Automatic region selection method to enhance image-based steganography

Sinan A. Naji [1], Hatem N. Mohaisen[2], Qusay S. Alsaffar[2], Hamid A. Jalab[3]

[1] Department of Postgraduate Studies, University of Information Technology and Communications
[2] Ministry of Higher Education and Scientific Research
[3] Faculty of Computer Science and Information Technology, University of Malaya

ABSTRACT

Image-based steganography is an essential procedure with several practical applications related to information security, user authentication, copyright protection, etc. However, most existing image-based steganographic techniques assume that the pixels that hide the data can be chosen freely, such as random pixel selection, without considering the contents of the input image. So, the "region of interest" such as human faces in the input image might have defected after data hiding even at a low inserting rate, and this will reduce the visual quality especially for the photos containing several human faces. With this view, we proposed a novel approach that combines human skin-color detection along with the LSB approach which can choose the embedding regions. The idea behind that is based on the fact that the Human Vision System HVS tends to focus its attention on selectively certain structures of the visual scene instead of the whole image. Practically, human skin-color is good evidence of the existence of human targets in images. To the best of our knowledge, this is the first attempt that employs skin detection in application to steganography which considers the contents of the input image and consequently can choose the embedding regions. Moreover, an enhanced RSA algorithm and Elliptic Curve Equation are used to offer a double level of security. In addition, the system embeds noise bits into the resulting stego-image to make the attacker's task more confusing. Two datasets are used for testing and evaluation. The proposed scheme achieves minimum visual defects with double level of security.

Keywords: Skin Detection, Steganography, Cryptography, RSA, LSB.

Corresponding Author:

Sinan A. Naji
Department of Postgraduate Studies,
University of Information Technology and Communications,
Baghdad, Iraq
E-mail: dr.sinannaji@uoitc.edu.iq

1. Introduction

Steganography is an ancient practice for hiding secret information in an innocent-looking carrier medium [1-3]. Steganography plays a crucial role in numerous information security systems with a wide-ranging of applications such as communications, databases, user authentication, and copyright protection [4, 5]. Many different digital mediums are utilized by various steganographic approaches [5, 6]. These may include images, video-clips, text and audio files, drawings, art works, and so on.

Nowadays, we are producing a massive amount of images. A noteworthy factor has certainly been the social media sites that provide the media hundreds of thousands of images every moment [7, 8]. When using an image as a cover medium, certain pixel values are substituted with the stream values of the text message which we want to hide [9] [10]. Subsequently, the resulting image is known as stego-image. It is very hard for ordinary people to notice the insignificant change in pixel intensities because the amount of the modification is so minor [11]. Practically, several challenges are related to steganography techniques that should be measured when building a confident system. These may include: robustness against statistical attacks, imperceptibility (i.e., the visual appearance of the stego-image is highly alike to the original image), the amount of secret data that can be hidden in the cover media (i.e., payload), and computational complexity [9] [12]. When building an image-based steganography system, the researcher usually faces three main issues. First, what domain to choose (i.e., spatial or frequency), second, what will be the method for hiding the secret data, and finally, where exactly the data should be hidden. This paper covers the third question with the ultimate goal to minimize the visual defects in the resulting stego-image.

