Chapter 7
A Study on Embedding Efficiency of Matrix Encoding

Lifang Yu
Beijing Jiaotong University, China

Yao Zhao
Beijing Jiaotong University, China

Yun Q. Shi
New Jersey Institute of Technology, USA

Rongrong Ni
Beijing Jiaotong University, China

Gang Cao
Beijing Jiaotong University, China

ABSTRACT

In this paper, the authors examine embedding efficiency, which influences the most concerned performance of steganography, security, directly. Embedding efficiency is defined as the number of random message bits embedded per embedding change. Recently, matrix embedding has gained extensive attention because of its outstanding performance in boosting steganographic schemes' embedding efficiency. Firstly, the authors evaluate embedding change not only on the number of changed coefficients but also on the varying magnitude of changed coefficients. Secondly, embedding efficiency of matrix embedding with different radixes is formularized and investigated. A conclusion is drawn that ternary matrix embedding can achieve the highest embedding efficiency.

INTRODUCTION

Digital steganographic techniques aim at embedding secret messages into a carrier signal by altering its least significant components for covert communication (Wang, 2004). On the opposite side, steganalytic techniques aim at finding out if a given signal bears secret messages or not. The most important requirement of steganography is undetectability (security) – malicious attackers should not be able to distinguish between cover and stego objects with success better than random guess.

Steganographic techniques can mainly be divided into two categories in terms of the ways they explored to enhance their security performance.

DOI: 10.4018/978-1-4666-4006-1.ch007

Techniques of the first category embed information into host signals in such a way that no image features are significantly perturbed during the embedding process (Mielikainen, 2006; Sharp, 2001; Sallee, 2004, 2005; Provos, 2001; Latham, 2008; Upham, 1997; Fridrich et al., 2004; Wu & Tsai, 2003; Kawaguchi & Eason, 1998; Hioki, 2002; Pevny et al., 2010; Westfeld, 2001; Kim et al., 2006; Goljan et al., 2006; Sachnev & Kim, 2010), while techniques of the other category embed data in such a way that it distorts the steganalyst's estimate of the cover image statistics (Solanki et al., 2007; Sarkar, Solanki et al., 2008; Sarkar, Nataraj et al., 2008; Yu et al., 2010). Nowadays, the most popular way is to seek the lowest possible rate of modification to the cover signal or the highest possible embedding capacity at a given distortion level, and it belongs to the first category.

Embedding efficiency (Westfeld, 2001) is a quantity that measures embedding capacity at given distortion level, which is defined as the number of random message bits embedded per one embedding change.

Matrix embedding is an effective technique to improve embedding efficiency. The idea of importing matrix embedding to steganography was proposed by Crandall (Crandall, 1998). Westfeld (2001) firstly implemented binary matrix embedding into F5, which resorts to the Hamming codes to reduce modification on the quantized block discrete cosine transform (BDCT) coefficients of a cover JPEG image. Later, binary matrix embedding is also used in modified matrix encoding (MME) (Kim, 2006) with side information and has demonstrated distinguished performance. Ternary matrix embedding is first proposed by Goljan et al. (2006) in spatial domain and has shown obviously superior embedding efficiency than binary matrix encoding. Then it is used by Sachnev et al. (2010) in JPEG domain which outperforms binary matrix embedding based MME.

Steganographic embedding efficiency of matrix embedding has been studied in (Fridrich et al., 2006), and ternary matrix embedding is shown to outperform binary matrix embedding by comparing upper bounds of their embedding efficiencies. But neither whether ternary matrix embedding outperforms binary matrix embedding in practice, nor whether ternary matrix embedding outperforms $r-$ary $(r>3)$ matrix embedding, is clear. In this paper, we evaluate embedding change not only on the number of changed coefficients but also on the varying magnitude of changed coefficients. Through mathematical analysis on embedding efficiency, we prove that ternary matrix embedding outperforms $r-$ary $(r \neq 3)$ matrix embedding in terms of embedding efficiency.

This paper is organized as follows. In the next section, we define change and drive the formula of embedding efficiency based on this definition. Terms and symbols used in this paper are also introduced in this section. Following this, we mathematically analyze properties of embedding efficiency and embedding rate, respectively. Then embedding efficiency of matrix embedding with different radixes are compared and ternary matrix embedding is demonstrated to gain the highest embedding efficiency. Finally, we draw our conclusions.

PRELIMINARIES

In this paper, we constrain ourselves on matrix embedding realized using $(1, n, k)$ Hamming codes (Morelos-Zaragoza, 2006), which means k message symbols will be embedded into each cover block of length n by modifying at most one coefficient of each block. Some parameters are defined as follows.

- r : Radix of matrix embedding using linear codes (Hamming codes). It is a prime power.