Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-57

Imperceptible image-based steganographic scheme using Bit-Plane Complexity Segmentation (BPCS)

Samer Atawneh, Putra Sumari

***Abstract*—Image-based steganography is the practice of embedding secret information into digital images with the intention to communicate the secret information. Embedding large sizes of secret information into digital images is one of the problems that image-based steganography encounters. The distortion of digital image increases with larger capacity, meaning that both are positively correlated. The latter makes image-based steganography fingerprints perceptually and statistically visible. In this paper, we propose a new spatial-domain steganographic scheme based on Bit-Plane Complexity Segmentation (BPCS). Experimental results reveals that the proposed algorithm offers better embedding performance compared with prior BPCS-based algorithms in terms of image quality and capacity.**

Keywords*—Image steganography, spatial domain, Bit-Plane Complexity Segmentation (BPCS)

I. Introduction

Steganography has become significant in today's digital world where information is frequently and easily exchanged through the Internet, emails and other ways using computers. These electronic communication means, which are susceptible to attacks and eavesdropping, make the current security measures more important than before, where security problems, such as modification and forgery, have reached critical extents. The need for creating effective methods for image-based secret sharing led to the new incentive research in the area of image steganography.

The main concept of contemporary steganography was described by Simmons [1] when he explained how two prisoners, Alice and Bob, were planning to escape. They are under the surveillance of Eve, the warden, and they need to communicate in a covert way with no raising suspicion [2]. A steganographic technique is mathematically defined as follows (the main processes are graphically represented in Fig. 1):

Let M denote to the set of embeddable messages, and C denote to the set of the cover images. Let k denote to the secret stego-key that is obtained from a set of stego-keys K. Two mappings are included in a steganographic scheme, namely the embedding mapping (Emb), and the extraction mapping (Ext):

$Emb: CxKxM \rightarrow C'$ (1)

$Ext: C' \rightarrow M,$ (2)

where $Ext(Emb(c,k,m)) = m$ for all $c \in C, k \in K,$ and $m \in M$. $C' = Emb(c,k,m)$ is referred to as the stego-image.

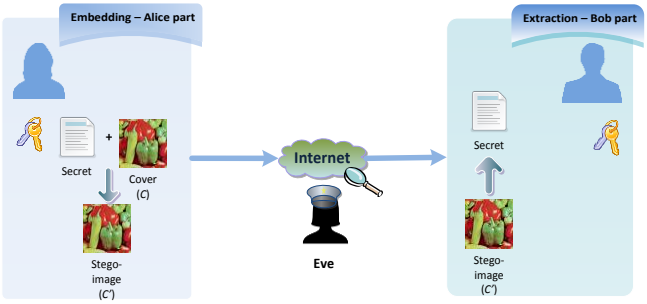


Fig. 1. A general steganography system showing the encoding and the decoding stages. C denotes to the cover image and C′ denotes to the stego-image (the cover C after embedding the secret information).

The main purpose of steganography is the secret communication [3]. However, it has different useful applications; the most interesting ones are file authentication [4], annotation [5], hide confidential data files (spreadsheets and documents) located inside computers [6], bank transactions [7], enhanced data structures [3] and protecting digital document files from forgery using self-embedding methods [8].

Several features characterize the performance of any image steganography technique [9]. The most important features are statistical undetectability, imperceptibility and embedding capacity [2, 10, 11]. Statistical undetectability means that no current method can statistically determine whether there is a hidden information embedded in the image [2], that is, the image after embedding the secret information, termed as stego-image, is consistent with the cover image. The term imperceptibility indicates how difficult it is for the human visual system (HVS) to recognize any difference between the stego-image and its original cover image. The size of the secret information that can be embedded in the image is known as embedding capacity (or payload).

