Evaluating the Suitability of Color Spaces for Image Steganography and its Application in Wireless Capsule Endoscopy

Khan Muhammad, Jamil Ahmad, Muhammad Sajjad,
Sung Wook Baik*
Digital Contents Research Institute
Sejong University, Seoul, South Korea
khanmuhammad@sju.ac.kr, jamilahmad@sju.ac.kr,
sajjad@sju.ac.kr, sbaik@sejong.ac.kr

Seungmin Rho
Department of Multimedia
Sungkyul University, Anyang, South Korea
smrho@sungkyul.ac.kr

***Abstract*— Image steganography is the art of concealing sensitive information inside cover images. Most of the existing steganographic algorithms use correlated color space such as RGB, where changes to one channel degrade the quality of stego-images due to its strong correlation, thereby making them less suitable for steganography. In this paper, we investigate the suitability of both correlated and uncorrelated color spaces for steganography considering time complexity and image quality. Based on this evaluation criteria, we suggest HSV as the most suitable color space for steganography among the four color models including RGB, YCbCr, HSI, and Lab. Furthermore, we propose an imperceptible steganographic method using the chosen color space based on block-wise magic least significant bit substitution which achieves balance between the time complexity and image quality. Our preliminary experimental results not only validate the superiority of the proposed method in terms of computational complexity and image quality but also suggest its potential application for secure transmission of key frames generated during wireless capsule endoscopy.**

Keywords— ***Image Steganography; Multimedia Security; Uncorrelated Color Space; Video Summarization; Information Security;***

I. INTRODUCTION

In current literature of information security, there are numerous image steganographic algorithms that embed secret information within host images. The ultimate goal is to embed as more secret data as possible while keeping the carrier image quality intact in a cost-effective manner. Majority of the existing steganographic methods use correlated color space (RGB), where changes to one plane affect the overall quality of the image [1]. This produces a stego image of low-quality where the embedded information can be detected using human visual system (HVS). Hence, RGB color model is relatively less suitable for achieving the ultimate goal of steganography. Besides RGB color space, there exists several uncorrelated color models such as HSI, HSV, YCbCr, and Lab which can be modified for information hiding [2]. However, it is relatively difficult to select a color space for steganography which could maintain the image quality as well as require less time complexity. The reason is that some color spaces need extensive time for conversion while others produce stego images of unsatisfied quality. Hence, it is desirable to exploit a color space that can maintain a balance between visual quality and time complexity.

In an attempt to achieve this goal, researchers have explored various uncorrelated color models for steganography [3, 4]. Agaian et al., [5] compared RGB, YCbCr, and HSV based on root-mean-square (RMS) error and argued that YCbCr and HSV are relatively better color spaces for steganography. However, they conducted no experiment for suitability of HSV and further selection within YCbCr and HSV. In addition, their evaluation criteria fails to consider running time and visual quality of marked images, which are comparatively more important than RMS. Therefore, in this paper, we surmount these limitations by considering the visual quality and time complexity in our evaluation criteria and present an imperceptible steganographic scheme using the chosen color space.

II. METHODOLOGY

In this section, we present an overview of the proposed method based on the designated HSV color space for data hiding. The reasons behind this selection include its de-correlated property, cost-effectiveness, and better image quality of marked images as verified by experimental results in Table 1. The embedding algorithm used in the proposed scheme is block-wise magic LSB method, improving the visual quality of stego images. In addition, it scatters the sensitive information within the whole image, making its extraction relatively difficult for malicious users. The major steps of the proposed embedding algorithm are given in Algorithm 1. For extraction of embedded data, the receiver has to apply the reverse operations of algorithm 1. A brief pictorial representation of the proposed scheme is depicted in Fig. 1.