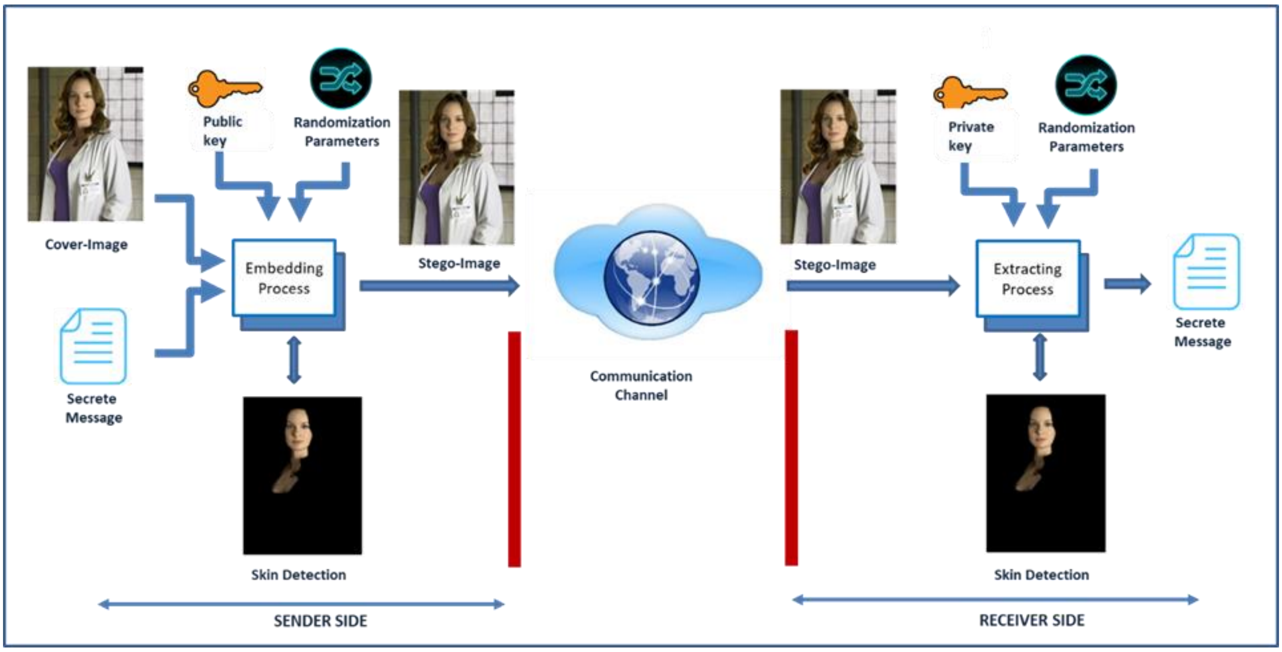

Figure 1. The outline of the overall design scheme

Unfortunately, most existing image-based steganographic techniques assume that the pixels that hide the data can be selected freely such as consecutive path pixels, zigzag path pixels, edge pixels, random pixel selection, etc. Nevertheless, this assumption is not always true, particularly when dealing with images containing human targets (e.g., selfie images). Based on extensive experiments, we found that the human body is considered as a "region of interest" to the Human Vision System (HVS). On the other hand, our HVS is less sensitive to changes in the background region and it can tolerate more changes (e.g., furniture, buildings, trees, and other noise-like regions). So, hiding secret data in "regions of interest" such as human faces can lead to serious defects. In other words, these regions cannot be used for hiding information. The important issue is how to locate "embedding regions" in a cover-image correctly.

The main contribution of this paper, supposedly, this is the first endeavor that utilizes the color feature of the human skin in the application to steganography which can choose the "embedding regions". Practically, skin color is good evidence of the existence of human targets in images [13] [14]. By locating the human targets in images, an improved Least Significant Bit (LSB) algorithm is used to hide information in such a way that keeps the human targets intact while secret information is embedded in noise-like regions directly. In addition, an enhanced RSA cryptography, Elliptic Curve Equation (ECE), and adding noise algorithms are also used together in one integrated system to provide an extra level of security. The outline of the overall design scheme of the proposed system is shown in Figure 1. The detailed description of each step will be discussed through the next sections.

This paper is structured like this: Section 2 presents the relevant works. Section 3 discusses the modified RSA technique. Section 4 presents human skin color detection and Section 5 describes the Elliptic Curve Equation.

Section 6 describes increasing the capacity of the standard LSB technique. Section 7 presents the addition of noise bits, while Section 8 describes the measures used for testing and evaluation. Section 9 presents the experimental results and Section 10 provides the conclusion.

2. Related work

Mukherjee and Sanyal [15] proposed a multi-level steganographic approach by combining the Power Modulus Scrambling (PMS) technique and Pixel Swapping Strategy (PSS). First, the input image is shuffled using the PMS technique. Then, another pass of shuffling is performed to enhance the permutation and randomness of images pixels. Rule-based strategies are used for block shifting of 2 by 2 pixels. Then, the embedding procedure is invoked for implanting the secret bits into the encrypted image. Finally, a reversing version of PMS is used to reconstruct the stego-image. Safarpour and Charmi proposed an interesting hybrid approach that aims at rising the payload using Pixel Value Differencing (PVD) along with Gray Level Modification (GLM) [16]. The authors stated that the system rises the payload by 25% while it preserves the imperceptibility. Saleh et al. proposed a technique that implies two steps [17]. Initially, an enhanced version of the AES algorithm called the AES_MPK technique is used for encrypting the input text-message. Then, the PVD-MPK and MSLDIP-MPK algorithms are joined together for embedding the encrypted message. Pujari and Shinde utilized the Blowfish technique to transform a text file into an encrypted file [18]. Then, the encrypted file is implanted in the image using the LSB technique. An enhanced Hash-LSB technique in conjunction with the RSA technique is proposed by Kumar and Sharma [19]. The Hash-LSB uses a hash function to produce a pattern for concealing text-message bits. The message bits are injected in the form of (3, 3, 2) bits into color channels R, G, and B of each point. Salimi et. al. [20] proposed to divide the input image into several blocks. Then, Differential Evolution (DE) technique is used to locate the best location for these blocks in the image for the embedding stage. Then, the DWT technique is used to calculate an optimized value of the coefficient for text-message embedding. The authors stated that the system is robust against different types of attacks. Hsu and Tu [21] presented a QR-based technique to enhance robustness against cropping attacks. To accomplish this goal, each bit of the watermark data is presented by four copies. These copies are concealed in the cover image at different image blocks. The sinusoidal function is used as an inserting rule, and the wavelength of the sinusoidal function controls the trade-off between imperceptibility and robustness. In the case of attacks, the four copies of the embedded bits may be inconsistent at the receiver side. Therefore, after extracting the four copies bits, the tampering detection is used to judge the actual value. Pillai et al. proposed using clusters concept where the input image is segmented into several segments and then conceals the text bits in these segments [22]. Indrayani et al. [23] proposed using the Advanced Encryption Standard (AES) technique for concealing data in MP3 files. The MD5 function is used for key generation. The encrypted data are hidden in the homogeneous frames. A similar technique that is based on dynamic key encryption was proposed by Patel and Meena [1]. In [24], the authors described a semi-fragile reversible authentication technique. First, the system accomplishes regional localization for multi-classes of geometries and topologies. A modified version of the Prediction Error Histogram PEH is used for the embedding stage. Then, an adaptive bin-width selection approach is also used to get discriminating histograms. More related works can be found in [4] [25] [26] [27] [28].