Cryptography and information hiding are two common disciplines used to protect information. Cryptography is the scrambling of a message by using a crypto-key, so it becomes meaningless. No matter how unbreakable is the encrypted message, it will arouse suspicion [12, 13]. Steganography is superior to cryptography in a sense that it is not by means to prevent others from being privy of the hidden information, but it is also to prevent them from being privy to the existence of the information [14]. Neither cryptography nor steganography is believed to be turnkey solutions to security issues in open systems. Nonetheless, both can facilitate considerable security of the system communication and connection [15]. Watermarking is the practice of altering digital media, in an imperceptible way, to add information about this media to protect its copyright [2]. In watermarking, the communication is the carrier data, and the protection lies in the hidden data in

Samer Atawneh and Putra Sumari
School of Computer Sciences, Univeristi Sains Malaysia.
Malaysia

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-57

the form of copyright protection, while in steganography, the communication is the secret and the carrier one is just a cover [3].

The rest of the paper is organized as follows: Section II gives the literature review of the domain. Section III presents the proposed method. Section IV shows the experimental results and analysis of the proposed method. Section V draws the conclusions and the future work of the paper.

II. Literature Review

Steganographic methods can be classified in different ways. A direct classification is according to the carrier used [10, 16]. This includes image steganography, video steganography, audio steganography, text steganography, protocol steganography and 3D steganography. Cheddad et al. [17] gave a standard classification by grouping the methods into spatial domain, frequency domain and adaptive techniques. Spatial domain steganographic methods embed the secret information in the LSBs of the cover image's pixels selected sequentially or randomly. On the other hand, the frequency domain steganographic methods mainly embed the secret information in the coefficients of the carrier and manage to satisfy the criteria of imperceptibility as well as robustness [18, 19]. The development of adaptive methods obviously require a full knowledge of representative features of the cover image to decide where to make changes [20]. Fig. 2 shows the steganographic methods that utilize the spatial domain or the frequency domain of digital images in hiding the secret information.

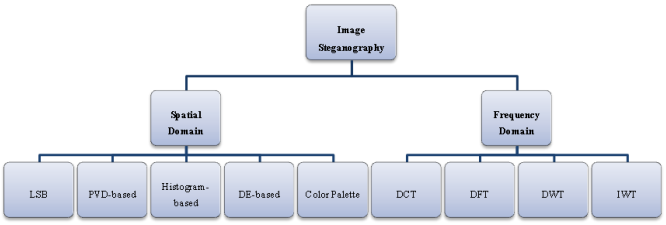


Fig. 2. Digital image steganography methods.

Spatial domain methods include bitwise methods applying the Least Significant Bit (LSB) insertion. These steganographic methods are widely used and are considered to act like simple systems [21]. The S-Tools technique is a particular method involving the modification of the LSB of each of the three colors of a pixel in a 24-bit image [22]. Palette-based image, such as GIF and BMP, is one of the popular images commonly used in multimedia and available on the Internet [23]. Saleh et al. [24] proposed a lossless hiding method for palette based images. The embedding process is based on analyzing the histogram of the image to determine the most-used colors and unused colors (zero-values in the histogram), and then the most-used colors are repeated in the indices that point to the unused colors.

Pixel-value differencing (PVD) information hiding is another commonly used embedding scheme in digital images. In PVD, the difference value between two or more adjacent pixels is utilized to embed secret information [25, 26]. The difference value controls the embedding capacity; that is, the higher the difference value is, the more secret information can be embedded and hence leading to a high embedding capacity [27]. Yang et al. [28] proposed a data hiding method based on using the PVD scheme. They divide the cover image into 2×2 disjoint blocks and arrange the pixels in each block according to their gray values. Each block is then partitioned into two groups, and a difference d_i for each group is calculated. The range [0, 255] is divided into set of contiguous ranges and $log_2(u_k - l_k + 1)$ secret bits are selected to be embedded in each group if the difference $d_i \in [l_k, u_k]$, where l_k and u_k are the lower and upper values of the range, respectively.

