A robust way of steganography by using blocks of an image in spatial domain

Author:

iD **Ladeh S.Abdulraman[1]**
iD **Sheerko R. Hma Salah[2]**
iD **Halgurd S. Maghdid[3]**
iD **Azhin T. Sabir[4]**

SCIENTIFIC RESEARCH

ABSTRACT

Steganography is a way to convey secret communication, with rapid electronic communication and high demand of using the internet, steganography has become a wide field of research and discussion. In this paper a new approach for hiding information in cover image proposed in spatial domain, the proposed approach divides the host image into blocks of size (8x8) pixels and message bits are embeds into the pixels of a cover image. The 64-pixel values of each block converted to be represented in binary system and compared with corresponding secret data bits for finding the matching and hold 6-pixels. The search process performed by comparing each secret data bit (8-bits) with created binary plane at the cover image, if matching is found the last row of the created binary plane which is (LSB) is modified to indicate the location of the matched bits sequence "which is the secret data" and number of the row, if matching is not found in all 7th rows the secret sequence is copied in to the corresponding 8th row location.

The payload of this technique is 6 pixels' message (48-bits) in each block. In the experiments secret messages are randomly embedded into different images. The quality of the stego-image from which the original text message is extracted is not affected at all. For validation of the presented mechanism, the capacity, the circuit complexity, and the measurement of distortion against steganalysis is evaluated using the peak-signal-to-noise ratio (PSNR) are analyzed.

[1] Ladeh S. Abdulraman is with the Software Engineering Department, Koya University, Koya, ladeh.sardar@koyauniversity.org.
[2] Sheerko R. Hma Salah is with the Software Engineering Department, Koya University,Koya, sherko.rahman@koyauniversity.org.
[3] Halgurd S. Maghdid is with the Software Engineering Department , Koya University, Koya, halgurd.sarhang @koyauniversity.org.
[4] Sabir A is with the Software Engineering Department , Koya University, Koya, Azhin.tahir @koyauniversity.org.

INTRODUCCTION

The rapid growth of the internet and exponentially using of it as a communication media increasing day by day. Requirements for a higher secure communication has become more important and resistant. Steganography is the techniques and science to create and establish safe channel between the sender and the receiver, and keeping information secure, integrity, and protecting its accessibility [1].

Steganography in the past several years considered as a guaranteeing way of e-communication and niche in security deals with hiding of an information in a various medium used as a cover such as text, audio, video, image, protocol [2].

Image considered as a suitable format for steganography, because it contains a high amount of redundancies in their canonical representation, redundancy mean the unnecessary bits that can be altered without the alteration being detected easily, so image formats comply with this demand [3]. The word steganography is of ancient Greek words which combination of two words Steganos means "protected or covered" and Graphie means "writing". The first recorded use of steganography was in 1499 by Johannes Trithemius [2] [4]. As it's obvious the objective of steganography is to promise a safe way of e-communication by concealing the secret message in to cover source. The opposite of "protected message" on the other side is trying to detect the payload, steganalysis which is the opposite of steganography on the other side working to detect the existence of the hidden message. Steganalysis is the art and science of detecting and identifying suspected hidden message and recover it if possible.

The good and the effective techniques in steganography must hold two important major challenges which are security of the carrier and the payload size, the two metrics must be balanced and considered well [5].

a- Perceptual transparency: The secret message has to be hidden, and it should result in a low distortion and must be undetectable to avoid raising the suspicions of eavesdroppers, because the technique fails when the stego-cover is precepted and finally the payload may be removed or replaced.

b- Payload size: Is the amount of the embedded data plays an important role in steganography "A larger hiding capacity allows the use of smaller cover for a message of fixed size and thus decreases the bandwidth required to transmit the stego-image".

The two popular methods used in steganography can be broadly divided into two main groups which are based on the hiding domain, spatial and frequency domain methods. In spatial domain, the information is inserted directly and embedded in the values of the cover image pixel. Frequency domain methods transform the cover image to frequency domain and information is hidden in this domain [2] [6]. Spatial domain methods are relatively simple compared to methods of frequency domain, and in general they are more sensitive to small changes on the cover media. The transform domain methods on the other hand are more robust to changes but the capacity of hiding information is lower compared to spatial domain methods [2].

In this study a new approach for hiding information in cover image presented in spatial domain, which hides covert message in digital image.

