The 11th International Conference on Multimedia Information Technology and Applications (MITA 2015)
June 30-July 2, 2015, Tashkent, Uzbekistan

Secure Visual Content Labelling for Personalized Image Retrieval

Khan Muhammad, Irfan Mehmood, Muhammad Sajjad, Jamil Ahmad, Seong Joon Yoo, Dongil Han, Sung Wook Baik*
Digital Contents Research Institute, Sejong University,
Seoul, Republic of Korea
khanmuhammad@sju.ac.kr , irfanmehmood@sju.ac.kr, sajjad@sju.ac.kr, jamilahmad@sju.ac.kr, sjyoo@sejong.ac.kr, dihan@sejong.ac.kr, sbaik@sejong.ac.kr

***Abstract*—Automatic image / video labeling and indexing is an enthusiastic research area where visual contents are described using low- and high-level features such as shape, color, texture, and visual saliency. Researchers have proposed different techniques for automatic labeling of imaging data, enhancing the performance of content-based image retrieval systems. However, the complex and diverse nature of visual contents make automatic labelling very challenging. Furthermore, traditional labeling methods do not consider security issues, making third party to easily manipulate and retrieve personal records. In this context, we propose an efficient framework for secure data labeling using multi-algorithmic image steganography, where the description of every image is embedded as a secret information inside it, resulting in stego images. At the time of required image retrieval from huge visual data, the hidden description is decrypted from the stego image, extracting semantically relevant contents. The proposed framework reduces the computational complexity, making it more suitable for secure, real-time and desired content retrieval from personalized image databases. The experimental results validate the efficiency and security of proposed framework as compared to other state-of-the-art methods.**

***Keywords*—Image Classification, Information Security, Multimedia Security, Image Steganography**

I. INTRODUCTION

The exponential growth in digital data has realized the researchers to develop efficient and optimized techniques for image labelling in a reasonable amount of time from huge imaging data. Various techniques exist for automatic image labelling and retrieval such as text-based methods, low and high-level features-based methods. In text-based methods, annotations are determined using the text provided by the users. However, most of these user-defined annotations are ambiguous, misleading accurate content retrieval from huge multimedia data. To address this issue, researchers have proposed various computer vision techniques for accurate and automatic labelling of huge imaging data. However, these computer vision based methods fail to describe the visual content, resulting in sematic gap between human perception and computer generated labels.

To understand a scene in a given image, computer vision methods extract low-level features (color, shape, and texture), map them to high-level features (objects detection, graph construction and graph matching) for scene understanding. This process requires extensive computations, making the existence techniques less efficient for image labeling, hence less suitable for content-based image retrieval systems. In addition, security is also a major issue in existing visual content labelling methods, while dealing with personalized records. In this paper, we propose a secure labelling method based on image steganography, resulting in efficient and secure retrieval and scene understanding systems.

II. METHODOLOGY

The proposed framework uses a two-step process for image labeling: (a) Description embedding using multi-algorithmic steganography and (b) Classification of images. The major steps of the proposed framework are pictorially shown in Fig. 1.

A. Description embedding using multi-algorithmic steganography

In this section, a distinctive description/labels data is embedded in a given image, selected from database as follows: Consider an input cover image $I_C \in \mathbb{R}^{MxN}$, partitioned into four equally sized sub-blocks I_{B1}, I_{B2}, I_{B3}, and I_{B4}. The motivational factor behind image partitioning is to scatter the secret description in different areas of the cover image and use four different light-weight algorithms for data hiding, making the extraction of secret information more challenging for unauthorized individuals. The secret description is divided into four blocks, each of which is then embedded into one of the sub-images I_{B1}, I_{B2}, I_{B3}, and I_{B4}, using one of the four algorithms, selected based on a secret key, deceiving the attackers. The algorithms used for labels hiding are least significant bit matching (LSB-M)[1], LSB-M revisited (LSB-MR)[2], our recently published algorithms cyclic steganographic technique (CST)[3] and HSI-LSB[4] with some improvements (HSI-MLSB). Description and input image division into sub-blocks and secret key based algorithm selection secure the image classification process, which are the major motivational reasons for their usage.