Bit-Plane Complexity Segmentation (BPCS) steganography is another common type of information hiding techniques where an n-bit host image is decomposed into n binary images (n bit-planes) before embedding process takes place as shown in Fig. 3. The complexity of each bit-plane is calculated by finding the sum of color changes between pixels in the planes. For example, a white-color pixel surrounded by four black-color pixels has a complexity of 4 (see Fig. 4 (a)). In general, for a block of $n \times n$ pixels, the maximum complexity is $2n(n-1)$ and the minimum complexity is 0. Fig. 4 (b) shows a checkerboard image of size 4 × 4 where the upper-left pixel is black. The total number of color changes in this block is 2 × 4 (4 – 1) = 24. Bhattacharyya et al. [29] proposed a steganographic method for 8-bit images based on finding the sum of color changes between pixels in the planes. Bit-planes with complexity higher than a threshold α is then segmented into 8x8 disjoint blocks and 2 secret bits are embedded in each block by a mapping scheme. As shown from experiments, the drawback of this method comes from its low embedding capacity (1.6% in best cases) with PSNR value less than 38dB. In this paper, a new spatial-domain steganographic method is proposed based on BPCS. Section III shows the proposed method.

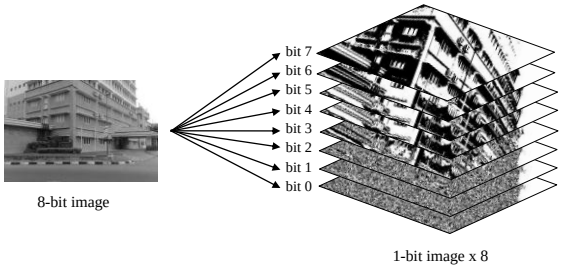


Fig. 3. BPCS steganography. A cover 8-bit image is decomposed into 8 binary images prior to the embedding process.

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-57

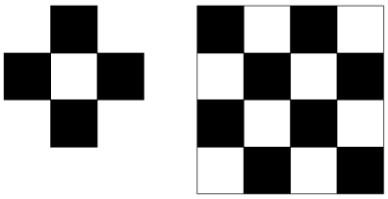


Fig. 4. BPCS (a) a white-color pixel surrounded by four black-color pixels, complexity is 4. (b) a black-white checkerboard of size 4 × 4, complexity is 24.

III. Proposed Method

In this section, a new spatial-domain steganographic algorithm based on BPCS is presented. The contribution here is to develop an algorithm that enhances the imperceptibility while maintaining the embedding capacity. The cover image is separated into 8 bit planes and all bit planes (except the LSB – bit plane) is segmented into blocks of size m × m. The complexity of each block is computed, and a digit of the secret information is embedded in each block based on the calculated complexity. The fundamental logic behind the proposed algorithm is that the secret information is converted into decimal form and, based on the complexity of the blocks and a user-defined threshold *t*, sequences of digits in base b, b = 3, 4 are extracted from the secret information using multiple-base notational system (MBNS). The exploiting modification direction (EMD) scheme [30] is then utilized to embed the extracted digits. By utilizing the EMD embedding scheme, only one pixel of two is increased or decreased by 1. Sections III. A and III. B describe the MBNS and EMD embedding scheme, respectively. Sections III. C and III. D describe the proposed method in further details, and Section III. E shows a simple example.

A. *Exploiting Modification Direction (EMD) Embedding Scheme*

The main idea of the EMD embedding scheme is that (2n+1) notational secret digit is embedded in n pixels of the cover image where only one pixel is increased or decreased by 1. For example, a secret digit in base-5 can be embedded in 2 pixels by modifying one of these 2 pixels. The following extraction function is defined to embed base-5 secret digits:

$$f(g_1, g_2) = (g_1 + 2g_2) \bmod 5 \quad (3)$$

where g_1 and g_2 are two consecutive pixels of the cover image. The secret digit s in base-5 is embedded in pixels g_1 and g_2 based on the conditions shown in Table 1.

