ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# Image steganography using uncorrelated color space and its application for security of visual contents in online social networks

Khan Muhammad [a], Muhammad Sajjad [b], Irfan Mehmood [c], Seungmin Rho [d], Sung Wook Baik [a,*]

[a] Intelligent Media Laboratory, Digital Contents Research Institute, College of Electronics and Information Engineering, Sejong University, Seoul, Republic of Korea

[b] Digital Image Processing Laboratory, Department of Computer Science, Islamia College Peshawar, Pakistan

[c] Department of Computer Science and Engineering, Sejong University, Seoul, Republic of Korea

[d] Department of Media Software, Sungkyul University, Anyang, Republic of Korea

## HIGHLIGHTS

- A secure framework for ensuring the security of visual contents in online social networks.
- Image scrambling using a light-weighted image scrambler before data embedding.
- Encryption of sensitive contents using iterative magic matrix-based encryption algorithm.
- Data hiding using an adaptive LSB substitution method.

## ARTICLE INFO

*Article history:*
Received 16 June 2016
Received in revised form
14 October 2016
Accepted 24 November 2016
Available online xxxx

*Keywords:*
Information security
Online social networks
Image steganography
Security in social networking
Image and video processing
Uncorrelated color space

## ABSTRACT

Image steganography is a growing research field, where sensitive contents are embedded in images, keeping their visual quality intact. Researchers have used correlated color space such as RGB, where modification to one channel affects the overall quality of stego-images, hence decreasing its suitability for steganographic algorithms. Therefore, in this paper, we propose an adaptive LSB substitution method using uncorrelated color space, increasing the property of imperceptibility while minimizing the chances of detection by the human vision system. In the proposed scheme, the input image is passed through an image scrambler, resulting in an encrypted image, preserving the privacy of image contents, and then converted to HSV color space for further processing. The secret contents are encrypted using an iterative magic matrix encryption algorithm (IMMEA) for better security, producing the cipher contents. An adaptive LSB substitution method is then used to embed the encrypted data inside the V-plane of HSV color model based on secret key-directed block magic LSB mechanism. The idea of utilizing HSV color space for data hiding is inspired from its properties including de-correlation, cost-effectiveness in processing, better stego image quality, and suitability for steganography as verified by our experiments, compared to other color spaces such as RGB, YCbCr, HSI, and Lab. The quantitative and qualitative experimental results of the proposed framework and its application for addressing the security and privacy of visual contents in online social networks (OSNs), confirm its effectiveness in contrast to state-of-the-art methods.



## 1. Introduction

Image steganography is a special branch of information security, where sensitive contents are embedded in images for hiding its existence without being detected by human visual system (HVS) [1,2]. Recent years have shown extensive research interests in image steganography as it offers the promise of overcoming some of the inherent limitations of

* Corresponding author. Fax: +82 02 3408 4339.
*E-mail addresses:* khan.muhammad.icp@gmail.com, khanmuhammad@sju.ac.kr (K. Muhammad), muhammad.sajjad@icp.edu.pk (M. Sajjad), irfan@sejong.ac.kr (I. Mehmood), smrho@sungkyul.edu (S. Rho), sbaik@sejong.ac.kr (S.W. Baik).

http://dx.doi.org/10.1016/j.future.2016.11.029
0167-739X/

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

cryptographic methods such as huge computational complexity and scrambled form of cipher, attracting the attention of attackers, resulting in modification or decryption of secret data [3]. Image steganography can also be utilized for a large number of useful applications such as secure communication between two communicating parties [4], secure mobile computing [5], securing online voting systems, captioning and contents protection [6,7], secure surveillance systems, personalized secure image retrieval, and privacy-protection of medical records. Watermarking is another closely related technology to image steganography, focusing on copyright protection of sensitive contents [8].

Image steganographic methods are divided into two broad categories: spatial domain and frequency domain. Spatial domain techniques [9–13] are concerned with the direct modification of image pixels, employing higher payload and imperceptibility, but lack resiliency against statistical attacks [14,15]. On the other hand, frequency domain methods [16–19] utilize the transformed co-efficients for data embedding, resulting from various transforms including DWT, DFT, and DCT. These methods have better resiliency against image processing attacks, but are computationally complex with limited payload [15], making them unsuitable for various real-time applications [20,21]. Therefore, keeping in view the proposed work, we discuss here only those image steganographic techniques that are related to the spatial domain.

Most spatial domain techniques are based on correlated color space (RGB), ranging from the simple LSB substitution method [22] to advanced edges and saliency based methods [23–26]. In the LSB approach, the LSB of each pixel is replaced with secret bits following a scanning path directed by a secret key, resulting in a payload of 1 bits per pixel (bpp). The payload can be increased by replacing the second and third LSB planes of the input image, but this produces noticeable distortion [27]. In an attempt to reduce the distortion, Wang et al. [28] utilized a genetic algorithm with LSB substitution but with extra computational complexity, which limits its effectiveness. Change et al. [29] attempted to reduce the time complexity presenting a fast LSB approach combined with dynamic programming. Lin et al. [30] explored modulus functions combined with the LSB method, producing better visual quality. Lou et al. [31] focused on resiliency against cover carrier attacks by hiding a variable amount of sensitive contents. This technique is simple with easy detection. Lin et al. [32] addressed image authentication using a steganographic method in contents sharing scenarios. In an attempt to improve visual quality, Chang et al. [33] nominated a pixel adjustment strategy for data embedding, which was further improved by Wu et al. [34] using pixel value differencing. The authors in [35] presented the LSB matching (LSBM) method that reduces the asymmetric effects by randomly adding $\pm 1$ to each pixel of the input image, but this addition depends on the secret bits and pixels of the cover image. Mielikainen [13] proposed an LSBM revisited (LSBMR) approach, which interprets the image pixels independently by concealing two bits in a two-pixels pair, further minimizing the asymmetric artifacts of the various LSB based approaches.

The aforementioned methods do not consider the pixel relationship during the process of data hiding, thereby equally affect all the smooth and edgy areas of the given image, resulting in limited payload and low visual quality. Tsai et al. [36] explored this concept of pixel relationship by hiding more data in the pixels lies in the edgy area while limiting the number of bits in the smooth area's pixels, increasing the capacity as well as visual quality. Taking motivation from this idea, different researchers proposed numerous improved versions of Tsai's approach. Chen et al. [26] boosted up the payload of Tsai's method by employing hybrid edge detection filters, which were integrated with the LSBMR method by Luo et al. [35], producing higher capacity and imperceptibility. Ioannidou et al. [25] extended this approach to RGB images, achieving 3 times greater capacity than previous methods. Kanan et al. [24] focused on edges based tunability keeping a balance between payload and image quality, making it more suitable for several applications.

The methods discussed so far utilize correlated color space for message embedding, where minor intentional changes in any of the channel affect other channels, resulting in lower quality. Furthermore, the current traditional methods hide sensitive contents without encryption, increasing the chances of data extraction by adversaries on successful attacks of data hiding algorithm, hence decreasing its security. In this article, we propose a novel framework to address these two problems. The main contributions of this work are summarized as follows:

1. A secure framework for an imperceptible steganographic algorithm utilizing UCS with reasonable balance between image quality and security, increasing its suitability for real-time security applications such as confidential networks and security of visual contents in online social networks. To the best of our knowledge, we have suggested the proposed application for the first time to handle the security issues of visual contents in OSNs using image steganography.
2. The cover image is scrambled using a light-weighted image scrambler before data embedding, persevering the privacy of image contents, which is one of the demanded requirements of OSN applications.
3. The sensitive contents are encrypted using an encryption algorithm based on the concept of iterative magic matrix, providing an encoded message. This introduces an extra barrier for adversaries during data extraction.
4. The encrypted sensitive contents are embedded using an adaptive LSB substitution method based on secret key-directed block-by-block mechanism, resulting in better visual quality as well as making the process of data extraction very challenging for attackers.