3. The RSA cryptography

The main goal of cryptography is to convert the confidential information into an encoded version so that only authorized persons can read and process it [28, 29]. Generally, encryption is used by different parties such as governments, corporations, and people to preserve the secrecy of data. While encryption is frequently used, sending an encrypted message may attract the attention of the others [30, 31]. Therefore, combining

steganography and cryptography in one integrated system provides a double level of security [17, 31]. Practically, the communicating parties are denoted by the *sender* and *receiver*. Each party needed to have a copy of a certain secret key. Only the holder of the key will be able to decrypt the data. Various methods such as ElGamal, RSA, Diffie-Hellman, MD5, IDEA, etc. are presented in the literature [28]. The RSA algorithm was invented by MIT researchers in 1977 and becomes one of the commonly used algorithms for secure data transmission [28]. It is an asymmetric algorithm and based on the modular exponentiation characteristic.
The RSA algorithm compromises three main steps as follows [28] [32]:

3.1. Key generation

First, the public and private keys are created by the sender as follows [28]:

1) Two prime numbers are selected by the sender. These are p and q.
2) Compute the modulus $n = p \times q$.
3) Determine $m = (p-1) \times (q-1)$.
4) Select e to be the public key. Here e is in range $(1, m)$ and $gcd(m, e) = 1$
5) Find the private key d where $d \times e \ mod \ m = 1$ and d is the multiplicative inverse of e.
6) The public key is represented as (e, n) and the private key is represented as (d, n)

3.2. Encryption

Then, with the public key (e, n), the cipher-text C is produced using Eq. 1 where:

$$C = M^e mod\, n \qquad (1)$$

3.3. Decryption

The private key (d, n) is used to regain the secret-text message M using Eq. 2 where:

$$M = C^d \ mod\, n \qquad (2)$$

Generally, RSA provides a high level of information security. Despite that, many attacks are used by attackers [28, 32]. In this study, we proposed an enhanced RSA algorithm by adding a new factor K along with the classical basic parameters p and q to make the attacker mission more problematic. Now, the cipher-text C is produced using Eq. 3 where:

$$C = (M^e mod\, n\,) \times K \qquad (3)$$

where K is a positive integer that increases the search space. So, the receiver can use the private key (d, n) and K to regain the original text M as follows:

$$M = \left(\frac{C}{K}\right)^d \ mod\, n \qquad (4)$$

The encrypted message is then embedded into the input image as will be shown in the next sections.

4. Automatic skin-color detection

The term automatic skin-color detection can be characterized as follows: given a subjective picture, the aim of skin color detection is to determine whether or not there are any potential human skin-color regions in the image and, if exist, get the image position and range of each region. The detected skin-color regions may include any exposed part of the individual like faces, shoulders, arms, and legs. From image-processing view point, automatic skin-color detection is basically a segmentation problem to locate human targets in images. It is an important pre-processing step with several practical applications like face recognition [33] [34], monitoring cameras [35] [36], hand gesture recognition [37] [38], naked image filters [39] [40] [41], content-based image retrieval [13], etc. The ultimate goal of this task is to segment the input image into two segments: one containing skin-regions (i.e., skin-map) and non-skin region (i.e., background). Typically, a binary image is utilized to show the output of the detector. The skin-maps are declared as a group of adjacent pixels that have 1's (white). In contrast, the non-skin regions are declared as a group of adjacent pixels that have 0's (black). Skin- maps usually masked with the input image to show skin detection results. In this work, we adopted the skin detection method presented by [42]. This method uses multi-skin color clustering models for detecting skin-regions. These are: light-colored, reddish, white, and Blackish skin. These skin-regions constitute the skin-map. Figure 2 shows the experimental results of the proposed skin detector where Figure 2(a) shows the input images. Figure 2(b) shows the corresponding skin maps and Figure 2(c) shows the skin detection results. As shown in this figure the results imply few non-skin regions that have a color close to skin color.

5. Elliptic curve equation

To enhance the security level of the steganography, a modified random pixel selection technique to hide the secret bits based on Elliptic Curve Equation ECE is proposed [11]. The ECE was initially presented by Neal Koblitz and Victor Miller in 1985 for encryption purposes [11]. The main idea of ECE is based on Elliptic Curve Discrete Logarithm Problem (ECDLP) where this problem takes full exponential time to be solved [43]. The simplified Elliptic Curve Equation is given as follows [11]:

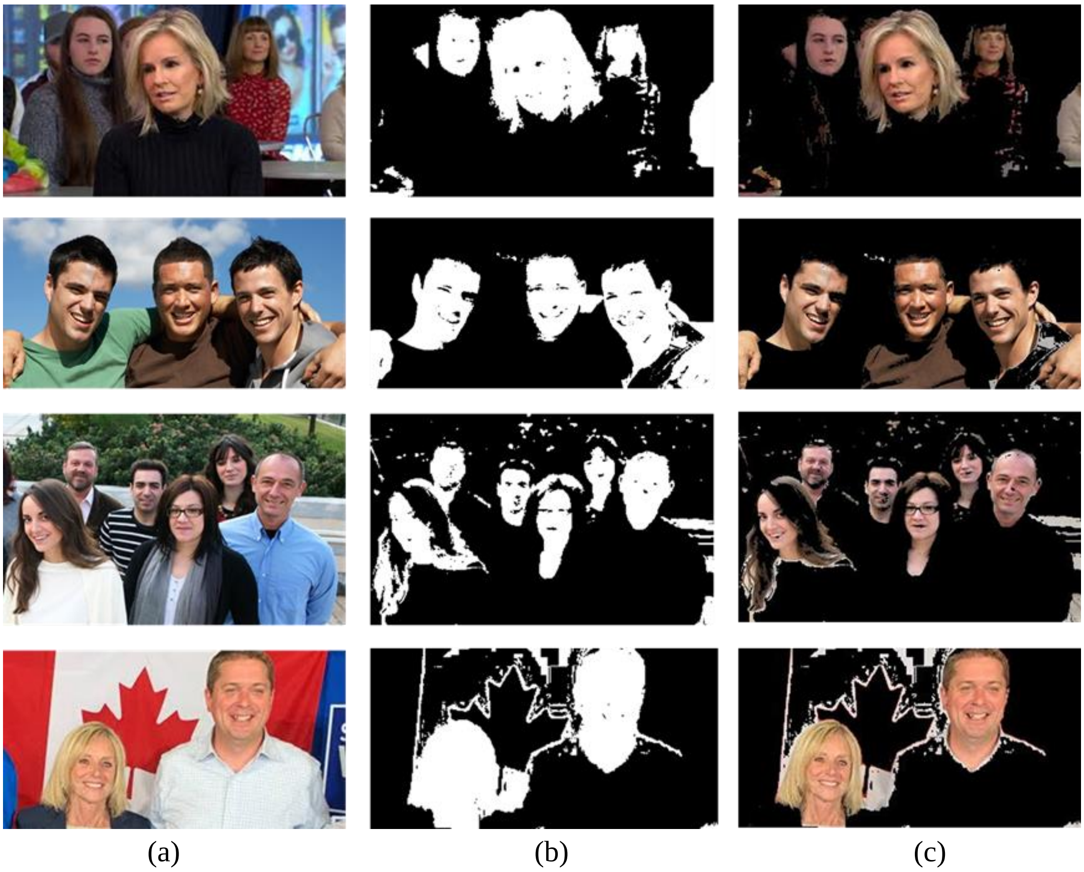

Figure 2. Automatic skin detection results. (a) Input image; (b) Skin Map; (c) Skin detection results

$$y^2 \equiv x^3 + ax + b \ (mod\ p) \qquad (5)$$

where a and b are randomly selected integers; and modulus p is randomly selected prime number greater than 3. The generation of the traversing path requires us first to choose five randomization parameters. These are:

the coordinates of a point called *Seed point* $(x_0, y_0), a, b,$ and modulus p. The solutions (x_i, y_i) on the elliptical curve is largely influenced by these parameters. Using different randomization parameters produces a completely different list of random points. Now, even though the attackers may succeed to locate which pixels hold the message bits, they will retrieve scrambled bits and have to find the correct combination of these bits for successful message reconstruction. Integrating ECE with the skin detection step is done as follows: If the newly generated ECE point belongs to the skin-map, it will be skipped. Otherwise, the newly generated point will be added to the traversing path.

6. Rising the payload

The Least Significant Bit (LSB) technique is one of the most commonly used techniques for information hiding [30] [25] [27] [44]. The central features of this technique contributed to the following factors: 1) it can be implemented in both spatial and frequency domains; 2) a lesser amount of distortion; 3) can be used with different types of digital carriers; 4) simple and fast implementation. With traditional LSB, the secret message is converted into a stream of bits. Then, each secret bit is implanted directly in the cover-image at the least significant bit (i.e., 8th bit) of some pixels [45] [46]. Based on many extensive experiments [30] [47] to substitute the (i.e., the 7th and 8th bits), the pixel will preserve the same visual color because the amount of the change remains very trivial in consideration to the enormous possible colors (i.e., over 16 million colors for 24-bit pixel representation). Aiming at rising the payload of the traditional LSB, we proposed using two-bit tokens rather than one-bit for embedding and extracting the secret bits. Therefore, the payload of embedding is doubled. Practically, rising the payload more and more (e.g., 3-LSBs) can affect the imperceptibility of the proposed system. It is known that there is a balance to be achieved between the payload and quality.

7. Adding noise

We propose adding noise bits to the stego-image. This makes the attacker's task more confusing. The attacker needs not only to locate the pixels that hold the secret bits (i.e., pixel values have been modified) but also to isolate the ones that hide the real message from the ones that imply noise.

In practice, the more noise embedded; the more confusing it is to the attackers but at the cost of image quality. Adding noise to an image is carrying out as follows: the user should identify the amount of noise L to be embedded. Then, L points are generated randomly. When a point is already overlapped with any point of the traversing path or skin-map, it will be discarded. On the other side, the receiver uses the above-mentioned parameters to reconstruct the actual hidden data. The general step-by-step algorithm of the proposed system at the sender's end is listed as shown in Algorithm 1.