TABLE 1: CONDITIONS AND ACTIONS OF EMBEDDING BASE-5 SECRET DIGITS USING EMD

Condition	Action
$\boldsymbol{If\ (s - f(g_1, g_2))\ mod\ 5 = 0}$	No modification
$\boldsymbol{If\ (s - f(g_1, g_2))\ mod\ 5 = 1}$	Increase g_1 by 1
$\boldsymbol{If\ (s - f(g_1, g_2))\ mod\ 5 = 2}$	Increase g_2 by 1
$\boldsymbol{If\ (s - f(g_1, g_2))\ mod\ 5 = 3}$	Decrease g_2 by 1
$\boldsymbol{If\ (s - f(g_1, g_2))\ mod\ 5 = 4}$	Decrease g_1 by 1

During the extraction phase, to extract the secret digit embedded in g_1 and g_2, the extraction function given in Eq. (3) is used.

B. *Multiple-Base Notational System (MBNS)*

Using MBNS [31], any positive integer R can be represented as digits in different bases:

$$R = (d_{n-1}, d_{n-2}, \dots, d_1, d_0)_{\{b_{n-1}, b_{n-2}, \dots, b_1, b_0\}}, \quad (4)$$

$$0 \le d_i \le b_i - 1,\ 0 \le i \le n - 1,$$

Where d_i is a digit represented in base b_i. Given a set of digits in different bases, the integer R is calculated using the equation:

$$R = \sum_{i=1}^{n-1} \left(d_i \times \prod_{j=0}^{i-1} b_j \right) + d_0. \quad (5)$$

For example, the decimal value 97 can be represented as $(1, 7, 2)_{\{10,12,5\}}$ since $1 \times 12 \times 5 + 7 \times 5 + 2 = 97$.

C. *Embedding Procedure*

Let *I* be a grayscale image of size 512 × 512 where its pixel values are reserved between 1 and 254, and *M* be the secret information. The detailed steps of embedding procedure are given below.

Input: A Cover grayscale image *I* of size 512 × 512, secret information *M*, block size *m*, threshold *t*.

Output: Stego-image I'.

Step 1: Convert the secret information *M* into its equivalent decimal form *S*.

Step 2: Make a copy of the input image and separate this copy into its 8 bit planes.

Step 3: Segment each bit plane (except the LSB – bit plane) into non-overlapping blocks of size *m* × *m*.

Step 4: Calculate the complexity *C* of the current block based on color changes between pixels. If *C* is less than or equals the pre-determined threshold *t* then let the base *b* = 4, otherwise let *b* = 5. The base *b* is used in Step 5.

Step 5: Extract a secret digit from the secret information *S* using Eq. (6)

$$S_b = S \bmod b \quad (6)$$

Step 6: Embed the extracted digit S_b into two consecutive pixels g_i and g_j of the cover image *I* using the EMD embedding scheme explained in Section III. A. Here, at most g_i or g_j is modified (i.e., increased or decreased by one) based on the conditions given in Table 1.

Step 7: If the complexity of the current block after embedding the secret digit S_b leads to change the base value calculated in Step 4, then 5 is added to the modified pixel if it is increased by one, otherwise 5 is subtracted from it.

Step 8: Set the new value of $S = (S - S_b) \bmod b$. If $S = 0$, then stop, otherwise, go to Step 4.