The rest of the paper is structured as follows. Section 2 presents the detail of the proposed framework along with its major sub-sections. Section 3 illustrates experimental results and discussion. The potential application of the proposed framework in OSNs with incorporation of image steganography technology is highlighted in Section 4, followed by conclusion and future research directions in Section 5.

## 2. Proposed framework

In this section, the proposed framework is described in detail augmented by its pictorial representation facilitating readers to easily understand its conceptual novelty. The proposed framework consists of three main components including an image scrambler, an iterative magic matrix based encryption algorithm (IMMEA), and an adaptive LSB substitution method for embedding encrypted data. These major components and intermediate steps of the proposed framework are illustrated in Fig. 1.

To understand the proposed work, we present a comprehensive explanation of the major steps of the proposed method using terminologies and symbols given in Table 1. Suppose $I_{RGB}$ is the input cover image and we want to embed the sensitive contents $S_{SC}$ inside it using the proposed method. First, $I_{RGB}$ is passed through a proposed image scrambler *ImgScrm*, as in Eq. (1), producing an encrypted image. The motivational reason behind image scrambling is to protect the privacy of the image contents, which is mostly desirable in social networking applications. Then $I_{SRM}$ is transformed from RGB color space to uncorrelated color space HSV, as in Eq. (2).

$$I_{SRM} = ImgScrm\,(I_{RGB},\ \mathrm{K}_{SK},\ \Psi) \tag{1}$$

$$I_{UCS} = RGB2HSV\,(I_{SRM}). \tag{2}$$

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

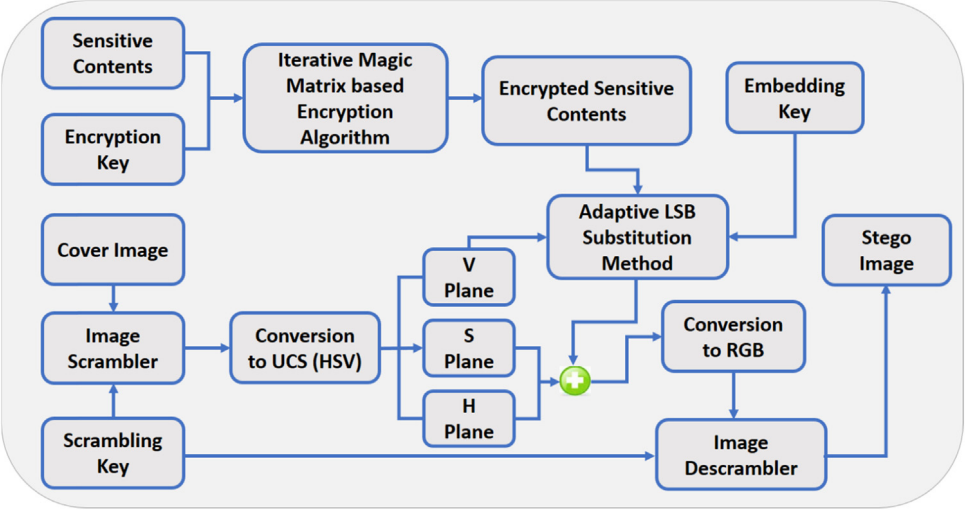


**Fig. 1.** Overview of the proposed framework.

**Table 1**
Description of symbols and parameters used in our work.

| Symbol/Parameter | Brief illustration |
|---|---|
| Input Image $I_{RGB}$ | Cover image, where sensitive contents are embedded |
| $I_{SRM}$ | Scrambled encrypted image, preserving the privacy of image contents |
| *ImgScrm* | Function for encrypting the input image prior to data hiding |
| $K_{SK}$ | Image scrambling key, making its decryption infeasible without it. |
| $\Psi$ | Number of iterations for encryption, controlling the encryption level |
| $I_{UCS}$ | Image in un-correlated color space |
| $H_{UCS}$ | Hue component of $I_{UCS}$ |
| $S_{UCS}$ | Saturation component of $I_{UCS}$ |
| $V_{UCS}$ | Intensity component (value) of $I_{UCS}$ |
| $S_{SC}$ | Sensitive contents, i.e., payload |
| IMMEA | Iterative magic matrix based encryption algorithm |
| $K_{EK}$ | Encryption key used in IMMEA |
| $\Phi$ | Number of iterations, controlling the encryption level of $S_{SC}$ |
| $S_{ESC}$ | Resultant cipher after encryption by IMMEA |
| $\ell$ | Magic matrix size, controlling security level, payload, and block size |
| $K_{EMK}$ | Embedding key for traversal and selection of blocks during data hiding |
| $V_{SUCS}$ | Stego $V_{UCS}$ after embedding process |
| $I_{ESRGB}$ | Encrypted stego image in RGB format |
| ImgDescrm | Function decrypting the encrypted stego image to its plain form |
| Stego Image $I_{FSRGB}$ | Final stego image in RGB with hidden encrypted sensitive contents |

There are several motivational factors validating the selection of HSV color space in the proposed framework for data hiding: (1) de-correlated color modal where changes to one channel do not affect other channels, (2) cost-effectiveness of UCS compared to RGB, and (3) better stego image quality after intentional data hiding as proved by experimental results tabulated in Table 2.

The resultant image from Eq. (2) is then divided into 3 sub-channels including $H_{UCS}$, $S_{UCS}$, and $V_{UCS}$ using Eq. (3) for hiding data into the intensity channel $V_{UCS}$. The sensitive contents $S_{SC}$ are encrypted according to the procedure mentioned in IMMEA, as in Eq. (4), prior to data hiding process to increase its security against attackers.

$$[H_{UCS},\ S_{UCS},\ V_{UCS}] = ChannelSeparator\ (I_{UCS}) \tag{3}$$

$$S_{ESC} = IMME\ (S_{SC},\ K_{EK},\ \Phi). \tag{4}$$

The encrypted sensitive contents $S_{ESC}$ are then embedded into the intensity plane $V_{UCS}$ using an adaptive LSB substitution method as illustrated in Eq. (5). As a result, the stego $V_{SUCS}$ plane is obtained, which is then combined with the rest of two planes ($H_{UCS}$ and $S_{UCS}$), constructing a stego image in uncorrelated color space $I_{SUCS}$. Next, the marked image $I_{SUCS}$ is converted back to RGB color space as depicted in Eq. (7). Finally, the encrypted marked image is descrambled into its original form using Eq. (8), generating the final stego image $I_S$.

$$V_{SUCS} = AdaptiveLSBEmbedding(S_{ESC},\ V_{UCS},\ \ell,\ K_{EMK}) \tag{5}$$

$$I_{SUCS} = StegoMaker\ (H_{UCS},\ S_{UCS},\ V_{SUCS}) \tag{6}$$

$$I_{ESRGB} = HSV2RGB\ (I_{SUCS}) \tag{7}$$

$$I_{FSRGB} = ImgDescrm\ (I_{SRGB},\ K_{SK},\ \Psi). \tag{8}$$

### 2.1. Image scrambler

In this sub-section, we discuss the process of image scrambling utilized in the proposed framework. The main goal of image scrambling is privacy preservation of the image contents [1], which is most desirable in social networking applications requiring privacy. To clarify the concept of image encryption in the proposed framework, we present it via mathematical equations. Consider the input grayscale image $I$ of dimension $m \times n$ having pixel value of bit-depth eight at each locations $(x, y)$, where $x = \{x_1, x_2, x_3, \ldots, x_m\}$ and $y = \{y_1, y_2, y_3, \ldots, y_n\}$ as in Eqs. (9)–(11).

$$I\ (x, y) = C_{x,y,0},\ C_{x,y,1},\ C_{x,y,2}, \ldots, C_{x,y,7} \tag{9}$$

$$C_{x,y,i} = \left[\frac{I(x, y)}{2^i}\right] \bmod 2, \quad i = 0,\ 1,\ 2,\ \ldots 7 \tag{10}$$

