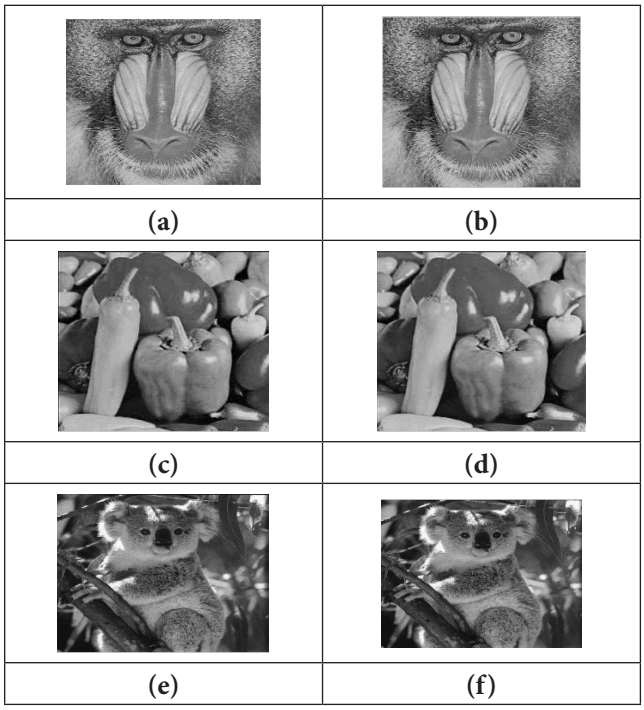

Figure 1. Cover and Stego images for **(a, b)** Baboon **(c, d)** Peppers **(e, f)** Koala

falling in the expected range which is greater than 40dB. This gives better quality of stego image as compared to the other methods. The results show that this scheme improves the embedding rate while preserving the quality. This method has overcome the trade-off between the embedding capacity and the image quality to a certain extent by embedding four lakh bits in the image with minimal distortion.

The proposed technique besides providing a significant improvement in PSNR provides high payload capacity. In Table 1 and 2, the PSNR values of various images which were calculated using the proposed method and using OPAP have been compared. It can be seen that the PSNR has increased by a minimum of 3dB while using the OPAP.

5. Conclusion

A new and different data hiding method is proposed in this paper, which improves the steganographic security of the data hiding scheme. The proposed technique first maps a cover image is into a 1D pixel sequence and then splits it into separate blocks for the embedding process. The blocks consist of two consecutive pixel values. The human eye has limited tolerance for texture and edge areas than for smoother areas, and as the difference between the pixel pairs in those areas is larger, the method uses PVD to solve the overflow and underflow problem.

The proposed scheme employs PVD technique to embed data in a cover image. The resultant stego image has low distortions. The distortions can be further reduced by employing OPAP to improve the stego image quality. Thus this method can be used in applications in which there are a need to transmit large amounts of data while protecting its confidentiality.

6. References

1. Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. *Signal Processing*. 2010 Mar; 90(3):727-52.
2. Chung KL, Yang WJ, Yang WN. Reversible data hiding for depth maps using the depth no-synthesis-error model. *Information Science*. 2014 Jun; 269:159-75.
3. Fridrich J, Goljan M, Du R. Reliable Detection of LSB Steganography in Grayscale and Color Images. *Proceeding ACM Work Multimedia and Security*. 2001, p.27-30.
4. Luo W, Huang F, Huang J. Edge Adaptive Image Steganography Based on LSB Matching Revisited. *IEEE Transaction Information Forensics Security*. 2010 Jun; 5(2): 201-14.
5. Ou B, Li X, Zhao Y, Ni R. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion. *Signal Process Image Communication*. 2014 Aug; 29(7):760-72.
6. Liu Y, Ju L, Hu M, Ma X, Zhao H. A robust reversible data hiding scheme for H, 264 without distortion drift. *Neurocomputing*. 2015 Mar; 151:1053-62.
7. Thanikaiselvan V, Bansal T, Jain P. Shastri. 9 / 7 IWT Domain Data Hiding in Image using Adaptive and Non Adaptive Methods . *Indian Journal of Science and Technology*. 2016 Feb; 9(5):1-7.
8. Tu TY, Wang CH. Reversible data hiding with high payload based on referred frequency for VQ compressed codes index. *Signal Processing*. 2015 Mar; 108:278-87.
9. Zhang X, Wang S. Efficient steganographic embedding by exploiting modification direction. *IEEE Communication Letter*. 2006 Nov; 10(11):781-83.
10. Wang ZH, Kieu TD, Chang CC, Li MC. A novel information concealing method based on exploiting modification direction. *Journal of Information Hiding Multimedia Signal Process*. 2010 Jan; 1(1):1-9.
11. Mielikainen J. LSB matching revisited. *IEEE Signal Processing Letter*. 2006 May; 13(5):285-87.

12. Shastri S, Thanikaiselvan V. PVO based Reversible Data Hiding with Improved Embedding Capacity and Security. *Indian Journal of Science and Technology*. 2016 Feb; 9(5):1-7.
13. Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. *Pattern Recognit*. 2004 Mar; 37(3):469-74.
14. Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letter*. 2003 Jun; 24(9-10):1613-26.