D. *Extraction Procedure*

Once the stego-image I' and other parameters are obtained, the embedded information can readily be extracted from I'. The extracting steps are given below:

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-57

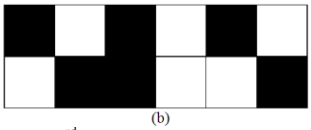
Input: A stego-image I', block size m, threshold t.
Output: Secret information M.
Step 1: Make a copy of the input image and separate this copy into its 8 bit planes.
Step 2: Segment each bit plane (except LSB – bit plane) into non-overlapping blocks of size $m \times m$.
Step 3: Calculate the complexity C for current block based on color changes between pixels. If C is less than or equals the pre-determined threshold t then put the base $b = 4$, otherwise $b = 5$.
Step 4: Use the extraction function given by Eq. (3) to extract a secret digit S_b (in base b) from two consecutive pixels g_i and g_j of the stego-image I'.
Step 5: After extracting all secret digits, the MBNS explained in Section III. B is applied to find the decimal secret information S.
Step 6: Convert the total decimal information S into the original secret information M. It is clear that the original cover image is not required in the extraction of the secret information.

E. *Simple Example*

To show how the proposed method works, suppose that the secret information M is $(00100101)_2$ and a cover image consists of 2 × 6 pixel values as shown in Fig. 5 (a) and the 3rd bit plane (shown in Fig. 5 (b)) of the cover image is utilized in the embedding and extraction procedures. Additionally, assume that the block's size value is $m = 2$ and the threshold $t = 2$. During the embedding phase, the secret information is converted into the equivalent decimal form $(37)_{10}$, and the 3rd bit plane is decomposed into 3 non-overlapping blocks each of size 2 × 2. The complexity C of the first block is 4, thus the base $b = 5$ and the value $S_b = (37 \bmod 5) = 2$ is extracted from the secret information. The value $S_b = 2$ is now embedded in the consecutive pixels 114 and 116 using the EMD scheme explained in Section III. A. Since $f(114, 116) = (114 + 2(116)) \bmod 5 = 1$ and $(S_b - f(114, 116)) \bmod 5 = (2 - 1)) \bmod 5 = 1$, the second condition of Table 1 is applied and the first pixel (i.e., 114) is increased by 1. The new values for the first two-consecutive pixels become 115 and 116. Since the new values do not change the complexity C of the first block, no modification is needed. The remaining secret information is $(37 – 2) \bmod 5 = 7$. For the second block, the complexity C is 2, thus $b = 4$ and the value $S_b = (7 \bmod 4) = 3$ is extracted from the secret information. Again, the value $S_b = 3$ is now embedded in the consecutive pixels 115 and 124 using the EMD scheme. Since $f(115, 124) = 3$ and $(3 - 3)) \bmod 5 = 0$, the first condition of Table 1 is applied and the pixels 115 and 114 do not change. The remaining secret information is $(7 – 3) \bmod 4 = 1$. For the third block, the complexity C is 4, thus $b = 5$ and the value $S_b = (1 \bmod 5) = 1$ is extracted from the secret information. Again, the value $S_b = 1$ is now embedded in the consecutive pixels 120 and 119 using the EMD scheme. Since $f(120, 119) = 3$ and $(1 - 3)) \bmod 5 = 3$, the fourth condition of Table 1 is applied and pixel 2 (i.e., 119) is decreased by 1. The new values for the third two-consecutive pixels become 120 and 118. Since the new values do not change the complexity C of the first block, no modification is needed. The remaining secret information is $(1 – 1) \bmod 5 = 0$, thus all secret information has been embedded. The resultant stego-image values are shown in Fig. 6 (a). Here, only 2 pixels have been modified to embed the value 37.

114	116	115	124	120	119
118	120	121	116	125	122

(a)



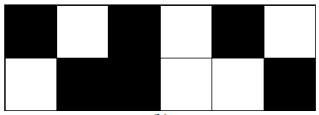
(b)

Fig. 5. (a) Cover image of size 2×6. (b) The 3rd bit plane of the cover image given in (a).