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

$$I(x,y) = \sum_{i=0}^{7} \left(2^i \times C_{x,y,i}\right). \quad (11)$$

Here, $i$ shows the plane number ranging from 0 to 7, $x$ and $y$ represent pixel indices of $I$ in the range $[1-m, 1-n]$, and $C$ denotes channel number, i.e., first LSB, second LSB up to MSB. To encrypt image $I$, we first generate 8 random matrices from $K_{SK}$ using Eq. (12) and then use Eqs. (13) and (14) for actual process of scrambling.

$$\Re^{(i)} = \left\{\Re^{(i)}_{x,y}\right\}_{m\times n} \quad i = 0,\ 1,\ 2,\ \ldots 7 \quad (12)$$

$$C'_{x,y,i} = C_{x,y,i} \quad i = 0,\ 1,\ 2,\ \ldots .7 \quad (13)$$

$$C'_{x,y,i} = C_{x,y,i} \oplus \Re^{(i)}_{x,y} \quad i = 0,\ 1,\ 2,\ \ldots 7. \quad (14)$$

Here, $\Re$ denotes random matrices used in image scrambling, $\oplus$ is XOR operation, and $C'_{x,y,i}$ is the scrambled form of $C_{x,y,i}$ for $i = 0, 1, 2, \ldots 7$. The scrambled image $I_{SRM}$ is obtained by merging all $C'_{x,y,i}$ as given in Eq. (15).

$$I_{SRM}(x,y) = \sum_{i=0}^{7} \left(2^i \times C'_{x,y,i}\right). \quad (15)$$

As RGB images are used in the proposed work, therefore, the process of scrambling is repeated for all the three channels including red, green, and blue. The intermediate encrypted channels are combined for getting the final scrambled image. The levels of encryption can be controlled by the number of iterations $\Psi$ by generating more random matrices from $K_{SK}$ and using them for further scrambling. This facilitates users to encrypt the image contents according to their requirements and type of the underlying application.

### 2.2. Iterative magic matrix based encryption algorithm

In this sub-section, we illustrate the process of encrypting the sensitive contents prior to embedding it into the cover image. The motivational reason for using IMMEA is to increase the security of embedded contents. Algorithm 1 illustrates the main steps of IMMEA:

**Algorithm 1.** Iterative Magic Matrix based Encryption Algorithm (IMMEA)

**Input**: Sensitive Contents $S_{SC}$ and Encryption Key $K_{EK}$

Set Cipher=" ", and determine window size $\omega$, and number of iterations $\Phi$

Permute $S_{SC}$ according to $\omega$ with concatenation of garbage characters to avoid overflow case

Set k=1

**While** (k<=$\Phi$), **do**

a. Generate a magic matric M of size $\omega$;
b. Temp ← Extract characters of size $\omega$ from $S_{SC}$;
c. Assign Temp's characters to M according to its indices;
d. Sub-cipher ← Raster order Scanning of M;
e. Cipher ← Concatenate(Cipher, sub-cipher);

**End**

**Output**: Encrypted Sensitive Contents $S_{ESC}$

### 2.3. Adaptive LSB substitution method

In this section, we describe the actual proposed data embedding mechanism. The embedding algorithm is mainly based on color model transformation and the block-wise adaptive LSB method, exploring the magic matrix. Incorporating the property of adaptability and block-wise magic LSB method improves the stego image quality and results in better security. The key steps of our proposed data hiding scheme are given in Algorithm 2.

**Algorithm 2.** Adaptive LSB Substitution Method

**Input**: Scrambled image $I_{SRM}$, Sensitive Contents $S_{ESC}$, and Embedding Key $K_{EMK}$

1. Determine block size $\ell$
2. Apply RGB2HSV transformation on $I_{SRM}$ for getting $I_{UCS}$
3. Separate $H_{UCS}$, $S_{UCS}$, and $V_{UCS}$ from $I_{UCS}$.
4. Permute the gray-levels of $V_{UCS}$ to avoid overflow condition
5. Select blocks of size $1\times\ell$ from $S_{ESC}$, according to $K_{EMK}$
6. Divide $V_{UCS}$ into non-overlapping blocks of size $\ell\times\ell$
7. Determine the scanning order of blocks according to $K_{EMK}$
8. Generate magic matrix $M$ of size $\ell\times\ell$ and assign $\ell^2$ pixels of a given block of $V_{UCS}$ to M
9. Set counter $(i) \leftarrow 1$ and block number $(j) \leftarrow 1$
10. **While** $\left(i \le Size\ of\ S_{ESC}\right)$, **do**
    a. Consider a block $B_j$ from $V_{UCS}$
    b. Apply reshape operations as follows:
        i. $B_j = reshape\left(B_j, \left[1, \ell^2\right]\right)$;
        ii. $M = reshape\left(M, \left[1, \ell^2\right]\right)$;
    c. **For** $k \leftarrow 1$ to $\ell^2$ **do**
        i. $P^{(t)} = Search(P_k, M)$, where $P^{(t)}$ is temporary pixel holder variable.
        ii. Perform $P^{(t)}(0) = S_{ESC}(i)$

    **End**
    d. Apply $B_j = reshape\left(B_j, [\ell, \ell]\right)$;
    e. $i \leftarrow i + \ell^2$ and $j \leftarrow j + 1$;

**End**

11. Reconstruct $I_{UCS}$ by combing $H_{UCS}$, $S_{UCS}$, and $V_{SUCS}$
12. Apply reverse transformation, i.e., HSV2RGB to get $I_{ESRGB}$.
13. Finally, de-scramble $I_{ESRGB}$ by *ImgDescrm* function for getting final stego-image $I_{FSRGB}$

**Output**: Final Stego Image $I_{FSRGB}$

## 3. Experimental results and discussion

This section presents a detailed overview of the experiments conducted to evaluate the performance of the proposed framework over other competing schemes. The overall performance of the proposed work is compared with six other methods such as classic LSB, LSBM [35], LSBMR [13], SCC method [37], simple HSI (SHSI) method [38], and HSI-MLSB [39] method. All the methods were simulated using MATLAB R2015a using globally accepted image datasets including COREL [40] and USC-SIPI-ID [41]. Some of the test images from the datasets and their corresponding marked versions for our proposed scheme are given in Fig. 2. In the coming

