Run Length Based Steganography for Binary Images

Sos. S. Agaian and Ravindranath C. Cherukuri

ASPIIRE Lab, University of Texas at San Antonio,
6900 North Loop 1604 west, San Antonio, Texas-78249
sagaian@utsa.edu, mailcravi@yahoo.co.in

Abstract. Binary images (like cartoons, text documents, signatures captured by signing pads and/or 2-color imagery) are very commonly used in our daily life. Changing the pixel values in these images for hiding the data, may produce a noticeable change in the cover media. The primary problem is the capacity of the embedding technique and preserving the visible artifacts of the cover image even after embedding the secured data. In this paper, we present a run length based steganography algorithm for embedding the secured data into binary images. The proposed algorithm alters pixels of the embeddable blocks of cover image depending on there run length characteristics and chactersitics values of the block. In addition, the new algorithm is based on variable embedding rate for each block, which enhances the security of embedded data and the capacity of the embedding method. We test the performance of the algorithm over 50 various sizes of binary cover images embedding various sizes of secured data. Comparisons with existing algorithms will be presented.

Keyword: Run length, steganography, binary image.

1 Introduction

Steganography is the science that deals with the hiding of the secured information in a harmless signal. Binary images are two color (Black & White) images with pixel values (either 1 or 0). Therefore, embedding the secured data can easily distort the cover image. Hence, the amount of data that can be securely embedded into the binary cover image is very low. Several embedding algorithms have been developed for binary images using one of the frame work presented below:

- By altering the pixel value i.e. flipping of black pixel to white or vice versa.
- By changing the characteristics of the block in consideration i.e. thickness of strokes, curvature, spacing or relative positions.

For example, K.H. Hwang et.al [1] proposed an embedding algorithm that's embeds in the edge portion of the cover image. The prime factor is that modifications made to edge portions of the cover are more difficult to be recognized. Run length mechanism was introduced to make sure that pixel alterations are carried out in the edge portions only. Min.Wu and Bee Liu [2] proposed an embedding algorithm for binary images. The secured data is embedded into shuffled blocks by manipulating the flip able pixels. The shuffling of the blocks before embedding ensures the equalization of embedding capacity from region to region. H.K. Pan et.al [3] introduced the use of weighted matrix rather than secret key matrix and also altered the logical operation. The distortion in quality of the cover image remains. J. Chen et.al [5] proposed a

S.K. Pal et al. (Eds.): PReMI 2005, LNCS 3776, pp. 481 – 484, 2005.

technique that improves the effectiveness of the pan's technique [3]. The cover is decomposed into several 4x4 blocks. Each block is again portioned into four 3x3 overlapping blocks. The characteristic value of each sub-block defined by the number of ones in each block is determined for each block. For quality control no embedding is performed in when a sub-block characteristic value is 9 or 0.

In this paper, we investigate the following issues

1. How to select pixels for alteration so as to embed information with as little visual changes as possible to the cover.
2. How to enforce a relation ship between the blocks and Pn-sequence so as to embed information securely into the cover.
3. How to maximize the capacity of the proposed technique by employing a variable embedding rate for each block.

The rest of the paper is organized as follows. In Section 2, we introduce the proposed scheme for embedding the secured data into a binary cover image. Section 3 introduces the simulation results for the proposed algorithm for various images. And section 4 provides the conclusion.

2 Proposed Algorithm

The proposed algorithm embeds the secured information in secured regions and also increases capacity of the image by employing variably block embedding rate. The figure 1 shows the characteristics values of various blocks. The general steps in embedding the secured information into a binary cover media are:

Input: Binary cover and secured data

Step 1: Transform the data into binary format.
Step 2: Decompose cover into various blocks and determine their characteristic value and compute the runs in each block.
Step 3: Embedded binary secured data into cover depending runs and an embedding key.
Step 4: Measures are considered to ensure that the characteristic of blocks are unaltered.
Step 5: Recombine the blocks to retrieve the cover image with secured data.

Output: Cover image with secured data and key

The secured data embedded using the proposed scheme could maximize the capacity and limit the changes to those areas that are visibly hard to differentiate between the original and embedded cover images. Embedded information could be retrieved by exact inverse of the above steps.