Algorithm 1.

```
The Proposed Algorithm (Sender Part)

Input:   Cover-image $I$ of size (M×N×3), Message, Public-key, the factor K, L , Randomization parameters.
Output:  Stego-image

1)   Convert the message into a number stream.
2)   Apply eq. No. (3) of the modified RSA to encrypt the number stream.
3)   Compute the size $Z$ of the ciphered stream.
4)   Apply skin detection technique to locate skin regions in the cover-image.
5)   Convert the 3D cover-image of size $N×M×3$ into 1D array $IS$ of size ($N×M×3$, 1) with an index of each pixel.
6)   Create a traversing path that will hold the secret bits using ECE along with the skin detection results of Step 4.
7)   Convert ciphered text bytes into a binary stream of 2-bit tokens.
8)   Conceal the secret bits in $IS$ based on the traversing path of random points that are generated by Step 6.
9)   Add noise bits into unused pixels of $IS$.
10)  Converting the 1D-array $I$S into 3D-matrix to rebuild the Stego-image.
11)  Output Stego-image.
```

8. Fidelity measures

This section presents the measures used to calculate the imperceptibility level of the proposed steganography technique. These are:

8.1. Mean square error (MSE)

The MSE tells us the difference level among the pixel values. In other words, the average squared variation among the actual pixel intensities of the host image and the new pixel intensities of the stego-image. The main goal is to minimize the MSE which is computed using Eq. 6 [12] [30]:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - E(i,j)]^2 \qquad (6)$$

where I and E refer to the source and stego-images. The m and n represent the image size.

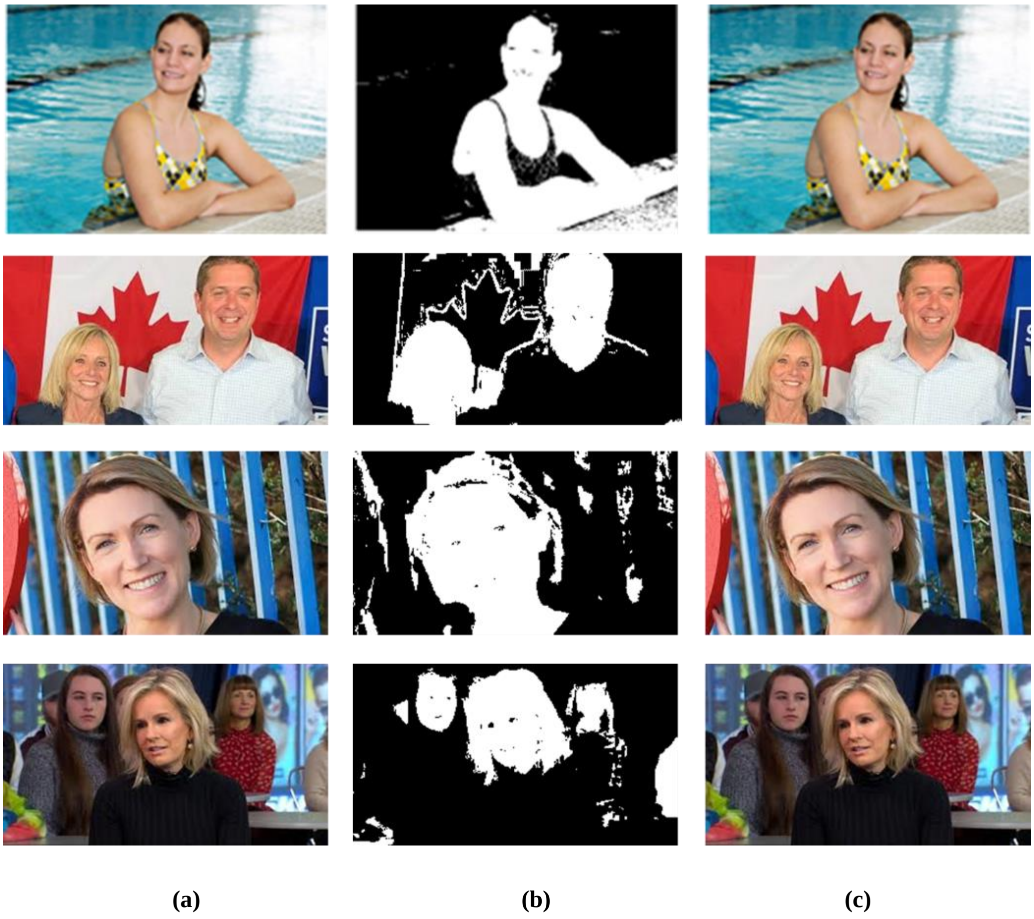

Figure 3. The experimental results of the proposed technique. (a) The original cover-image; (b) The corresponding skin-map; (c) The resulting stego-image

8.2. Peak signal to noise ratio (PSNR)

The PSNR is a measure of perceptibility that represents the relation between the highest probable signal power and the power of error. It is a measure for comparing two images of the same size. The PSNR is computed using Eq. 7 [11] [48]:

$$PSNR = 10\, log_{10} \frac{R^2}{MSE} \qquad (7)$$

where R usually equals 256. As PSNR is higher, the closeness between the two images is higher.

8.3. Structural similarity index measure (SSIM)

The SSIM is considered one of the recent measures to evaluate the visual quality of the stego-image. The SSIM is computed using Eq. 8 [49]:

$$\text{SSIM(x,y)} = \frac{(2\,\mu_x\,\mu_y + C_1)\,(2\,\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1\,)(\sigma_x^2 + \sigma_y^2 + C_2\,)} \qquad (8)$$

Where the constants C_1 and $\mathrm{C}_2 > 0$ are used to ensure stability when the other parameters approach 0's. The σ is the standard deviation and μ is the average intensity. Two images are highly alike when the SSIM approaches one.