The rest of this paper is organized as the following sections. The first section is an overview of related work, in the next section the proposed hiding technique is described in detail with an example to explain the technique, section IV emphasizing on experimental results and comparing it with other related studies, finally section V concludes the proposed method and outlines future studies directions.

BACKGROUND AND RELATED WORKS

A survey on steganographic approaches for Least Significant Bit (LSB) substitution in spatial domain introduced. Generally, schemes in a spatial domain often lead to fast processing and higher capacity in embedding, but might not be robust as well, but the

experiments of this approach give a good and acceptable result compared with presented approaches in the literature.

In [7], the typical and standard spatial domain algorithm using LSB replacement overviewed, each pixel in fact can be represented in 1-Byte, starting at the left hand from MSB to LSB the LSB contains no visual sense and Human Vision Sense HVS never realize any change in this bit. In this technique the only altered bit plane is the first right side bit of each pixel which is LSB. The main constraint in this technique is robustness against steganalysis because most stganalysis attacks are able to detect and retrieve the existence of the secret message.

As explained in reference [8]. A new steganography method using image layers proposed in this method the host image divided into blocks of (8-by-8) fixed size of pixels and converted to binary representation (bit-plane), the corresponding secret bits embeds into each block using the layers (plane) generated by the binary representation. The algorithm tries to find the similarity between the secret data bits and the rows and columns of the layers. The sequence of the layer and the location of the row and column marked by modifying minimum number of bits in the Least Significant Bits of the block, which provides minimum amount of degradation in the cover image, this method tries to find match in the higher layers of host image, which is the key strozng of this method that increase the robustness, but the main constraint in this study is to hide only one secret pixel in each block (64-pixels).

The proposed scheme in [9]. It hides a secret message in a cover image by finding identical bits between secret message and cover image. After the comparison done and the similarity found, the location of hidden data bits marked at the cover image and can be retrieved beyond the legal receiver. By this scheme minimum bits in stego-image will be changed so the quality will never degrade. The used cover image in this technique is color image with 4-bit binary intensity values. The probability of finding exact matching between the secret message and pixels of an image is restricted which affect the payload size.

The author in paper [10]. In this study a new steganographic technique improved and discussed, by embedding secret characters into cover image (RGB image). The algorithm performs the search and tries to find matches between secret character and the cover image. Each secret character after represented in a binary is divided in to 3 segments of (3-bits, 3-bits, and 2-bits), the first 3bits stored in 8-bits of Red palette after matching is found, and the same for second 3-bits into Green palette, finally the remaining 2-bits in blue palette in RGB pixel of cover image. In the case if searching done without finding exact similarity, all non-identical bits will be stored in LSB of the corresponding pixel. This technique is efficient because secret message cannot be spotted by steganalysis easily.

A new method proposed in [11]. In this method Plan Bit Substitution Method (PBSM) were used in which secret bits are embedded into the pixel values of a cover image. The whole process is divided into two parts, first solving binary operation for manipulation of cover image with help to least significant bit (LSB) operator-based matching. Second the secret message encrypted before embedding and decrypted after extraction process. This method considered as an adaptive technique, because it tries to store more than one bit in each pixel rather than storing the data in every least significant bit of the pixels, which increase the robustness. To estimate the number of bits which can be embedded in the pixels of the host image, it uses the side information of neighboring pixels to hide the secret data called (PBSM).

The proposed approach in our study performs other related works in which embed 6-pixels in each block rather than 1-pixel as [8] [9] [10], and outperforms [7], in which secret message randomly emended in side the cover image rather than sequentially embedding it, therefore it's more secure as it can not be extracted by eavesdropper easily.