3 Computer Simulation

Computer simulation was performed over 50 binary images of various sizes. Figure 1 original cover and the cover image after embedding 158 bits of the secured information in 82 blocks. The difference of 61 bits between the cartoon cover images before and after embedding the secured data of 158 bits is also presented.

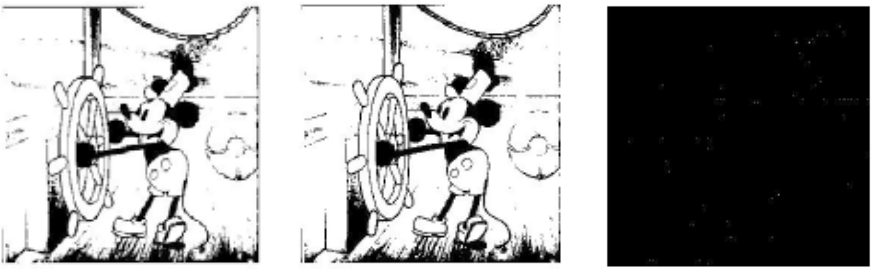

Fig. 1. The original cartoon cover of size 160 by 171, the cover image after embedding 158 bits and the difference of 61 bits between the cartoon cover images before and after embedding the secured data of 158 bits

Fig. 2. The Map cover image before, after and difference in cover images

Table 1. Simulation results for embedded information and distorted bits along the embedding and security coefficients

Image	Bits embedded	Distorted bits	EC	SC
Cartoon	158	61	0.00164	6.177
Sarkis	603	258	0.00268	5.872
Rock	759	297	0.00290	6.261
Map	134	44	0.00818	5.253

Table 2. Simulation results for various algorithms that embedded information in similar number of blocks

CV =3	New Method	Hwang et.al [1]	J.Chen [6]
Sarkis	1721	1204	918
Rock	2617	1908	1092
Map	267	178	159
Cartoon	450	534	233

Figure 2 the original cover and the cover image after embedding 134 bits of the secured information in 57 blocks. The difference of 44 bits between the cartoon cover images before and after embedding the secured data of 134 bits is also presented.

Table 1 introduces the simulation results for various images of varying sizes. The amount of data that is securely embedded is shown by number of bits embedded. The distance between the binary cover before and after embedding the data is presented by number of distorted bits. The embedding and security coefficient should be optimal for high robustness. We could enhance the security level of the embedded information by minimizing the security coefficient. Table 2 shows the comparison between various other existing algorithms in terms of maximum embedded information. We also introduce a visual comparison for determining if there is any loss in the visible artifacts of the cover image

4 Conclusion

We have presented a new block based steganography algorithm that utilizes run length characteristics for embedding the secured data into binary images. We employ a variable embedding rate for each block depending on its characteristic value for maximizing the capacity of new technique. In addition, the new algorithm enhances the security level of secured data embedded into a binary cover image by limiting the altered pixels to edges only. We also present a visualization comparison between the new and existing algorithms.

Acknowledgement

This research was partially funded by Center for Infrastructure Assurance and Security (CIAS).

References

1. K. F. Hwang and C. C. Chang, “A Run Length Mechanism for Hiding Data into Binary Images”, In proceedings of pacific rim workshop on digital steganography 2002, pp.71-74.
2. Min Wu; Bede Liu; “Data hiding in binary image for authentication and annotation” in proceedings of IEEE Transactions on multimedia, Vol: 6, Aug 2004 Pg: 528 – 538.
3. H.K. Pan, Y.Y. Chen and Y.C. Tseng, “A Secure Data Hiding Scheme for Two-Color Images”, in proceedings of 5th IEEE Symposium on computers and communication, 2000 pp.750-755.
4. Yu-Chee Tseng; Hsiang-Kuang Pan, “Secure and invisible data hiding in 2-color images”, in proceedings of 20 th IEEE Computer and Communications Societies, INFOCOM 2001 Volume: 2, Pg: 887 - 896 April 2001.
5. J. Chen; T. S. Chen & M. W Cheng, “A New Data Hiding Method in Binary Image”, in proceedings of 5th IEEE international symposium on multimedia software engineering 2003