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

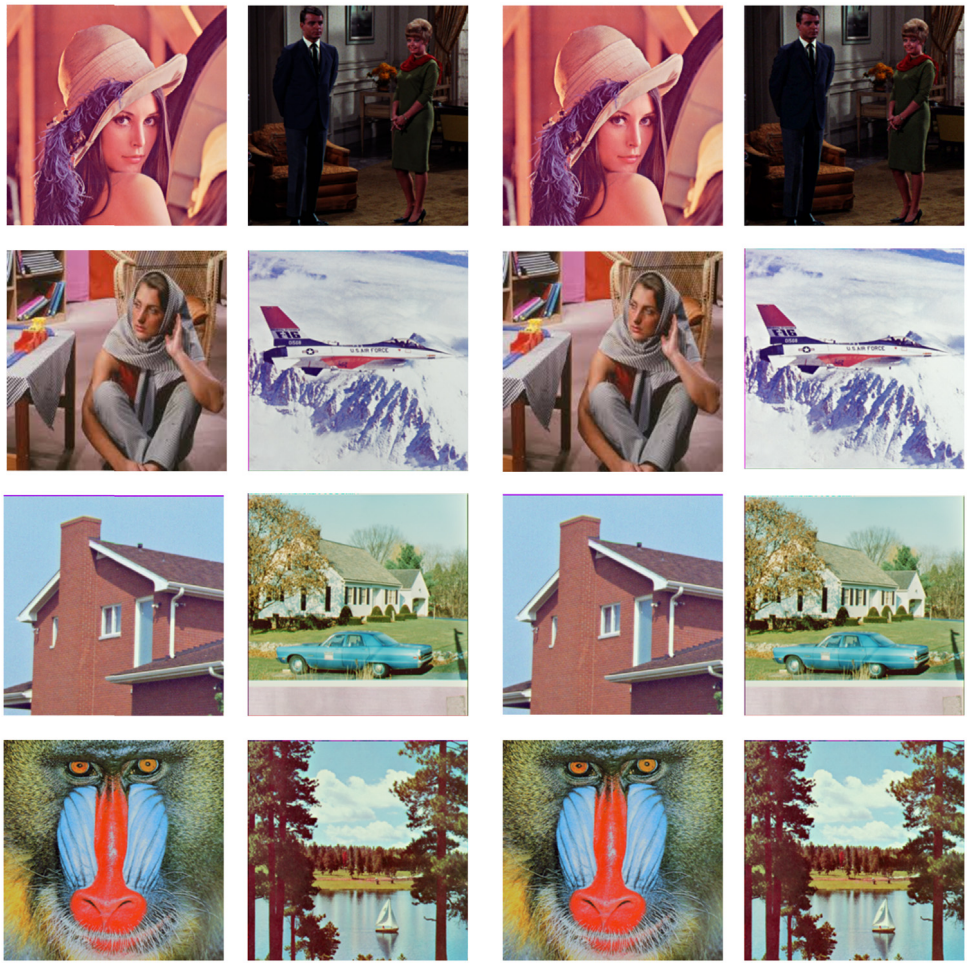

**Fig. 2.** Sample standard test images from the mentioned datasets and their corresponding stego images. First two columns are input cover images while 3rd and 4th column represent stego images of our proposed scheme.

sub-sections, the results of various experiments for performance evaluation are presented.

### 3.1. Objective evaluation

In objective evaluation, various image quality assessment metrics (IQAMs) are used to measure the image quality of the stego-images. These IQAMs include peak-signal-to-noise ratio (PSNR) [42], normalized-cross-correlation (NCC) [43], and structural similarity index metric (SSIM) [44,45], whose formulae are given in Eqs. (16)–(19) as follows:

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^2}{MSE}\right) \tag{16}$$

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_{x,y}^{C} - I_{x,y}^{S}\right)^2 \tag{17}$$

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_{x,y}^{C} \times I_{x,y}^{S}\right)}{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_{x,y}^{S}\right)^2} \tag{18}$$

$$SSIM\left(I_{x,y}^{C}, I_{x,y}^{S}\right) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}. \tag{19}$$

Here, $I^S$ and $I^C$ represent the stego and cover image respectively, $x$ and $y$ are counter variables, $M$ and $N$ are image dimensions, and the rest of the symbols are statistical parameters.

Table 2 illustrates one of the reasons for selecting HSV color space in the proposed work for data hiding. In this experiment, we embed a message of size 8192 bytes inside 50 standard images using the mentioned color spaces. The color channel enclosed in small parenthesis is used for data embedding. According to Table 2, Lab color space achieves the smallest execution time but its visual quality is very low and hence cannot be used for data hiding. HSI gives worse results in terms of execution time than other four color models, but its image quality is acceptable as compared to red and green channel of RGB, YCbCr, and Lab color space. The proposed UCS sustains a better trade-off between execution time and image quality compared to other models, hence validating its suitability for steganographic algorithms.

Table 3 presents PSNR scores that are computed over 50 images by hiding a message of 8192 bytes inside each image using the proposed scheme and other techniques. The last line shows the average value of PSNR in bold font for 50 images. Our proposed framework achieves comparatively better results due to utilization of UCS and adaptive block-wise magic LSB substitution method as evident from Table 3. The proposed scheme maintains the image quality, thus it is more suitable for transmission of secret data over the Internet compared to other competing algorithms.

For further evaluation, we used NCC which is another well-known IQAM. Fig. 3 illustrates the performance of all mentioned methods using this metric over 50 images, where LSB, SHSI,

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

**Table 2**
Selection of UCS (HSV) [46]: Performance evaluation of different color models using an evaluation criteria consisting of PSNR and execution time for data hiding. The channel enclosed in small parenthesis in each color space is utilized for data hiding.

| 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 (s) for 50 images | 49.73 | 49.3292 | 49.2898 | 51.541 | 49.6435 | 13.761 | **49.2669** |
| Execution time per image (s) | 0.9946 | 0.9865 | 0.9857 | 1.030 | 0.9928 | 0.2752 | **0.9853** |

**Table 3**
Quantitative evaluation based on PSNR with correlated and un-correlated color spaces-based steganographic methods.

| Serial# | Image Name | LSB Method | LSBM [35] | LSBMR [13] | SCC [37] method | SHSI [38] | HSI-MLSB [39] | Proposed method |
|---|---|---|---|---|---|---|---|---|
| 1 | Lena | 42.5103 | 42.6173 | 42.5971 | 42.6036 | 42.1875 | 42.214 | 56.104 |
| 2 | Couple | 48.4091 | 43.2019 | 45.8306 | 47.9157 | 51.0492 | 49.7614 | 56.4489 |
| 3 | Army | 49.2427 | 50.3571 | 50.3192 | 49.8409 | 49.149 | 48.5179 | 55.2188 |
| 4 | Lena2 | 56.7667 | 53.5104 | 53.2572 | 49.073 | 52.8284 | 52.5173 | 56.1829 |
| 5 | Barbara | 46.0426 | 40.748 | 43.9976 | 43.8513 | 44.5126 | 44.4109 | 45.2446 |
| 6 | Competition | 45.2381 | 42.6036 | 42.3511 | 42.4127 | 43.5592 | 43.6609 | 44.5183 |
| 7 | Hackers | 41.9787 | 40.909 | 51.0121 | 41.4136 | 42.4669 | 42.3954 | 42.8749 |
| 8 | Design1 | 45.9782 | 42.6711 | 43.1503 | 46.1499 | 46.4898 | 46.4094 | 48.0227 |
| 9 | Design2 | 38.1099 | 33.4232 | 32.6252 | 37.7652 | 42.7385 | 42.5088 | 43.2604 |
| 10 | Scene1 | 49.5272 | 52.3261 | 53.3866 | 45.1944 | 47.6945 | 48.152 | 49.1024 |
| 11 | Scene2 | 50.7739 | 45.2771 | 46.6156 | 46.8765 | 49.4624 | 49.3679 | 50.3792 |
| 12 | Scene3 | 41.7376 | 42.1569 | 42.1765 | 41.9445 | 41.3416 | 41.3613 | 49.5546 |
| 13 | Scene4 | 25.2958 | 25.3776 | 25.3734 | 25.2925 | 25.3228 | 25.317 | 49.5974 |
| 14 | Flowers | 44.1484 | 40.1295 | 42.8967 | 42.0494 | 44.5818 | 44.721 | 46.3738 |
| 15 | Waterfall1 | 42.7883 | 39.0204 | 48.9587 | 40.353 | 42.3375 | 42.0763 | 43.1932 |
| 16 | Waterfall2 | 46.8229 | 41.2205 | 43.8929 | 45.7811 | 45.7153 | 45.742 | 46.8528 |
| 17 | Baboon2 | 43.3026 | 43.2116 | 43.067 | 42.234 | 43.0028 | 43.2208 | 44.729 |
| 18 | Baboon3 | 41.2222 | 38.0864 | 38.9495 | 39.0511 | 42.2517 | 42.1089 | 43.0718 |
| 19 | Trees1 | 56.6622 | 44.83 | 47.85 | 33.8345 | 53.5754 | 53.2381 | 56.0393 |
| 20 | Trees2 | 40.7337 | 50.8053 | 51.2332 | 38.6249 | 41.5838 | 41.5271 | 43.1448 |
| **Avg. of 50 images** | | **49.1984** | **48.9746** | **50.1746** | **45.2191** | **50.4034** | **50.3888** | **52.4555** |