*Corresponding author; Tel.: +82-02-3408-3797; Fax: +82-02-3408-4339

978-1-4673-8685-2/16/$31.00 ©2016 IEEE

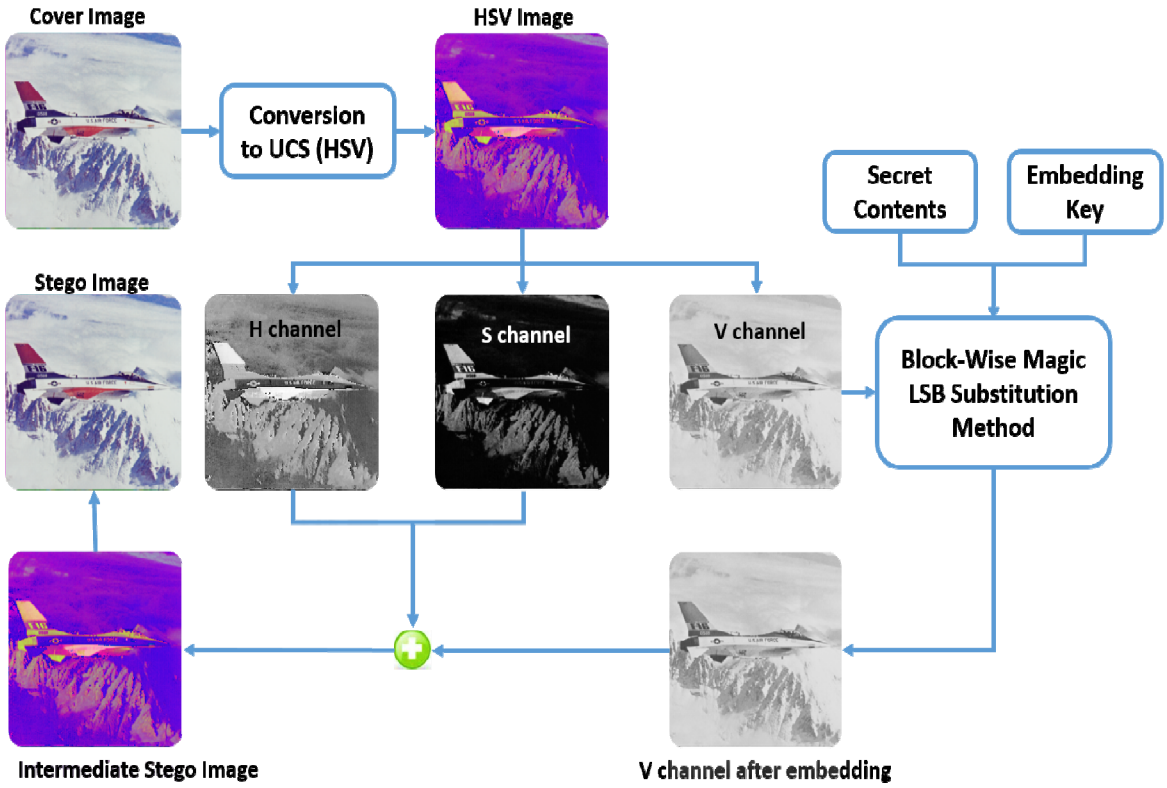

Fig. 1. Pictorial representation of the proposed scheme

Algorithm 1. Block-wise Magic LSB Substitution Method

Input: Input image I, Sensitive Contents S, and Embedding Key K

1. Determine block size ℓ and transform I from RGB to HSV.
2. Select blocks of size $1\times\ell$ from S, according to K
3. Divide V plane of HSV image into $\ell\times\ell$ sized blocks
4. Generate $\ell\times\ell$ sized magic matrix M
5. Set counter $(i)\leftarrow 1$ and block number $(j)\leftarrow 1$
6. **While** $(i \le Sizeof\, S)$, **do**
   a. Consider a block B_j from V
   b. Replace LSBs of the block pixels according to M values.
   c. $i \leftarrow i+\ell^2$ and $j \leftarrow j+1$;

   End
7. Combine H, S, and stego V and transform it to RGB to get stego image.

Output: Final Stego Image I_{SRGB}

III. Experiments and Results

The proposed scheme is compared with six state-of-the-art methods including classic LSB, LSBM [6], LSBMR [7], SCC[8], simple HSI (SHSI) [3], and HSI-MLSB [4]. The comparison is done based on image dataset USC-SIPI-ID[9] using peak-signal-to-noise ratio (PSNR) and structural similarity index metric (SSIM). Table 1 shows the results of various color spaces based on our evaluation criteria. A message of size 8192 bytes is embedded within 50 images by using the channels enclosed in parenthesis as shown in Table 1. The results validate the suitability of nominated color space for steganography.