THE PROPOSED APPROACH

This section describes the proposed method which embeds the message bits into the pixel values of an image; That's the cover image is divided into a number of fixed size of (8x8) pixels of blocks. From each block a palette of 8x64 bits is constructed as shown in figures 1 and 2. The palette consists of 8 row which represents digits in the corresponding block starts from the MSB to the LSB of the pixels i.e. the first row of the palette represents the MSB of each pixel in the block, the followed row consists of the second MSB of each pixel and so on.
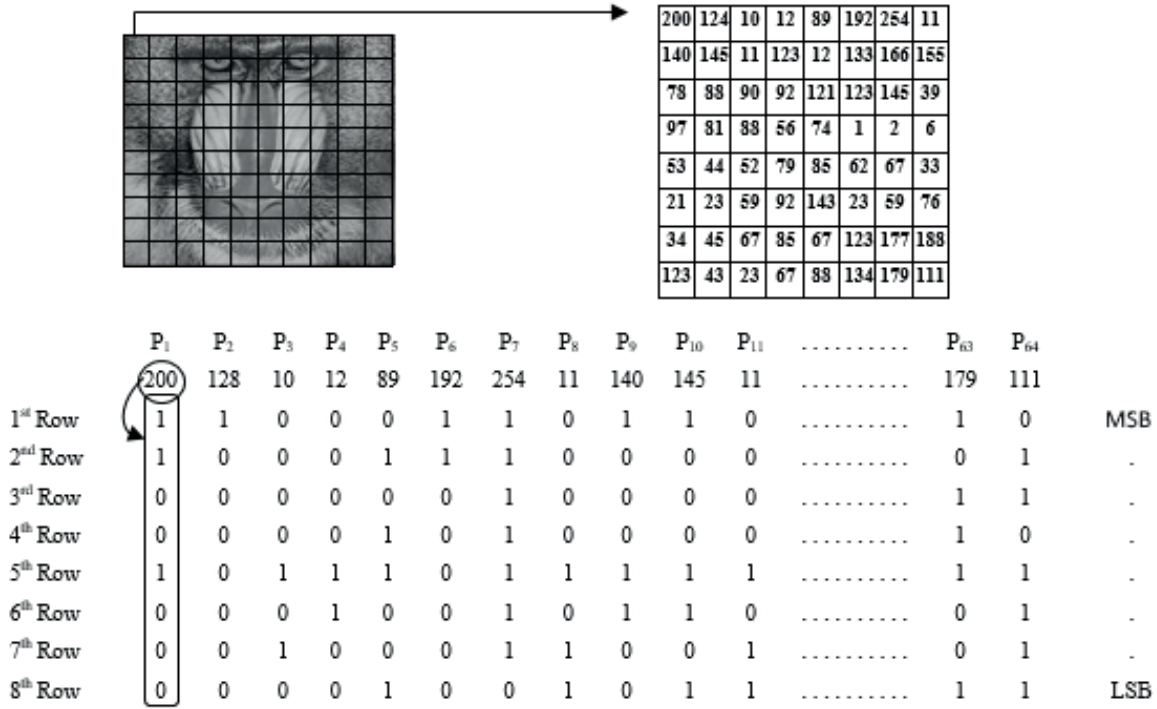

200	124	10	12	89	192	254	11
140	145	11	123	12	133	166	155
78	88	90	92	121	123	145	39
97	81	88	56	74	1	2	6
53	44	52	79	85	62	67	33
21	23	59	92	143	23	59	76
34	45	67	85	67	123	177	188
123	43	23	67	88	134	179	111

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	....	P_{63}	P_{64}	
	200	128	10	12	89	192	254	11	140	145	11	....	179	111	
1st Row	1	1	0	0	0	1	1	0	1	1	0	....	1	0	MSB
2nd Row	1	0	0	0	1	1	1	0	0	0	0	....	0	1	.
3rd Row	0	0	0	0	0	0	1	0	0	0	0	....	1	1	.
4th Row	0	0	0	0	1	0	1	0	0	0	0	....	1	0	.
5th Row	1	0	1	1	1	0	1	1	1	1	1	....	1	1	.
6th Row	0	0	0	1	0	0	1	0	1	1	0	....	0	1	.
7th Row	0	0	1	0	0	0	1	1	0	0	1	....	0	1	.
8th Row	0	0	0	0	1	0	0	1	0	1	1	....	1	1	LSB

Figure 1. Representing one image block and its palette

1st Row= 11000110110010101101010100001011110001010101101010100000 11010111
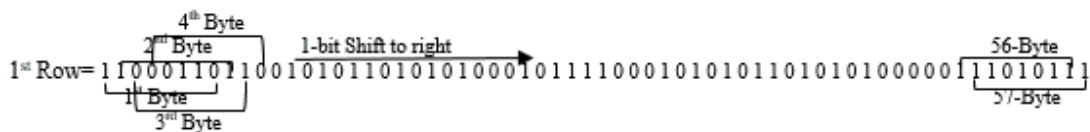
Figure 2. Search space generation for the 1st row