* Corresponding author: Sung Wook Baik

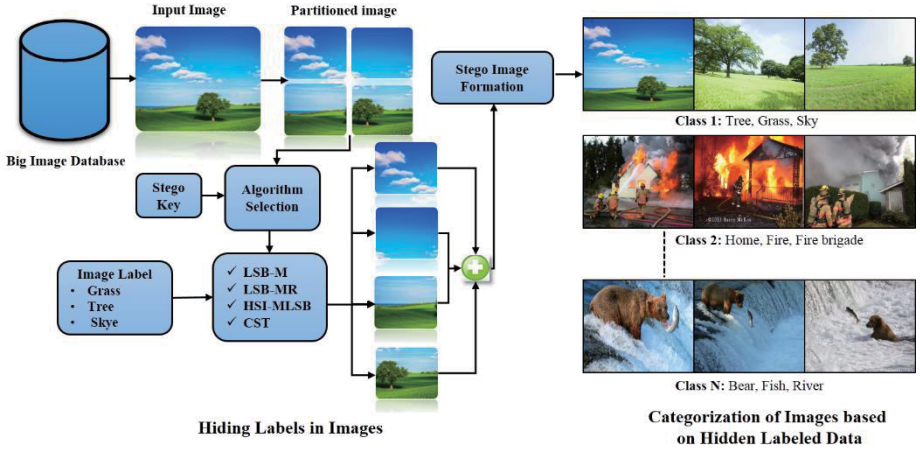

Fig. 1: Framework of the proposed classification system

B. *Classification of Images*

In this section, a given stego image is assigned to its corresponding class based on the extracted description and labels. The hidden information is extracted using the reverse operations of description embedding process. This makes the image classification secure as well as efficient because the proposed framework uses light-weight algorithms for description hiding in spatial domain.

III. EXPERIMENTAL RESULTS

The proposed system is compared with low-level and high-level features extraction based techniques on UKBench dataset. The security aspect of proposed framework is compared with four state-of-the-art data hiding algorithms (LSB-M, LSB-MR, CST and HSI-MLSB[5]) based on standard metric peak signal-to-noise ratio (PSNR), which computes distortion caused in stego images after embedding secret data. Higher PSNR score shows better quality of stego images. The experimental results based on execution time and PSNR are shown in Fig. 2 and Fig. 3, clearly dominating the various features extraction based techniques and data hiding techniques.

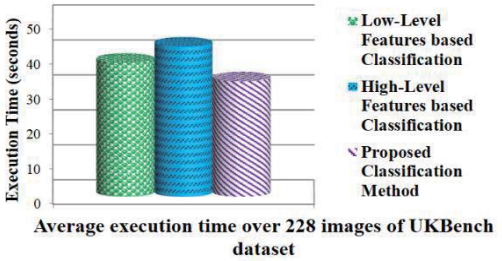

Fig. 2: Comparison of the proposed system with low-level and high-level features extraction based image classification methods using execution time

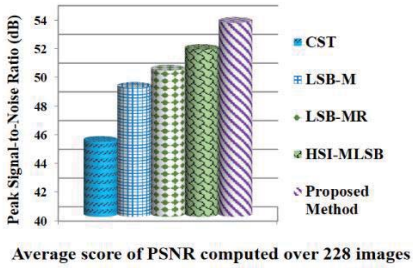

Fig. 3: Security comparison of the proposed system using PSNR with other four methods

IV. CONCLUSION

In this paper, an efficient and cost-effective framework is presented using multi-algorithmic image steganography for visual content labeling. The proposed system hides relevant and distinctive descriptions inside images using multi-algorithmic method, resulting in better security and making content-based retrieval methods more secure and efficient. Experimental results validate the effectiveness of the proposed framework in making the labelling process efficient, secure, and one of the best candidate for real-time image content-based retrieval systems.

ACKNOWLEDGMENT

This research is supported by the ICT R&D program of MSIP/IITP. [2014(R0112-14-1014), the Development of Open Platform for Service of Convergence Contents].

REFERENCES

[1] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *Signal Processing Letters, IEEE,* vol. 12, pp. 441-444, 2005.

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

[3] N. U. R. Jamil Ahmad, Zahoor Jan, Khan Muhammad, "A Secure Cyclic Steganographic Technique for Color Images using Randomization," *Technical Journal, University of Engineering and Technology Taxila, Pakistan,* vol. 19, pp. 57-64, 2014.

[4] 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.

[5] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. 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.