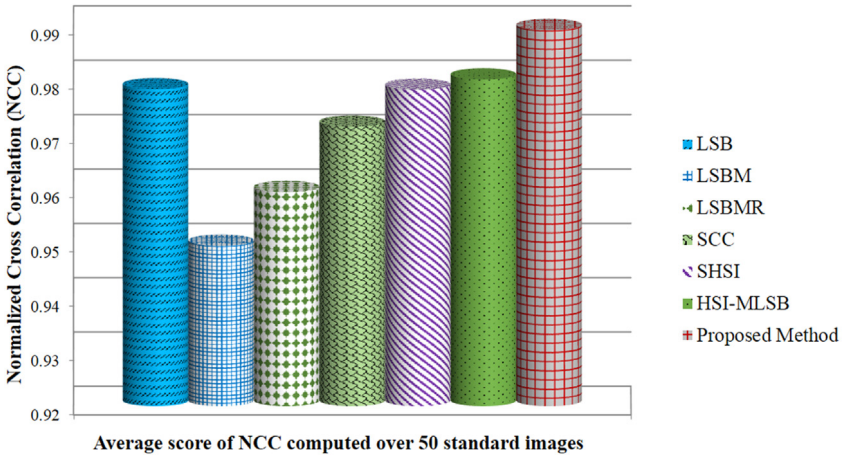


**Fig. 3.** NCC based quantitative evaluation.

and HSI-MLSB method achieve almost the same scores. LSBM technique gives worse results in this experiment. The proposed scheme dominates the remaining six methods by achieving the highest NCC score, hence confirming its better performance.

It is infeasible for PSNR and NCC sometimes to capture the structural information distorted completely by intentional data concealing. Therefore, a human-perception oriented metric SSIM is additionally considered for image quality assessment. The SSIM based statistics for our algorithm and other methods are given in Fig. 4, clarifying that the proposed method results in a higher SSIM score compared to other schemes, hence providing better image quality.

In the aforementioned experiments, the size of sensitive contents is same, i.e., 8192 bytes. Therefore, here we evaluate the proposed framework by embedding a variable amount of sensitive contents, so that the performance can be fully filtered. Fig. 5 illustrates the performance of our scheme along with other six techniques based on PSNR for twenty selected images. The circle nearer to the center shows low performance, while the one away from center represents better performance. Hence, it is clear from Fig. 5 that the proposed method achieves better performance in terms of PSNR compared to other schemes.

To further evaluate the performance, we conducted another experiment by changing the image dimension for each method. A message of the size of 8192 bytes was hidden in various images of different dimensions in this experiment. Fig. 6 illustrates the performance of the proposed approach from another perspective using PSNR over 50 images. Our proposed scheme achieves a higher PSNR score in this experiment also. This validates its better performance against other state-of-the-art methods.

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

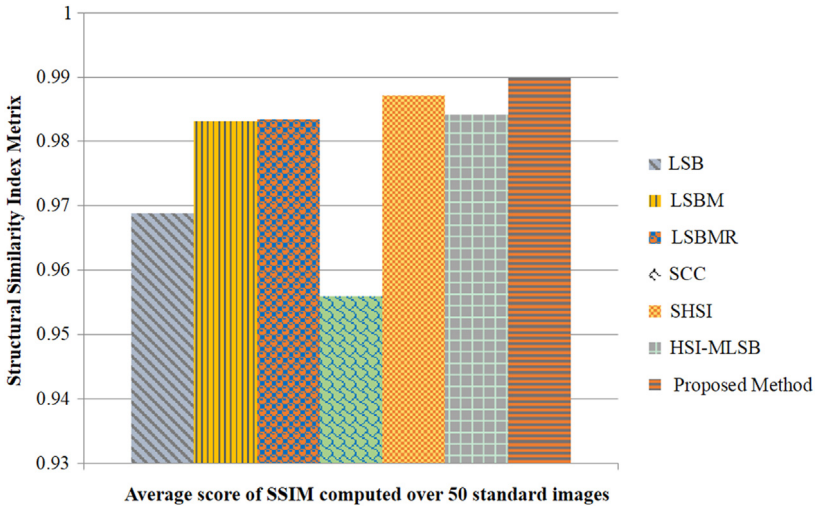


**Fig. 4.** Quantitative evaluation based on SSIM.

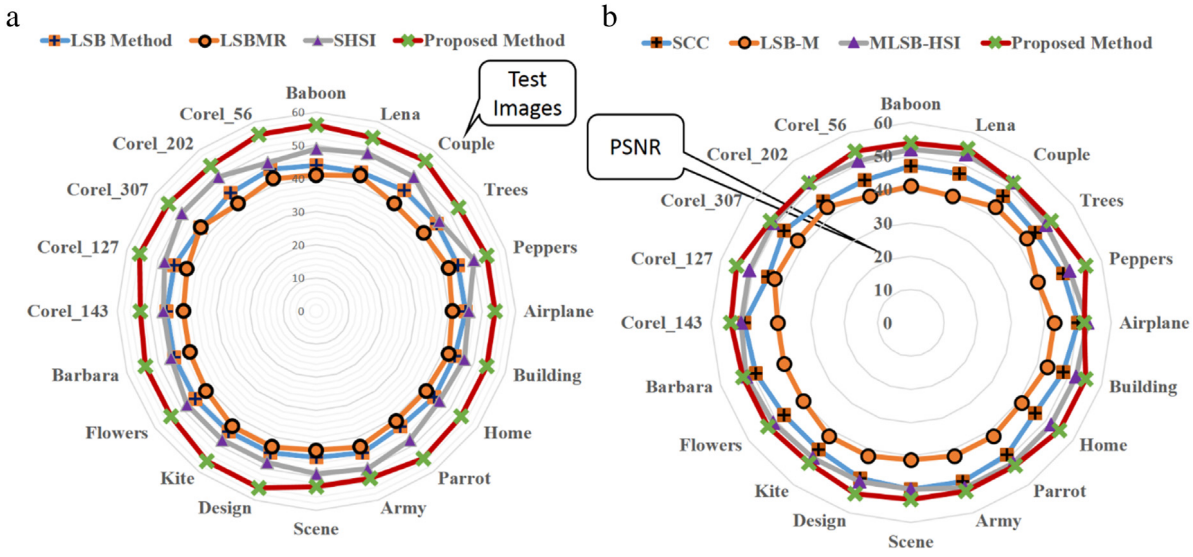


**Fig. 5.** Quantitative evaluation using PSNR with variable amount of sensitive contents (a) results for 20 images with sensitive contents size = 6144 bytes (b) PSNR based results with data size = 8192 bytes for 20 images, selected from the dataset.