During the extraction phase, with the knowledge of the block size m and the threshold t, the secret information can readily be extracted from the stego-image I'. Given the stego-image pixel values shown in Fig. 6 (a), the 3rd bit plane (shown in Fig. 6 (b)) is decomposed into three non-overlapping blocks each of size 2 × 2. The complexity C of the first block is 4, thus the base $b = 5$. Using the extraction function given by Eq. (3), $f(115, 116) = 2$, thus the first extracted secret digit is $(2)_5$. For the second block, the complexity C is 2 and hence $b = 4$. The value of $f(115, 124) = 3$, thus the second extracted secret digit is $(3)_4$. For the last block, the complexity C is 4 and hence $b = 5$. The value of $f(120, 118) = 1$, thus the third extracted secret digit is $(1)_5$. Now, the extracted secret digits are converted into decimal value using the MBNS explained in Section III. B. This gives the value $S = (1, 3, 2)_{\{5, 4, 5\}} = 1 \times 4 \times 5 + 3 \times 5 + 2 = (37)_{10}$. The original secret information M is then obtained by converting S into the binary value $(00100101)_2$.

115	116	115	124	120	118
118	120	121	116	125	122

(a)



(b)

Fig. 6. (a) Stego-image of size 2×6. (b) The 3rd bit plane of the stego-image given in (a).

IV. Experimental Results and Analysis

This section presents the experimental results of the proposed technique. In our experiments, 7 grayscale digital images (6 of them are benchmarks) of sizes 512 × 512 were used as test images to evaluate the performance of the proposed method. The visual analysis of the image is performed by computing the peak signal-to-noise-ratio (PSNR). PSNR is used to measure the image quality through a comparison between the cover image and the stego-image:

$$PSNR = 10 \log_{10} \frac{(2^d - 1)^2}{MSE} dB \quad (7)$$

where d denotes to the bit depth of the cover image, and is equal to 8 for grayscale images. The MSE denotes to the mean square error between the cover image and the stego-image, and is defined as:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (S_{ij} - C_{ij}) \quad (8)$$

where S_{ij} and C_{ij} denote to the pixel values of the cover image and the stego-image, respectively. M and N represent the dimensions of the cover image. Table 2 shows the PSNR

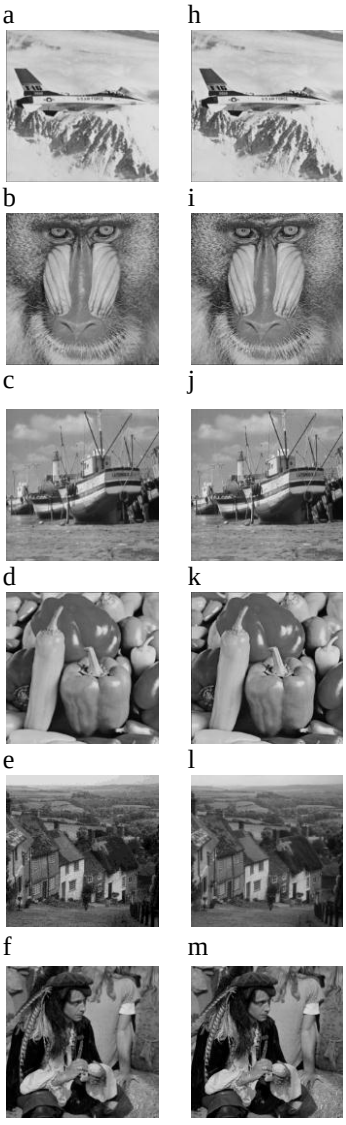
Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-57

values of different stego-images generated by the proposed method for different capacities. The cover images used for last experiments (i.e., capacity = 131072) are shown in Fig. 7 (a)-(g) where Fig. 7 (h)-(n) show the generated stego-images. It is obvious that the distortion that results due to the embedding process is invisible for human perception. Furthermore, a comparison with other related algorithms is presented in Table 3. It is clear from the table that the proposed method produces the lowest visual distortion to the original cover images after the embedding of secret information.