9. Experimental results

Two image datasets are used to evaluate the proposed technique. These are:

- Set A: The University of Southern California image database “USC-SIPI” [50]. The dataset is publically available to support various types of researches in the field of image processing. It was divided into different subsets according to the basic character of the images. In this work, we had used the ”Miscellaneous” subset that offers high quality colored images.
- Set B: Our own image dataset. This dataset comprises 260 images collected from the Internet from different sources. It emphasizes images with human targets (i.e. single and multi-human targets).

Figure 3 presents the qualitative evaluation examples of the proposed technique. Figure 3(a) shows the cover-images. Figure 3(b) shows the corresponding skin-maps. Figure 3(c) shows the resulting stego-images. As shown in this figure, the original cover-images and stego-images are visually very similar with no detectable defects. Furthermore, the results show that the embedding process has no effect on human targets because these regions do not hide any information.

Table 1 show quantitative evaluation examples where lower MSE values mean less error. As PSNR values are higher and SSIM approaches to 1, the best quality of the stego-image is obtained. The message length used in this table: 52, 105, 158, and 211 characters. As shown in Table 1, the performance of the proposed technique indicates a significant security level with high image quality.

Table 1. The fidelity measures using different message lengths

Message Length (Char)	Average PSNR	Average MSE	Average SSIM
52	82.800335	0.000406	0.999999
105	81.352555	0.000802	0.999999
158	81.637475	0.001230	0.999998
211	79.237475	0.001668	0.999998

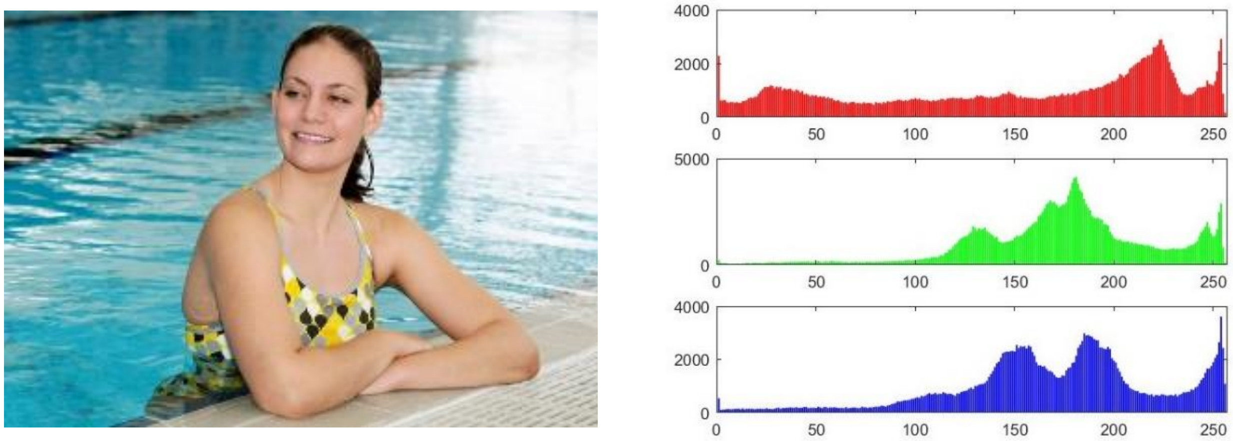

Figure 4. The cover-image and its corresponding histograms of the three-color channels (i.e., Red, Green, and Blue)

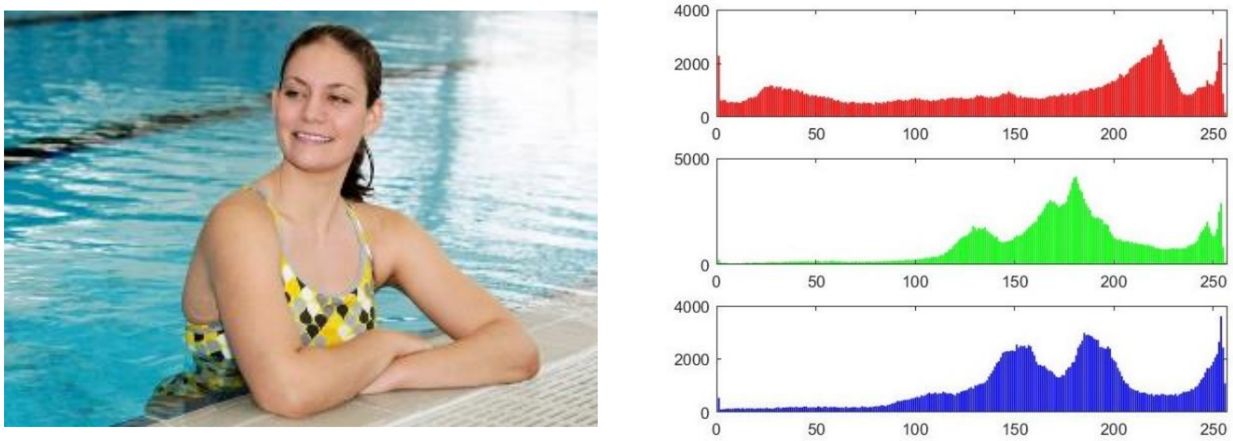

Figure 5. The stego-image and its corresponding histograms of the three color channels (i.e., Red, Green, and Blue)

An image histogram is considered another interesting evaluation parameter that can be used to show the quality of the steganographic technique. Figure 4 presents the cover-image and its corresponding histograms. Figure 5 presents the corresponding histograms after hiding 52 characters. As shown in these figures, both histograms are extremely alike. By considering that the input image comprises many non-overlapped segments (i.e., subregions) which can be segmented based on some predefined features, different segments usually have different payloads for concealing the secret data bits. This is the main reason for the proposed approach which will keep skin regions as they are (i.e., unmodified) while the embedding procedure will implant the secret bits into non-skin regions as far as possible.