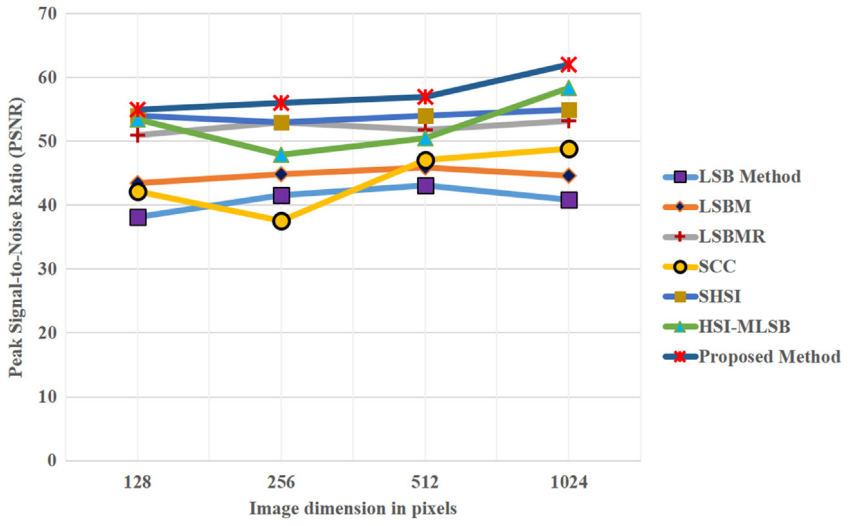


**Fig. 6.** PSNR based evaluation with equal size sensitive contents and varying image dimensions.

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

**Table 4**
Subjective evaluation based on MOS score.

| Image name | LSB method | LSBM | LSBMR | SCC | SHSI | MLSB-HSI | Proposed method |
|---|---|---|---|---|---|---|---|
| Lena | 3.6 | 3.4 | 3.7 | 3.5 | 3.9 | 4.3 | 4.4 |
| Baboon | 3.7 | 3.5 | 3.8 | 3.6 | 3.6 | 4.0 | 4.5 |
| Airplane | 4.0 | 3.9 | 3.7 | 3.7 | 4.0 | 4.3 | 4.6 |
| Home | 3.6 | 3.4 | 3.7 | 3.5 | 3.8 | 4.0 | 4.2 |
| Couple | 4.1 | 3.5 | 3.4 | 3.3 | 4.1 | 4.2 | 4.3 |
| Barbara | 3.5 | 3.6 | 3.5 | 3.2 | 3.7 | 3.7 | 3.9 |
| Peppers | 3.3 | 3.4 | 3.6 | 3.4 | 3.6 | 3.6 | 4.1 |
| Trees | 3.1 | 3.1 | 3.2 | 3.2 | 3.4 | 3.8 | 4 |
| Army | 3.9 | 3.5 | 3.6 | 3.5 | 3.7 | 3.9 | 4.2 |
| Scene | 3.7 | 3.3 | 3.5 | 3.4 | 3.8 | 4.2 | 4.5 |
| **Average of 10 images** | **3.65** | **3.46** | **3.57** | **3.43** | **3.76** | **4.0** | **4.27** |

### 3.2. Subjective evaluation

In this sub-section, our proposed system is compared with six other state-of-the-art methods using subjective evaluation, which is one of the primarily required approach for stego quality assessment. Mean opinion score (MOS) was used as subjective evaluation metric in this strategy as used by [43,47] for quality assessment. To collect the MOS scores, a total of 10 persons were requested for rating stego image quality, produced by our method and other techniques. The range for rating was kept 0 (poor quality)–5 (high quality). The quality evaluators team consists of five male and five female students (Ph.D. and Post-doc fellows), who are working in different laboratories of digital contents in the vicinity of our laboratory and university. The students were trained for one hour about the domain knowledge of security and strategy of quality assessment. The students were then given ten standard cover images from the dataset and their corresponding stego images produced by our proposed scheme and other methods. The averaged rated MOS scores given by ten students are tabulated in Table 4. The last line of Table 4 shows the average MOS score computed over 10 standard test images. The collected results indicate that the our scheme achieves the highest MOS score by the expert image quality evaluators compared to other schemes. This minimizes the detectability chances of HVS, leading to better preservation of embedded data against attackers, hence making the proposed framework more feasible for security of visual contents in OSNs.

### 3.3. Security analysis

Analyzing the security level and sturdiness of a newly developed steganographic method is one of the major concerns in this area. Therefore, we evaluate the security strength of our scheme in terms of time complexity based on Kirchhoff's principle [48]. According to this principle, an attacker knows about the data hiding algorithm and the security of the system lies in secret key [19]. This assumption makes secret key selection more crucial for the security of a communication system. Considering this concern, we incorporated three different secret keys in our proposed framework for sensitive contents encryption, data hiding, and image scrambling. Each key is 64 bit long, the combination of which results in a master key of 192 bits, making the key space long enough to resilient against brute-force attack. The detailed illustration for calculating the time required for breaking the secret key only is given below:

Master key length $= 192$ bits

Total number of possible keys $= 2^{192}$

Suppose the attacker generates $10^9$ keys in one second, the required amount of time is calculated as follows:

$$\text{Years required for secret key breakage} = \frac{2^{192}}{10^9 \times 365 \times 86400} = 1.9905 \times 10^{41}$$

$$\text{Number of years in average} = 9.9523 \times 10^{40}.$$

It can be confirmed from the above analysis that the proposed system provides sufficient security to be resilient against a brute-force attack without using any complex algorithms, hence increasing its suitability for various potential security applications.

## 4. Application of the proposed framework for security of visual contents in online social networks

In this section, we illustrate one of the potential applications of our proposed framework in addressing the security of visual contents in online social networks. Due to advancement in modern technology and smartphones, online social networks such as Facebook, Twitter, and Myspace are widely used by individuals of almost all ages for sharing of images as well as messages, concerning their life-moments and events. Currently, there are no strict restrictions on these social websites by copyright organizations, resulting in security risks and authenticity of visual contents being uploaded to these OSNs [49–51]. For example, the private and semantically relevant images uploaded by any individual on his timeline for some special purpose can be easily modified by adversaries, leading to privacy leakage of the concerned user. Therefore, addressing the privacy issues in OSNs remains a big challenge. In this context, the cryptographic techniques [52] can be applied but such schemes transforms the appearance of visual contents into scrambled form. This makes the visual contents suspicious enough to attract the attackers' attention, leading to modification or decryption of visual contents, hence compromising the privacy of OSN users. To tackle this problem, the proposed steganography-assisted framework can be used, which seems the best choice for visual contents' authenticity in OSNs. In the proposed model, the login information of actual owner, date, and time, and other secret parameters can be embedded as a secret message inside the uploaded picture. A sample scenario of the proposed suggested application for privacy preservation in OSNs is shown in Fig. 7.

In this scenario, the visual contents on a given timeline in OSN can be checked for authenticity by extracting the embedded information. If the extracted information is same as embedded information, then the corresponding visual contents are not modified by attackers, otherwise modified. The suggested application has numerous advantages to OSNs such as (1) privacy preservation of users, (2) visual contents authenticity, (3) secure chat messaging along with sharing of important life moments between friends and family members, and (4) top-secret research discussion on sensitive topics.

## 5. Conclusion and future work

In this paper, the problem of secure sensitive contents transmission using uncorrelated color space based steganography

