View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Periodicals of Engineering and Natural Sciences (PEN - International University of...

Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 1, February 2020, pp.67-78

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, Baghdad, Iraq
[2] Ministry of Higher Education and Scientific Research, Baghdad, Iraq
[3] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

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 degrade the visual quality especially for the images 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 provide 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 experimental results show that the proposed system 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 cover medium [1-3]. Steganography plays a crucial role in numerous information security systems with a wide-ranging of applications such as confidential communications, data storing, user authentication, and copyright protection [4, 5]. Many different mediums such as digital images, sound files, text files, video clips, etc., are used by different steganography techniques [5, 6].

Nowadays, we are generating a huge number of images. A very significant contributing factor has definitely been the social media sites which provide the media millions of images daily [7, 8]. With image-based steganography, some image bits are replaced with bits of the secret message which we want to hide [9] [10]. After hiding the message, the resulting image is called stego-image. It remains difficult for ordinary individuals to detect the slight change in pixel intensities due to the fact that the amplitude of the change is so small [11]. But in practice, many challenges are associated with steganography techniques that should be carefully considered when designing a secure system. These may include: robustness against statistical

attacks, invisibility (i.e., implies that the stego-image looks very similar to the original image), the amount of secret

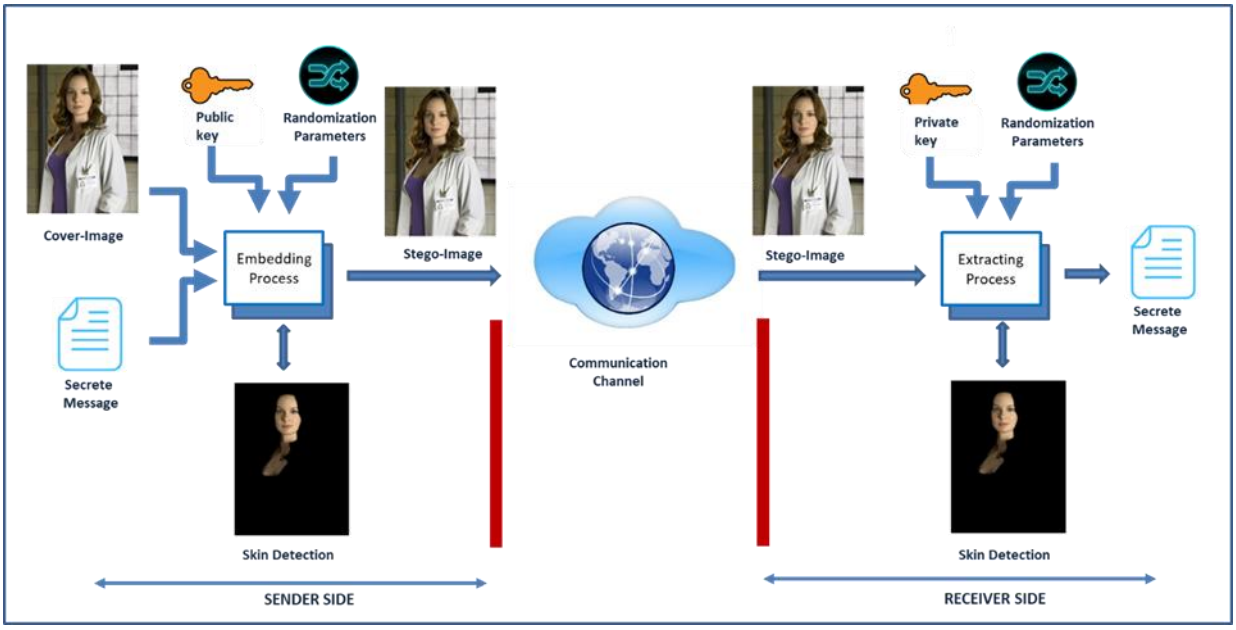


Figure 1. The outline of the overall design scheme

data which can be hided in the cover media (i.e., capacity), 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 hided. This paper covers the third question with the ultimate goal to minimize the visual defects in the resulting stego-image.

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, to the best of our knowledge, this is the first attempt that employs skin color feature in 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.

The remaining sections of this study are organized as follows: Section 2 presents the relevant works. Section 3 discusses the modified RSA technique. Section 4 presents human skin color detection and Section 5 describes 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 presents the fidelity measures. Section 9 provides the experimental results of the proposed technique. Lastly, Section 10 provides the conclusion.