10. Conclusion

In this paper, a skin detection method to enhance image-based steganography approach in the spatial LSB domain is presented. This method can also be used for watermarking and copyrighting applications. As mentioned in Section 4, our Human Vision System HVS tends to focus its attention on selectively certain structures of the visual scene instead of the whole image. If embedding message bits is done in these regions of interest, the stego-image becomes more random with visual defects that are easy to detect. It is clear that these regions should not be used for hiding information. In most existing image-based steganographic techniques, the pixels that hide the data are selected freely without considering the content of the input image. However, this assumption is not always true, particularly when dealing with images containing human targets. The main contribution of this paper, supposedly, this is the first endeavor that utilizes the color feature of the human skin in the application to steganography which can choose the “embedding regions”. Practically, skin color is good evidence of the existence of human targets in images. By locating the human targets in images, a modified Least Significant Bit (LSB) algorithm is used to hide information in such a way that keeps the human targets intact to preserve the visual quality. In addition, an enhanced RSA cryptography and Elliptic Curve Equation (ECE) are also used together in one integrated system to provide an extra level of security. The idea of implanting the secret bits into points generated based on randomization parameters rather than using systematic methods inhibits the steganalysis from anticipating the pixels that hold the real bits. By considering the traditional LSB and RSA techniques along with human skin detection, the proposed system shows minimum visual defects with a double level of security. Furthermore, our proposed approach can be extended to be applied for other digital host files such as video clips and art works in the spatial or frequency domains.

References

[1] N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography," presented at the International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.

[2] S. Almuhammadi and A. Al-Shaaby, "A survey on recent approaches combining cryptography and steganography," *Computer Science Information Technology (CS IT),* 2017.

[3] M. A. Alsarayreh, M. A. Alia, and K. A. Maria, "A Novel Image Steganographic System Based on Exact Matching Algorithm and Key-Dependent Data Technique," *Journal of Theoretical and Applied Information Technology,* vol. 95, p. 1212, 2017.

[4] A. Baby and H. Krishnan, "Combined Strength of Steganography and Cryptography-A Literature Survey," *International Journal of Advanced Research in Computer Science,* vol. 8, 2017.

[5] J. Ali and S. P. Ghrera, "CWEA: A Digital Video Copyright Protection Scheme," *International Journal of Computer Information Systems and Industrial Management Applications. ISSN,* vol. vol. 10, pp. 2150-7988, 2018.

[6] M. Mishra, G. Tiwari, and A. K. Yadav, "Secret communication using public key steganography," presented at the International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 2014.

[7] B. Furht, E. Akar, and W. A. Andrews, *Digital Image Processing: Practical Approach*: Springer, 2018.

[8] J. C. Russ, *The image processing handbook*: CRC press, 2016.

[9] S. Sun, "A new information hiding method based on improved BPCS steganography," *Advances in Multimedia,* vol. 2015, 2015.

[10] K. Joshi, K. Puniani, and R. Yadav, "A Review on Different Image Steganography Techniques," *Digital Image Processing,* vol. 8, pp. 179-186, 2016.

[11] A. Y. Tuama, M. A. Mohamed, A. Muhammed, and M. H. Zurina, "Randomized Pixel Selection for Enhancing LSB Algorithm Security against Brute-Force Attack," *Journal of Mathematics and Statistics* vol. 13, pp. 127-138, 2017.

[12] A. Tiwari, S. R. Yadav, and N. Mittal, "A review on different image steganography techniques," *International Journal of Engineering and Innovative Technology (IJEIT) Volume,* vol. 3, pp. 19-23, 2014.

[13] A. Y. Taqa and H. A. Jalab, "Increasing the reliability of fuzzy inference system-based skin detector," *American Journal of Applied Sciences,* vol. 7, p. 1129, 2010.

[14] M. R. Mahmoodi and S. M. Sayedi, "A Comprehensive Survey on Human Skin Detection," *International Journal of Image, Graphics & Signal Processing,* vol. 8, 2016.

[15] S. Mukherjee and G. Sanyal, "A multi level image steganography methodology based on adaptive PMS and block based pixel swapping," *Multimedia Tools and Applications,* vol. 78, pp. 17607-17622, 2019.

[16] M. Safarpour and M. Charmi, "Capacity enlargement of the PVD steganography method using the GLM technique," *arXiv preprint arXiv:1601.00299,* 2016.

[17] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," *IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 7, pp. 390-397, 2016.

[18] A. A. Pujari; and S. S. Shinde, "Data Security using Cryptography and Steganography," *IOSR Journal of Computer Engineering,* vol. 18, 2016.

[19] A. Kumar and R. Sharma, "A secure image steganography based on RSA algorithm and hash-LSB Technique," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, 2013.

[20] L. Salimi, A. Haghighi, and A. Fathi, "A novel watermarking method based on differential evolutionary algorithm and wavelet transform," *Multimedia Tools and Applications,* pp. 1-18, 2020.

[21] C.-S. Hsu and S.-F. Tu, "Enhancing the robustness of image watermarking against cropping attacks with dual watermarks," *Multimedia Tools and Applications,* pp. 1-27, 2019.