The process of embedding secrete message is performed by searching the palette from the 1st to the 7th rows, the last row is used as an indicator to mark the location of the secrete sequence bits. The searching process is started by comparing the 1_{st} eight bits (b1-b8) of the first row with the eight bits of the secrete message, if there is an exact matching between them, then the last row is updated to indicate the location. In the last row the first ten bits are reserved for indication, the 1st bit represents whether there is an exact matching or not. If there is an exact matching, it's assigned to 1, from the 2nd to the 4th bits are assigned to indicate the row number, because there are 7 rows, hence three bits are required for representation. The remained 6 bits are used to indicate the column number that the secret message starts from, because there are 64 columns therefore the minimum number of the bits are required is 6 bits. In the case if the exact matching did not exist in the first search at the first row, the process of searching will continue by shifting one bit to the right to generate another byte for comparison i.e. from bit

b2-b9. In the shifting step one byte is generated for comparison, as a result 57 bytes are produced in a single row, that means there are 57 probabilities for finding the exact matching. So in total 399 probabilities are generated from the whole rows. The 2_{nd} eight bits are embedded by using the second ten bits of the last row as indicator with the same searching process, the last ten bits of the last row which is b51-b60 indicates the location of the 6_{th} bits sequence of the secrete message, this process results in hiding 6 letters in a block.

Given the secret bit sequence, the technique applies a search process over all rows except last row at the palette, attempting to find matching by performing a XOR between them, if the result between the (1-Byte) of the secret sequence bits and (1-Byte) of the cover-image is equal to 0 it means the exact matching is found, otherwise mismatching will occur. Probably mismatching is the second case which may occur, in this case the 1_{st} two bits from the corresponded ten bits are assigned to 0 and the rest bits holds the mismatched message as its. The technique finds an exact match in the experiments is %56 in the worst case if embedding rate is %100, that's considered as a great number of matching because the search space of finding an exact matching is 399 probabilities as discussed before in this section

EXPERMENTAL RESULTS

In the experiments the performance of the proposed method is evaluated and measured by the degree of robustness against steganalysis, Peak Signal to Noise Ratio PSNR that measured in (dB) and Mean Square Error (MSE) are used. PSNR is a good measure for comparing resolution results between the original (cover-image) and embedded (stego-image), where defined as:

$$PSNR=10*log10$$
$$MSE=$$

Where is the cover-image, is the stego-image, and are the size of the images. The comparison of average PSNR and average modification rate MSE are viewed in table (1), with number of matched and mismatched pixels. This table is a result of embedding randomly selected secret messages into 8 standard images.

Tabla 1. Results of proposed Steganographic Algorithms using average PSNR

Payload Ratio	No. Of embedded secret pixel	Matching Ratio	PSNR	MSE
25%	6144	51.8%	57.5	0.05
50%	12288	53%	54.6	0.09
75%	18432	55.2%	53.1	0.15
100%	24576	56.1%	51.9	0.21