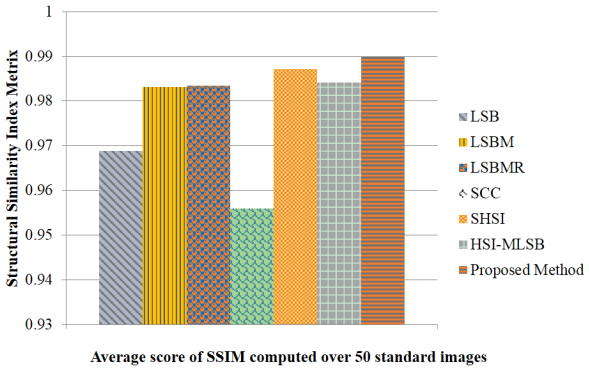

Fig. 2: Quantitative evaluation based on SSIM

PSNR sometimes fails to capture all the structural information distorted by data embedding. Therefore, we use an additional metric SSIM, considering the human perception while measuring the image quality [10]. The statistics computed using SSIM are shown in Fig. 2, providing better image quality of the proposed scheme compared to other methods.

TABLE I. PERFORMANCE EVALUATION OF VARIOUS COLOR SPACES FOR DATA HIDING BASED ON PSNR AND EXECUTION TIME.

Evaluation Metric	RGB (R)	RGB (G)	RGB (B)	HSI (I)	YCbCr (Y)	Lab (L)	HSV (V)
Average PSNR score over 50 images	52. 7957	49.7898	54.3541	53.230	52.1612	27.610	**56.3413**
Total execution time (Sec) for 50 images	49.73	49.3292	49.2898	51.541	49.6435	13.761	**49.2669**
Execution time per image (sec)	0.9946	0.9865	0.9857	1.030	0.9928	0.2752	**0.9853**

IV. Conclusions and Futute Work

In this paper, we have evaluated the performance of correlated and uncorrelated color spaces for selecting the best color model for steganography. We have considered five color representation systems including RGB, HSI, HSV, YCbCr, and Lab. Our evaluation criteria reflecting upon image quality and time complexity suggests HSV as the most feasible choice for steganography compared to other color models. Additionally, we have proposed an imperceptible block-wise magic LSB substitution scheme using the designated color space, which provides better security while keeping the marked images intact in a cost-effective way. Finally, we have suggested an important application of the proposed scheme for secure transmission of key frames generated during wireless capsule endoscopy.

In future, we plan to increase the security and payload of the proposed scheme by encrypting the sensitive contents prior to embedding and considering edge detection models[11] during data hiding, respectively. We also have intension to further explore the suggested application of the proposed method in wireless capsule endoscopy

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2061978).

References

[1] M. Khan, A. Jamil, F. Haleem, J. Zahoor, S. Muhammad, and B. Sung Wook, "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption," *KSII Transactions on Internet and Information Systems (TIIS),* vol. 9, pp. 1938-1962, 2015.

[2] S. S. Agaian and J. P. Perez, "New Pixel Sorting Method for Palette Based Steganography and Color Model Selection," *The University of Texas, San Antonio,* 2004.

[3] K. Muhammad, J. Ahmad, H. Farman, and M. Zubair, "A Novel Image Steganographic Approach for Hiding Text in Color Images Using HSI Color Model," *Middle-East Journal of Scientific Research,* vol. 22, pp. 647-654, 2014.

[4] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools and Applications,* pp. 1-27, 2015/05/24 2015.

[5] S. S. Agaian, B. Rodriguez, and J. P. Perez, "Stego sensitivity measure and multibit plane based steganography using different color models," in *Electronic Imaging 2006*, 2006, pp. 60720Q-60720Q-12.

[6] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *Information Forensics and Security, IEEE Transactions on,* vol. 5, pp. 201-214, 2010.

[7] J. Mielikainen, "LSB matching revisited," *Signal Processing Letters, IEEE,* vol. 13, pp. 285-287, 2006.

[8] K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Multimedia Tools and Applications,* vol. 30, pp. 55-88, 2006.

[9] "The USC-SIPI Image Database. http://sipi.usc.edu/services/database/Database.html. 2003.."

[10] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and R. J. Qureshi, "A secure cyclic steganographic technique for color images using randomization," *Technical Journal, University of Engineering and Technology Taxila,* vol. 19, pp. 57-64, 2015.

[11] K. Muhammad, I. Mehmood, M. Y. Lee, S. M. Ji, and S. W. Baik, "Ontology-based Secure Retrieval of Semantically Significant Visual Contents," *Journal of Korean Institute of Next Generation Computing,* vol. 11, pp. 87-96, 2015.