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

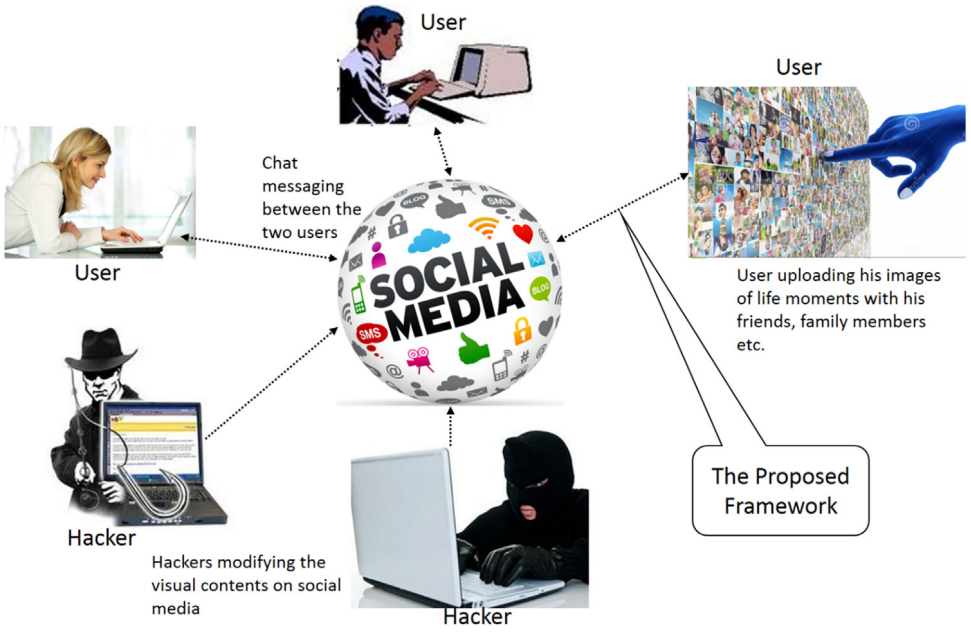


**Fig. 7.** Authenticity of visual contents on OSNs using the proposed method.

has been addressed. The idea of UCS has been inspired from its characteristics of efficiency in processing, de-correlation, better stego-image quality, and suitability for steganography as verified by various experiments. Most of the existing methods have used correlated color space such as RGB in which minor modification to one channel affects the image quality, producing low-quality stego-images and thereby decreasing their suitability for data hiding algorithms. Therefore, in this paper we surmount this problem by using an imperceptible adaptive LSB substitution framework based on UCS. We also introduce an image scrambler for the preservation of image contents and an encryption algorithm (IMMEA) for the encoding of sensitive contents prior to data hiding. Furthermore, the incorporation of the secret key-directed block magic LSB method adaptively embeds secret data inside the scrambled image, resulting in better security and visual quality. Finally, an application of the proposed framework is suggested in addressing the security of visual contents in OSNs. We conclude that HSV is the best choice for steganography compared to RGB, HSI, Lab, and YCbCr color models and its suggested application with image steganography technology can help OSNs in ensuring the privacy of users and authenticity of visual contents.

Despite of the better performance of our method compared to other techniques, there is a limitation of resiliency against different attacks such as compression, cropping, and noising. Our proposed method as well as all other steganographic methods of spatial domain face this problem. In the future, we intend to work on the practical implementation of the suggested application in real OSNs in combination with image hashing technology. We also plan to explore different image analysis [53] and segmentation methods [54] combined with visual attention modeling and sparse coding for further improvement in terms of payload as well as secure personalized retrieval [55] for different applications [56]. Another possible direction is to combine the proposed scheme with sleep stage classification methods [57] for secure sleep monitoring in sensitive departments such as intelligence and atomic plants.

## Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2016R1A2B4011712).

## References

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: Survey and analysis of current methods, Signal Process. 90 (2010) 727–752.
[2] L. Bin, W. Ming, L. Xiaolong, T. Shunquan, H. Jiwu, A strategy of clustering modification directions in spatial image steganography, IEEE Trans. Inf. Forensics Secur. 10 (2015) 1905–1917.
[3] L. Bin, T. Shunquan, W. Ming, H. Jiwu, Investigation on cost assignment in spatial image steganography, IEEE Trans. Inf. Forensics Secur. 9 (2014) 1264–1277.
[4] G. Linjie, N. Jiangqun, S. Yun Qing, Uniform embedding for efficient JPEG steganography, IEEE Trans. Inf. Forensics Secur. 9 (2014) 814–825.
[5] W. Mazurczyk, L. Caviglione, Steganography in modern smartphones and mitigation techniques, IEEE Commun. Surv. Tutor. 17 (2014) 334–357.
[6] Z. Liu, F. Zhang, J. Wang, H. Wang, J. Huang, Authentication and recovery algorithm for speech signal based on digital watermarking, Signal Process. 123 (2015) 157–166.
[7] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Trans. Inf. Forensics Secur. 10 (2015) 507–518.
[8] A. Khan, A. Siddiqa, S. Munib, S.A. Malik, A recent survey of reversible watermarking techniques, Inform. Sci. 279 (2014) 251–272.
[9] A. Anees, A.M. Siddiqui, J. Ahmed, I. Hussain, A technique for digital steganography using chaotic maps, Nonlinear Dynam. 75 (2014) 807–816.
[10] K. Qazanfari, R. Safabakhsh, A new steganography method which preserves histogram: Generalization of LSB⟨sup⟩ + +⟨sup⟩, Inform. Sci. 277 (2014) 90–101.
[11] C.-H. Yang, C.-Y. Weng, S.-J. Wang, H.-M. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems, IEEE Trans. Inf. Forensics Secur. 3 (2008) 488–497.
[12] W. Zhang, X. Zhang, S. Wang, A double layered "plus-minus one" data embedding scheme, IEEE Signal Process. Lett. 14 (2007) 848–851.
[13] J. Mielikainen, LSB matching revisited, IEEE Signal Process. Lett. 13 (2006) 285–287.
[14] Z. Xia, X. Wang, X. Sun, Q. Liu, N. Xiong, Steganalysis of LSB matching using differences between nonadjacent pixels, Multimedia Tools Appl. 75 (2016) 1947–1962.
[15] K. Muhammad, J. Ahmad, N.U. Rehman, Z. Jan, M. Sajjad, CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method, Multimedia Tools Appl. (2016) 1–30. http://dx.doi.org/10.1007/s11042-016-3383-5.
[16] M. Fakhredanesh, M. Rahmati, R. Safabakhsh, Adaptive image steganography using contourlet transform, J. Electron. Imaging 22 (4) (2013) 043007–043007.
[17] S. Ahani, S. Ghaemmaghami, Colour image steganography method based on sparse representation, IET Image Process. 9 (2015) 496–505.
[18] M. Ali, C.W. Ahn, M. Pant, P. Siarry, An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony, Inform. Sci. 301 (2015) 44–60.
[19] S.A. Parah, J.A. Sheikh, A.M. Hafiz, G. Bhat, Data hiding in scrambled images: a new double layer security data hiding technique, Comput. Electr. Eng. 40 (2014) 70–82.
[20] M. Sajjad, K. Muhammad, S.W. Baik, S. Rho, Z. Jan, S.-S. Yeo, et al., Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices, Multimedia Tools Appl. (2016) 1–18. http://dx.doi.org/10.1007/s11042-016-3811-6.
[21] I. Mehmood, M. Sajjad, S.W. Baik, Mobile-cloud assisted video summarization framework for efficient management of remote sensing data generated by wireless capsule sensors, Sensors 14 (2014) 17112–17145.