TABLE 2: PSNR VALUES OF DIFFERENT STEGO-IMAGES USING DIFFERENT CAPACITIES

Stego-image	Capacity (bit)		
	32768	65536	131072
Airplane	61.5367	58.3547	55.4359
Baboon	62.0207	59.4027	56.3904
Boat	61.4740	58.5190	55.6808
Peppers	61.6911	58.7346	55.8770
Goldhill	61.4540	58.3568	55.8322
Man	62.5794	59.7804	56.6922
School	61.7954	58.5814	56.1102
Average	**61.7930**	**58.8185**	**56.0027**



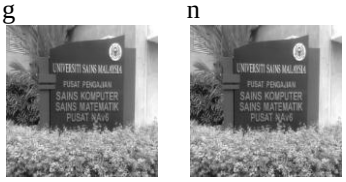


Fig. 7. The experimental results of the proposed method: (a)-(g) the test images, (h)-(n) the stego-images.

TABLE 3: QUALITY COMPARISONS WITH OTHER RELATED STEGANOGRAPHIC METHODS (COVER IMAGE: LENA OF SIZE 512×512)

Method	Capacity	PSNR (dB)
Bhattacharyya et al. [29]	32768	39.9760
Shi et al. [32]	24576	58.3274
LSB Substitution	32768	60.1802
Proposed	32768	61.4338

V. Conclusions and Future Work

In this paper, we proposed a new spatial-domain steganographic scheme based on BPCS method. The proposed scheme adopts the EMD technique and hides secret digits into pixels' pairs of the cover image. It has better embedding performance over other BPCS-based and LSB substitution methods in terms of capacity and image quality. As future work, different steganalytic methods, such as RS steganalysis attack [33] and PVD histogram analysis [34] will be used to determine the level of the security that the proposed scheme can achieve.

Acknowledgment

This research has used the High Precision Floating point (HPF) Matlab-based tool, written by John D'Errico, which offers more than 16 digits of accuracy.

References

[1] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Proceedings of International Conference on Advances in Cryptology (CRYPTO83)*, Paris, 1984, pp. 51-67.

[2] J. C. Ingemar, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2 ed. USA: Burlington, Morgan Kaufmann, 2008.

[3] P. Wayner, *Disappearing cryptography: information hiding: steganography and watermarking*, 3rd edition ed. USA: Morgan Kaufmann Publishers, 2009.

[4] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. Paiz, and S. Pogreb, "Applications for data hiding," *IBM systems journal*, vol. 39, pp. 547-568, 2000.

[5] M. Wu and B. Liu, "Data hiding in image and video. I. Fundamental issues and solutions," *IEEE Transactions on Image Processing*, vol. 12, pp. 685-695, 2003.

[6] C. Bergman and J. Davidson, "An Artificial Neural Network for Wavelet Steganalysis," presented at the Proceedings of Mathematical Methods in Pattern and Image Analysis, San Diego, CA, 2005.

[7] S. Premkumar and A. Narayanan, "New visual Steganography scheme for secure banking application," in *International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, Kumaracoil, 2012, pp. 1013-1016.

[8] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," *Signal Processing*, vol. 89, pp. 2324-2332, 2009.