The results in the above table shows that the PSNR still above (50 dB) in the worst case when full embedding rate is given, and the quality of the image is preserved because distortion can't be spotted in naked eyes. If we look at the trends towards increasing embedding rate, the capacity of the payload is high because this method embeds 6-pixels in each block. Figure3 shows the orignal image of size (512*512) pixels, while figure 3-a through 3-d display the stego-images after adding the payload ratio of 25%,50% ,75%, and 100% respectively.
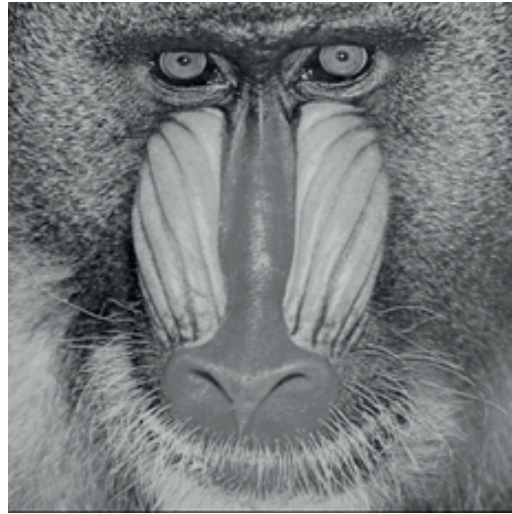
Figure 3. Original Image
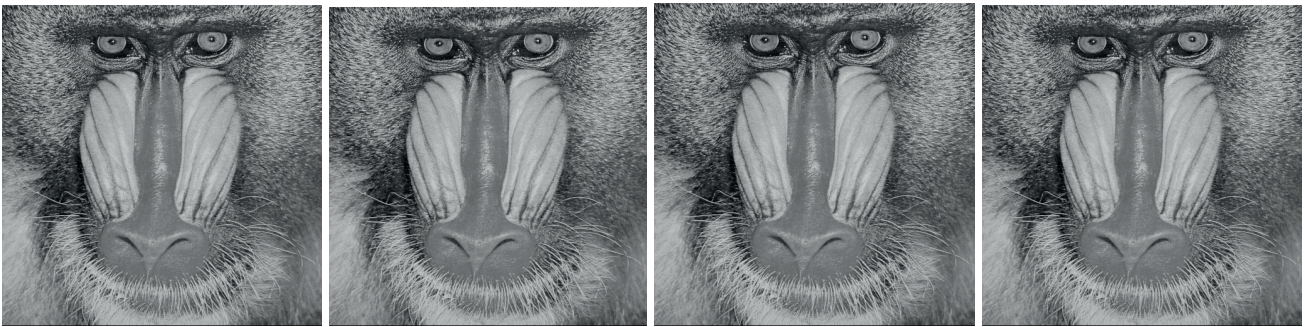
Figure 3-a. Payload of 25%   **Figure 3-b.** Payload of 50%   **Figure 3-c.** Payload of 75%   **Figure 3-d.** Payload of 100%

CONCLUSIONS

This paper introduced a new data hiding method in spatial domain. The main reason of steganography is to establosh secure link between sender and receiver, to Exchange confidential information by embedding it in to a cover image, secure and roubest steganographic mechanism implemented in this study, almost most of the techniques in spatial domain focus on only Least Significant Bits to embed the secret message as explained before for the reason of preserving the quality of the stego-image. But the proposed technique uses different way in embedding secret data by attempting to find matching at the higher order digits of the pixel values which is the most significant bits, that is considered as a special characteristic to increase and improve security of the stego-image. Security in steganography refers to the ability of embedded data to remain intact if the stego-image undergoes extraction by the illegal receiver. Also hiding capacity play an important role in steganography, the high performance and strong points in this method is the payload size, that is capable to embed 6-pixels into each block. And also randomly embedding secret sequence bits for the purpose of increasing level of security while maintaining and preserving the visual quality and size of the embedded image.

REFERENCES

1. Borse, Dipalee and Patil, Shobhana. Review and Analysis of Multifarious Spatial Domain Steganography Techniques. 2015; 4(1-Jan-2015).
2. Akhter F. A novel approach for image steganography in spatial domain. 2013; 13(7).
3. Neeta DaSKaJD. Implementation of LSB steganography and its evaluation for various bits. 2006.
4. Samaratunge S. New steganography technique for palette based images. 2007;(IEEE). https://doi.org/10.1109/ICIINFS.2007.4579198
5. Cheddad AaCJaCKaMKP. Digital image steganography: Survey and analysis of current methods. 2010; 90. https://doi.org/10.1016/j.sigpro.2009.08.010
6. Liu, Qingzhong and Sung, Andrew H and Ribeiro, Bernardete and Wei, Mingzhen and Chen, Zhongxue and Xu, Jianyun. Image complexity and feature mining for steganalysis of least significant bit matching steganography. 2008; 178. https://doi.org/10.1016/j.ins.2007.08.007
7. Chan, Chi-Kwong and Cheng, Lee-Ming. Hiding data in images by simple LSB substitution. 2004; 37. https://doi.org/10.1016/j.patcog.2003.08.007
8. Kurtuldu, Omer and Arica, Nafiz. A new steganography method using image layers. 2008. https://doi.org/10.1109/ISCIS.2008.4717893
9. Al-Shatnawi AM. A new method in image steganography with improved image quality. 2012; 6.
10. Prasad, Koyi Lakshmi and Rao, T Ch Malleswara. A Novel Secured RGB LSB Steganography with Enhanced Stego-Image Quality. 2013; 3.
11. Sravanthi, GS and Devi, B Sunitha and Riyazoddin, SM and Reddy, M Janga. A spatial domain image steganography technique based on plane bit substitution method. 2012; 12(15).