[22] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering and encryption techniques," presented at the 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016.

[23] R. Indrayani, H. A. Nugroho, R. Hidayat, and I. Pratama, "Increasing the security of mp3 steganography using AES Encryption and MD5 hash function," presented at the 2016 2nd International Conference on Science and Technology-Computer (ICST), 2016.

[24] S. Borah and B. Borah, "Prediction Error Expansion (PEE) based Reversible polygon mesh watermarking scheme for regional tamper localization," *Multimedia Tools and Applications,* pp. 1-22, 2020.

[25] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing,* vol. 90, pp. 727-752, 2010.

[26] S. Jindal and N. Kaur, "Digital image steganography survey and analysis of current methods," *International Journal of Computer Science and Information Technology & Security,* vol. 6, pp. 10-13, 2016.

[27] B. Li;, J. He;, J. Huang;, and Y. Q. Shi;, "A Survey on Image Steganography and Steganalysis," *Journal of Information Hiding and Multimedia Signal Processing,* vol. 2, 2011.

[28] V. Pachghare, *Cryptography and information security*: PHI Learning Private Limited, Delhi, India, Second Edition, 2015.

[29] O. F. Rashid, Z. A. Othman, and S. Zainudin, "A novel DNA sequence approach for network intrusion detection system based on cryptography encoding method," *International Journal on Advanced Science, Engineering and Information Technology,* vol. 7, pp. 183-189, 2017.

[30] K. U. Singh, "A Survey on Image Steganography Techniques," *International Journal of Computer Applications,* vol. 97, 2014.

[31] S. Saraireh, "A Secure Data Communication system using cryptography and steganography," *International Journal of Computer Networks & Communications,* vol. 5, p. 125, 2013.

[32] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced method for RSA cryptosystem algorithm," presented at the Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on, 2012.

[33] S. Kolkur, D. Kalbande, P. Shimpi, C. Bapat, and J. Jatakia, "Human skin detection using RGB, HSV and YCbCr color models," *arXiv preprint arXiv:1708.02694,* 2017.

[34] S. Bilal, R. Akmeliawati, M. J. E. Salami, and A. A. Shafie, "Dynamic approach for real-time skin detection," *Journal of Real-Time Image Processing,* vol. 10, pp. 371-385, 2015.

[35] K. Gautam and S. K. Thangavel, "Video analytics-based intelligent surveillance system for smart buildings," *Soft Computing,* vol. 23, pp. 2813-2837, 2019.

[36] R. D. F. Feitosa, A. da Silva Soares, and L. C. Pereyra, "A New Clustering-based Thresholding Method for Human Skin Segmentation Using HSV Color Space," presented at the 2018 IEEE Symposium on Computers and Communications (ISCC), 2018.

[37] T. J. McBride, N. Vandayar, and K. J. Nixon, "A Comparison of Skin Detection Algorithms for Hand Gesture Recognition," in *2019 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA),* 2019, pp. 211-216.

[38] K. Yadav, L. P. Saxena, B. Ahmed, and Y. K. Krishnan, "Hand Gesture Recognition using Improved Skin and Wrist Detection Algorithms for Indian Sign," *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org,* vol. 9, 2019.

[39] J. Wehrmann, G. S. Simões, R. C. Barros, and V. F. Cavalcante, "Adult content detection in videos with convolutional and recurrent neural networks," *Neurocomputing,* vol. 272, pp. 432-438, 2018.

[40] J. S. Lee, Y. M. Kuo, P. C. Chung, and E. L. Chen, "Naked image detection based on adaptive and extensible skin color model," *Pattern Recognition,* vol. 40, pp. 2261-2270, Aug 2007.

[41] D. Ganguly, M. H. Mofrad, and A. Kovashka, "Detecting Sexually Provocative Images," presented at the 2017 IEEE Winter Conference on Applications of Computer Vision (WACV), 2017.

[42] R. Zainuddin, S. Naji, and J. Al-Jaafar, "Suppressing False Negatives in Skin Segmentation," presented at the International Conference on Future Generation Information Technology, 2010.

[43] L.-p. Lee and K.-w. Wong, "An elliptic curve random number generator," in *Communications and Multimedia Security Issues of the New Century,* ed: Springer, 2001, pp. 127-133.

[44] A. K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm," *IJISET-International Journal of Innovative Science, Engineering & Technology,* vol. 2, pp. 858-862, 2015.

[45] A. Senarathne and K. De Zoysa, "ILSB: Indexing with Least Significant Bit Algorithm for Effective Data Hiding," *International Journal of Computer Applications* vol. 161, 2014.

[46] G. Swain and S. K. Lenka, "A novel steganography technique by mapping words with LSB array," *International Journal of Signal and Imaging Systems Engineering,* vol. 8, pp. 115-122, 2015.

[47] M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques," *International Journal of Advanced Science and Technology,* vol. 54, 2013.

[48] J. Rani and T. A. Khan, "Performance Optimized DCT Domain Watermarking Technique with JPEG," *International Journal of innovative Technology and Exploring Engineering,* vol. 4, 2014.

[49] K. Rao and H. Wu, "Structural similarity based image quality assessment," in *Digital Video image quality and perceptual coding,* ed: CRC Press, 2005, pp. 261-278.

[50] The USC-SIPI image database [http://sipi.usc.edu/database/] [Online].