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-57

[9] S. Atawneh, A. Almomani, and P. Sumari, "Steganography in digital images: Common approaches and tools," *IETE Technical Review*, vol. 30, p. 344, 2013.
[10] Z. K. AL-Ani, A. Zaidan, B. Zaidan, and H. Alanazi, "Overview: Main fundamentals for steganography," *Journal of Computing*, vol. 2, pp. 158-165, 2010.
[11] E. T. Lin and E. J. Delp, "A review of data hiding in digital images," in *Proceedings of the Image Processing, ImageQuality, Image Capture Systems Conference (PICS'99)*, Georgia, USA, 1999, pp. 274-278.
[12] D. Bloisi and L. Iocchi, "Image based Steganography and cryptography," *Computer Vision theory and applications*, vol. 1, pp. 127-134, 2007.
[13] D. T. Meva and A. D. Kothari, "Adoption of Neural Network Approach in Steganography and Digital Watermarking for Covert Communication and Copyright Protection," *International journal of Information Technology and Knowledge Management*, vol. 4, pp. 527-529, 2011.
[14] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Shamsuddin, "Information hiding using steganography," in *4th National Conference on Telecommunication Technology (NCTT 2003)*, Shah Alam, Malaysia, 2003, pp. 21-25.
[15] B. Dunbar, "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment," SANS Institute, Bethesda, Maryland18 January 2002 2002.
[16] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in *International Conference on Contemporary Computing (IC3-2008)*, Noida, India, 2008, pp. 105-114.
[17] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, 2010.
[18] M. Chen, R. Zhang, X. Niu, and Y. Yang, "Analysis of Current Steganography Tools: Classifications & Features," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06)*, Pasadena, CA, USA, 2006, pp. 384-387.
[19] S. Atawneh and P. Sumari, "Hybrid and Blind Steganographic Method for Digital Images Based on DWT and Chaotic Map," *Journal of Communications*, vol. 8, pp. 690-699, November-2013 2013.
[20] E. Franz and A. Schneidewind, "Adaptive steganography based on dithering," in *Proceedings of the ACM workshop on Multimedia and security*, Magdeburg,Germany, 2004, pp. 56-62.
[21] N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in *Information Hiding conference*, Oregon, USA, 1998, pp. 273-289.
[22] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Enhancing Steganography in digital images," in *Canadian Conference on Computer and Robot Vision*, Windsor, Ontario, 2008, pp. 326-332.
[23] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, 2005, pp. 1-12.
[24] N. A. Saleh, H. N. Boghdady, S. I. Shaheen, and A. M. Darwish, "High capacity lossless data embedding technique for palette images based on histogram analysis," *Digital Signal Processing*, vol. 20, pp. 1629-1636, 2010.
[25] J. C. Joo, H. Y. Lee, and H. K. Lee, "Improved steganographic method preserving pixel-value differencing histogram with modulus function," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, pp. 1-13, February 2010 2010.
[26] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, pp. 1613-1626, 2003.
[27] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *Journal of Systems and Software*, vol. 81, pp. 150-158, 2008.
[28] C. H. Yang, C. Y. Weng, H. K. Tso, and S. J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images," *Journal of Systems and Software*, vol. 84, pp. 669-678, 2011.
[29] S. Bhattacharyya, A. Khan, A. Nandi, A. Dasmalakar, S. Roy, and G. Sanyal, "Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography," in *World Congress on Information and Communication Technologies (WICT)*, Mumbai, 2011, pp. 36-41.
[30] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 432-444, 2012.
[31] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," *Signal Processing Letters, IEEE*, vol. 12, pp. 67-70, 2005.
[32] P. Shi, Z. Li, and T. Zhang, "A technique of improved steganography text based on chaos and BPCS," in *Advanced Computer Control (ICACC), 2010 2nd International Conference on*, 2010, pp. 232-236.
[33] J. Fridrich and M. Goljan, "Reliable detection of LSB steganography in color and grayscale images," USA Patent, 2004.
[34] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognition Letters*, vol. 25, pp. 331-339, 2004.

About Authors:

Samer Atawneh obtained his Master degree in Computer Science from University of Jordan in 2003. Currently, Mr. Atawneh is a Ph.D. candidate at the School of Computer Sciences, Universiti Sains Malaysia (USM), Malaysia. His research interests lie in Computer Security and Digital media fields like Steganography in Digital Images.

Putra Sumari obtained his MSc and PhD in 1997 and 2000 from Liverpool University, England. Currently, he is an Associate Professor at the School of Computer Sciences, Universiti Sains Malaysia (USM). His research areas include video on demand system, multimedia storage server, MPEG standard, image/video compression and retrieval, image Cryptography. He has published more than 70 papers related to these areas. He is the head of the Multimedia Computing Research Group, School of Computer Science, USM.