2. Related work

Many steganographic methods have been proposed in the literature. Uppal et al. developed a system of double layers that combines an enhanced RC6 algorithm for encryption and LSB technique for hiding the data [15]. The enhanced RC6 cryptography uses 8 × 32-bit registers. Along with these registers, the inclusion of integer multiplication in this algorithm increases the diffusion per round. The authors show that their system provides highly secured communication. In [16], Saraireh proposed the filter bank cipher technique for encryption that offers high speed and enhanced security level. Message embedding is achieved using the Discrete Wavelet Transform (DWT)-based steganography. Saleh et al. offered a system that comprises two stages [17]. At first, the secret message is encrypted using a modified version of the AES algorithm that is named the AES_MPK algorithm. In the second stage, the PVD- MPK and MSLDIP-MPK techniques are combined to hide the encrypted message in gray-scale images. Pujari and Shinde proposed applying the Blowfish encryption algorithm to transform a text file into an encrypted file [18]. Then, the produced ciphered text is embedded into a cover image using LSB-based steganography. Kumar and Sharma presented a modified LSB algorithm alongside the RSA algorithm to provide greater security [19]. The Hash-LSB is based on a hash function for generating a pattern to hide the message bits. Then, each 8-bits of the message are inserted in sequence of (3, 3, 2) bits into Red, Green, and Blue (RGB) channels of each pixel. Similar work was presented by Satar et. el. [20]. They proposed using the Diffie-Hellman algorithm to generate the traversing path of pixels to be used for hiding message bits. Dhamija and Dhaka described a secure scheme for exchanging information within cloud servers [21]. The proposed scheme uses one's complement method, that they named SCMACS. It is based on symmetric key principles. In the steganography step, they use the standard LSB algorithm. Pillai et al. presented a method of clusters where the cover image is divided into several segments and then hides the message bits in these segments [22]. Among the numerous clustering methods, the authors suggested using the K-means clustering technique to produce clustering results. In [23], the authors proposed using MP3 files for hiding data. The secret data are encrypted using the Advance Encryption Standard (AES) algorithm along with Message Digest (MD5) hash function for key generation and processing. Then, the encrypted data are embedded in the homogeneous frames of the MP3 audio files. Patel and Meena presented a similar system that uses dynamic key cryptography [1]. The dynamicity of the key is based on rotating the key where each rotation step generates a new key. In this scheme, the Pseudo Random Number Generator (PRNG) is used to generate points that will hold the message bits. More related works can be found in [4] [24] [25] [26] [27].

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]. Governments, companies, and individuals typically apply encryption to protect their data and files stored in computers, servers, cloud computing, and mobile devices such as cell phones or notebook. Although encryption is commonly used for protecting data, sending an encrypted message could attract the immediate attention of a third party [16, 30]. Therefore, combining steganography and cryptography in one integrated system provides a double level of security [16, 17]. Many cryptography techniques are in use today such as DES, RSA, Diffie-Hellman, DSA, ElGamal, ECC, MD5, IDEA, etc. [28].

The RSA technique was proposed by three researchers from MIT, Ron Rivest, Adi Shamir and Leonard Adleman in 1977 [28]. It is based on the property of modular exponentiation and presents the structure of public key cryptosystem. The RSA is an asymmetric technique. The advantage of this technique is that it offers high security level when the key is sufficiently large. The same algorithm can be used for encryption and decryption. Nowadays, the RSA method has become one of the most widely-used public key encryption techniques and plays a crucial role in a wide range of information security applications.

Using the RSA technique involves three steps: key generation, encryption, and decryption as follows [28] [31]:

3.1. Key generation

In standard RSA, the sender creates his public and private keys with the following procedure [28]:

1) Choose two prime numbers p and q.
2) Calculate the modulus $n = p \times q$.
3) Calculate $m = (p-1) \times (q-1)$.

4) Choose the public encryption key e, where $1 < e < m$ and $gcd(m, e) = 1$
5) Determine the private key d. Utilize Euclidean algorithm to get $d \times e \ mod\ m = 1$ where d is the multiplicative inverse of e.
6) The public key consists of (e, n)
7) The private key consists of (d, n)

3.2. Encryption

Now, for encrypting a secret plain text message M, the message is converted into an integer number using any padding scheme. Then, the cipher text C is generated using the public key (e, n) as follows:

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

3.3. Decryption

The decryption in RSA is also an exponential operation. So, the original plain text M is retrieved using the private key (d, n) as follows:

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

Although RSA technique offers high security level, many different attacks are possible against this technique. These may include brute-force, guessing, timing attack, and mathematical attack [28, 31]. In this study, we proposed an enhanced RSA algorithm by adding a new factor F along with the classical basic parameters p and q to make the cryptanalysis task more difficult. Now, for encrypting a secret plain text message M, the message is converted into an integer number. Then, the cipher text C is generated using the public key (e, n) as follows:

$$C = (M^e mod\ n) \times F \quad (3)$$

where F is a randomly chosen positive integer that increases the search space that enhances the security level. At the receiver end, retrieving the original message M will require the use of the private key (d, n) and F as follows:

$$M = \left(\frac{C}{F}\right)^d\ mod\ n \quad (4)$$

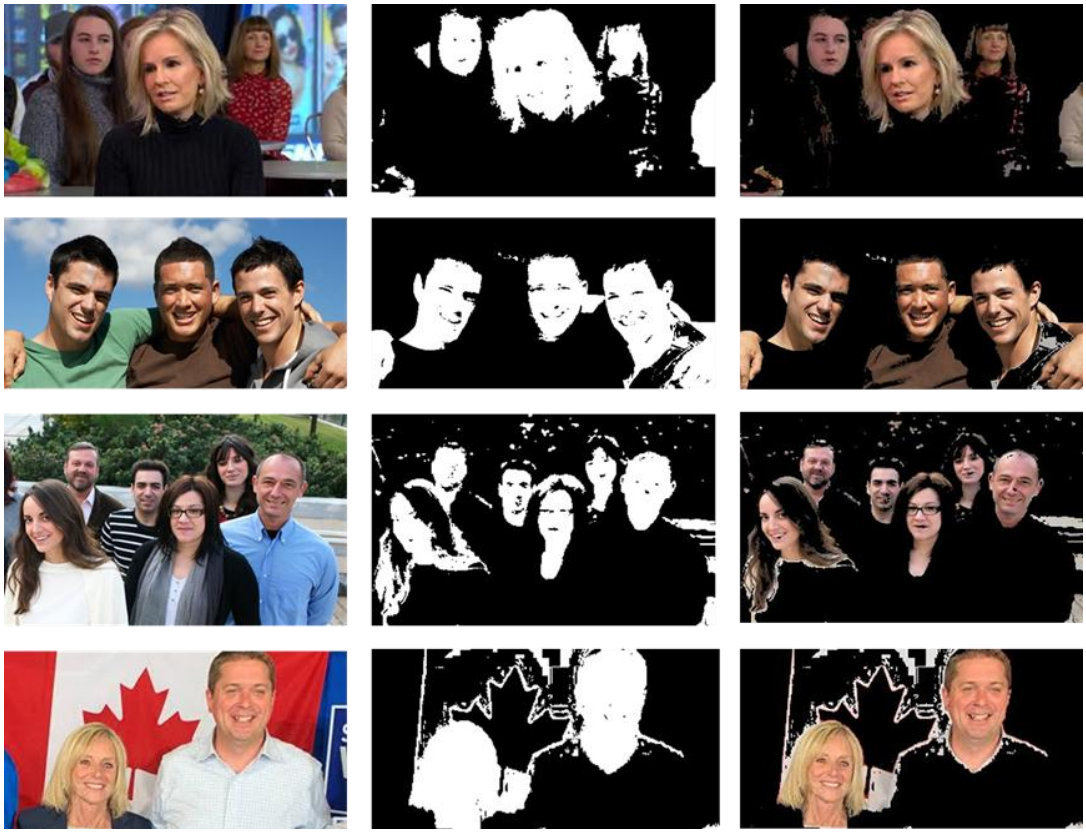
The encrypted message is then embedded into the input image as will be shown in the next sections.

4. Automatic skin-color detection

The term Automatic skin-color detection can be defined as follows: given an arbitrary image, the goal of skin color detection is to determine whether or not there are any potential human skin-color regions in the image and, if present, return the image location and extent of each region. The detected skin-color regions may include any exposed part of the human body such as 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 such as face detection/recognition [32] [33], video surveillance systems [34] [35], hand gesture recognition [36] [37], naked image filters [38] [39] [40], 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 used to represent the output of the skin detector. The skin-maps in the binary images are represented as a set of connected pixels of value 1 (white), while the background is set to value 0 (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 [41]. This method uses multi-skin color clustering models to detect skin-regions. These are: Blackish skin, white skin, reddish skin, and light-colored 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 some non-skin regions that has color similar to skin color.

5. Elliptic curve equation

To enhance the security level of the steganography, we propose a modified random pixel selection technique to hide the secret bits based on Elliptic Curve Equation ECE [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.



(a) (b) (c)

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

Discrete Logarithm Problem (ECDLP) where this problem takes full exponential time to be solved [42]. The simplified Elliptic Curve Equation is given as follows [11]:

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

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.