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029

[22] X. Li, B. Yang, D. Cheng, T. Zeng, A generalization of LSB matching, IEEE Signal Process. Lett. 16 (2009) 69–72.
[23] L. Weiqi, H. Fangjun, H. Jiwu, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forensics Secur. 5 (2010) 201–214.
[24] H.R. Kanan, B. Nazeri, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, Expert Syst. Appl. 41 (2014) 6123–6130.
[25] A. Ioannidou, S.T. Halkidis, G. Stephanides, A novel technique for image steganography based on a high payload method and edge detection, Expert Syst. Appl. 39 (2012) 11517–11524.
[26] W.-J. Chen, C.-C. Chang, T.H.N. Le, High payload steganography mechanism using hybrid edge detector, Expert Syst. Appl. 37 (2010) 3292–3301.
[27] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, S.W. Baik, A secure method for color image steganography using gray-level modification and multi-level encryption, KSII Trans. Internet Inf. Syst. 9 (2015) 1938–1962.
[28] R.-Z. Wang, C.-F. Lin, J.-C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognit. 34 (2001) 671–683.
[29] C.-C. Chang, J.-Y. Hsiao, C.-S. Chan, Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy, Pattern Recognit. 36 (2003) 1583–1595.
[30] C.-C. Thien, J.-C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognit. 36 (2003) 2875–2881.
[31] D.-C. Lou, J.-L. Liu, Steganographic method for secure communications, Comput. Secur. 21 (2002) 449–460.
[32] C.-C. Lin, W.-H. Tsai, Secret image sharing with steganography and authentication, J. Syst. Softw. 73 (2004) 405–414.
[33] C.-K. Chan, L.-M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognit. 37 (2004) 469–474.
[34] H.-C. Wu, N.-I. Wu, C.-S. Tsai, M.-S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proc., Vis. Image Signal Process. 152 (2005) 611–615.
[35] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forensics Secur. 5 (2010) 201–214.
[36] S. Dumitrescu, X. Wu, Z. Wang, Detection of LSB steganography via sample pair analysis, IEEE Trans. Signal Process. 51 (2003) 1995–2007.
[37] K. Bailey, K. Curran, An evaluation of image based steganography methods, Multimedia Tools Appl. 30 (2006) 55–88.
[38] K. Muhammad, J. Ahmad, H. Farman, M. Zubair, A novel image steganographic approach for hiding text in color images using HSI color model, Middle-East J. Sci. Res. 22 (2014) 647–654.
[39] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S.W. Baik, A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image, Multimedia Tools Appl. 75 (2016) 14867–14893.
[40] J. Laaksonen, M. Koskela, S. Laakso, E. Oja, PicSOM–content-based image retrieval with self-organizing maps, Pattern Recognit. Lett. 21 (2000) 1199–1207.
[41] W.-C. Cheng, M. Pedram, Chromatic encoding: a low power encoding technique for digital visual interface, IEEE Trans. Consum. Electron. 50 (2004) 320–328.
[42] R.J. Mstafa, K.M. Elleithy, A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes, Multimedia Tools Appl. (2015) 1–23.
[43] M. Sajjad, I. Mehmood, S.W. Baik, Sparse representations-based super-resolution of key-frames extracted from frames-sequences generated by a visual sensor network, Sensors 14 (2014) 3652–3674.
[44] J. Yang, Y. Lin, Z. Gao, Z. Lv, W. Wei, H. Song, Quality index for stereoscopic images by separately evaluating adding and subtracting, PloS One 10 (2015) e0145800.
[45] K. Muhammad, M. Sajjad, S.W. Baik, Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy, J. Med. Syst. 40 (2016) 1–16.
[46] K. Muhammad, J. Ahmad, M. Sajjad, S. Rho, S.W. Baik, Evaluating the suitability of color spaces for image steganography and its application in wireless capsule endoscopy, in: 2016 International Conference on Platform Technology and Service (PlatCon), 2016, pp. 1-3.
[47] N. Ejaz, I. Mehmood, S.W. Baik, Efficient visual attention based framework for extracting key frames from videos, Signal Process., Image Commun. 28 (2013) 34–44.
[48] F. Cayre, P. Bas, Kerckhoffs-based embedding security classes for woa data hiding, IEEE Trans. Inf. Forensics Secur. 3 (2008) 1–15.
[49] C. Zhang, J. Sun, X. Zhu, Y. Fang, Privacy and security for online social networks: challenges and opportunities, IEEE Netw. 24 (2010) 13–18.
[50] Z. Yan, W. Feng, P. Wang, Anonymous authentication for trustworthy pervasive social networking, IEEE Trans. Comput. Soc. Syst. 2 (2015) 88–98.
[51] Y. Zheng, W. Chen-zi, F. Wei, W. Zi-long, Survey of trustworthy pervasive social networking, Chin, J. Network Inf. Secur. 2 (2016) 30–40.
[52] R. Hamza, F. Titouna, A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map, Inf. Secur. J. (2016) 1–18.
[53] B. Chen, H. Shu, G. Coatrieux, G. Chen, X. Sun, J.L. Coatrieux, Color image analysis by quaternion-type moments, J. Math. Imaging Vis. 51 (2015) 124–144.
[54] Y. Zheng, B. Jeon, D. Xu, Q. Wu, H. Zhang, Image segmentation by generalized hierarchical fuzzy C-means algorithm, J. Intell. Fuzzy Systems 28 (2015) 961–973.
[55] K. Muhammad, I. Mehmood, M.Y. Lee, S.M. Ji, S.W. Baik, Ontology-based secure retrieval of semantically significant visual contents, J. Korean Inst. Next Gener. Comput. 11 (2015) 87–96.
[56] K. Muhammad, J. Ahmad, M. Sajjad, S.W. Baik, Visual saliency models for summarization of diagnostic hysteroscopy videos in healthcare systems, SpringerPlus 5 (2016) 1495.
[57] S.M. Isa, A. Noviyanto, W. Jatmiko, A.M. Arymurthy, The effect of electrocardiogram signal compression using beat reordering and SPIHT on automatic sleep stage classification, Procedia Eng. 41 (2012) 888–896.

**Khan Muhammad** received his B.C.S. degree in computer science from Islamia College, Peshawar, Pakistan with research in information security. Currently, he is pursuing MS leading to Ph.D. degree in digitals contents from College of Electronics and Information Engineering, Sejong University, Seoul, Republic of Korea. He is working as a researcher at Intelligent Media Laboratory (IM Lab) since 2015 under the supervision of Prof. Sung Wook Baik. His research interests include image and video processing, data hiding, image and video steganography, video summarization, diagnostic hysteroscopy, wireless capsule endoscopy, and CCTV video analysis. He has published 15+ papers in peer-reviewed international journals and conferences such as Journal of Medical Systems, Biomedical Signal Processing and Control, IEEE Access, Multimedia Tools and Applications, SpringerPlus, KSII Transactions on Internet and Information Systems, Journal of Korean Institute of Next Generation Computing, NED University Journal of Research, Technical Journal, Sindh University Research Journal, Middle-East Journal of Scientific Research, MITA 2015, PlatCon 2016, and FIT 2016. He is a student member of the IEEE.

**Muhammad Sajjad** received his Master degree from Department of Computer Science, College of Signals, National University of Sciences and Technology, Rawalpindi, Pakistan. He received his Ph.D. degree in Digital Contents from Sejong University, Seoul, Republic of Korea. He is now working as an assistant professor at Department of Computer Science, Islamia College Peshawar, Pakistan. He is also head of "Digital Image Processing Laboratory (DIP Lab)" at Islamia College Peshawar, Pakistan. His research interests include digital image super-resolution and reconstruction, medical image analysis, video summarization and prioritization, image/video quality assessment, and image/video retrieval.

**Irfan Mehmood** received his B.S. degree in Computer Science from National University of Computer and Emerging Sciences, Pakistan. He completed Ph.D. degree from Sejong University, Seoul, Korea. Dr. Irfan is Assistant Professor in College of Electronics and Information Engineering at Sejong University, Seoul South Korea. His research interests include video and medical image processing, big data analysis, and visual information summarization.

**Seungmin Rho** is a faculty of Department of Media Software at Sungkyul University in Korea. In 2012, he was an assistant professor at Division of Information and Communication in Baekseok University. In 2009–2011, he had been working as a Research Professor at School of Electrical Engineering in Korea University. In 2008–2009, he was a Postdoctoral Research Fellow at the Computer Music Lab of the School of Computer Science in Carnegie Mellon University. He gained his B.S degree in Computer Science from Ajou University. He received his MS and Ph.D. degrees in Information and Communication Technology from the Graduate School of Information and Communication at Ajou University, South Korea. He visited Multimedia Systems and Networking Lab in University of Texas at Dallas from Dec. 2003 to March 2004. Before he joined the Computer Sciences Department of Ajou University, he spent two years in industry. His current research interests include database, big data analysis, music retrieval, multimedia systems, machine learning, knowledge management as well as computational intelligence.

**Sung Wook Baik** received the B.S degree in computer science from Seoul National University, Seoul, Korea, in 1987, the M.S. degree in computer science from Northern Illinois University, Dekalb, in 1992, and the Ph.D. degree in information technology engineering from George Mason University, Fairfax, VA, in 1999. He worked at Datamat Systems Research Inc. as a senior scientist of the Intelligent Systems Group from 1997 to 2002. In 2002, he joined the faculty of the College of Electronics and Information Engineering, Sejong University, Seoul, Korea, where he is currently a Full Professor and Dean of Digital Contents. He is also the head of Intelligent Media Laboratory (IM Lab) at Sejong University. His research interests include computer vision, multimedia, pattern recognition, machine learning, data mining, virtual reality, and computer games. He is a member of the IEEE.

Please cite this article in press as: K. Muhammad, et al., Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.029