

Weighted bipartite graph for locating optimal LSB substitution for secret embedding*

Cheng-Hsing Yang

*Department of Computer Science
National Pingtung University of Education
Pingtung
Taiwan 900
R.O.C.*

Shiuh-Jeng Wang[†]

*Department of Information Management
Central Police University
Taoyuan
Taiwan 333
R.O.C.*

Abstract

Simple least-significant-bit (LSB) substitution is an approach used to embed a secret image in the least significant bits of the pixels in a host image. In order to reduce the degradation of host image after embedding, an optimal LSB substitution scheme was proposed by [9]. Because the exhaustive search for an optimal solution was very time consuming, however, Wang et al. [9] proposed a genetic algorithm to search for approximate optimal solutions. Also, Chang et al. [10] proposed a dynamic programming strategy to efficiently obtain an optimal solution. In this paper, in virtue of efficient algorithm, we propose a new approach to find an optimal solution, which is inspired on the maximum matching of a weighted bipartite graph. Regardless the time required for constructing a weighted bipartite graph, in theory, the time complexity of our approach is $O(N^3)$ only, it is obviously better than the complexity analysis of $O(2^N)$ in [10], where N is equal to 2^k for k -LSB.

Keywords : *Information hiding, LSP, bipartite graph, maximum matching.*

*This work was supported in part by National Science Council in R.O.C. under Grant No. NSC-42186F and No. NSC 94-2213-E-015-001.

[†]E-mail: sjwang@mail.cpu.edu.tw

Journal of Discrete Mathematical Sciences & Cryptography

Vol. 9 (2006), No. 1, pp. 153–164

© Taru Publications