For brute-force attack, the attacker not only needs to find the pixels that hold the secret bits but also must determine the appropriate combination of these bits to reconstruct the hidden data. 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. Increasing the capacity of LSB

The Least Significant Bit (LSB) technique is one of the most commonly used techniques for hiding data [30] [25] [27] [43]. The main characteristics of this technique can be summarized as follows: 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. The standard LSB is based on a

substitution procedure to replace the least significant bit (i.e., 8th bit) of original pixel intensity with the secret bit directly [44] [45]. Based on many extensive experiments [30] [46], it was found that even when altering the two least significant bits (i.e., the 7th and 8th bits) of pixel's intensity, the pixel appearance will preserve the same look due to the fact that the amplitude of the change is still so small in comparison with the huge number of possible colors (i.e., over 16 million colors). With the goal to raise the capacity of the standard LSB, we proposed using two-bit tokens instead of one-bit for message encoding, message embedding, and message extracting. With this variation, the LSB can hide up to six bits in each pixel instead of three (i.e., two bits in each color channel of RGB color space). In other words, the maximum data that can be embedded into the cover image is doubled. In general, the capacity of the steganographic method can be further raised by raising the number of the substituted bits (e.g., 3-LSBs) but there is always a trade-off between the number of bits used for hiding data and the quality of the resulting stego-image.

7. Adding noise

In this study, we propose adding noise bits to the stego-image. This makes the attacker's task more confusing. The attacker needs not only to identify which pixels are hiding data (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 added to an image; the more confusing it is to the attackers but at the cost of image quality. Adding noise to an image is done as follows: suppose that K is the maximum amount of noise to be added. At the sender's end, K points are generated randomly.
When a point is already overlapped with any point of the traversing path or skin-map, it will be discarded. At the receiving end, the receiver will use the stego-image and the above-mentioned parameters to retrieve the original message. 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 F, 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 $N \times M \times 3$ into 1D array IS of size ($N \times M \times 3$, 1) with index of each pixel.
6) Generate a traversing path of random points that will hold the secret message bits using ECE along with skin detection results of Step 4.
7) Convert ciphered text bytes into binary stream of 2-bit tokens.
8) Hide the binary stream bits of the ciphered text in IS using the modified LSB algorithm at random points that are generated by Step 6.
9) Add noise bits into unused pixels of IS.
10) Reconstruct the image by converting the 1D array IS into Stego-image.
11) Output Stego-image.

8. Fidelity measures

Fidelity measures refer to the type of measures utilized to compute the difference level between the cover-image and the resulting stego-image. The most used fidelity measures are:

8.1. Mean square error (MSE)

The mean square error represents the cumulative squared error (i.e., pixel differences) between the two images. The MSE is calculated as follows [12] [30]:

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

where, m and n are the image dimensions, I and E are the input image and stego-image respectively. The lower the value of MSE, the lower the error.

(a) **(b)** **(c)**

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 the peak error. The PSNR is calculated as follows [11] [47]:

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

where R is the maximum possible value of the pixels' intensities. The higher PSNR implies high closeness between the two images.

8.3. Structural similarity index measure (SSIM)

Inclusion of a recent measure such as Structural Similarity Index Metric (SSIM) can provide a fair comparison along with MSE and PSNR. The SSIM is regarded as one of the most powerful methods of assessing the visual closeness of images, which can be calculated as follows [48]:

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

where μ is the mean intensity, σ is the standard deviation, C_1 and C_2 are constants > 0 that are included to avoid instability when $\mu_x, \mu_y, \sigma_{xy}, \mu_x^2, \mu_y^2, \sigma_x^2, \sigma_y^2$ are very close to zero. The SSIM is in range [-1,1]. The higher SSIM close to 1, implies high visual similarity between the two images.

9. Experimental results

The experimental results provided in this section show the performance of the proposed technique. The experiments were conducted using two datasets:

- Set 1: The "USC-SIPI image database" of the University of Southern California [49]. This dataset is maintained primarily to support researchers in image processing and machine vision. The database is divided into categories with many famous images such as Lenna, Mandrill, Peppers, etc.
- Set 2: Our own image dataset comprises a collection from the Internet. This dataset consists of 260 images collected from different sources and includes various image types.

For qualitative evaluation, Figure 3 shows examples of applying the proposed technique. Figure 3(a) shows the original 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.

For quantitative evaluation, the lower the value of MSE, the lower the error. The higher PSNR value and SSIM close to 1, implies the better visual quality of the image. Table 1 shows the calculated PSNR, MSE and SSIM using different secret messages. The length of the secret message includes 52, 105, 158, and 211 characters. As shown in Table 1, the system achieves a significant security level with high image quality.

Table 1. The PSNR, MSE, and SSIM experimental results

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

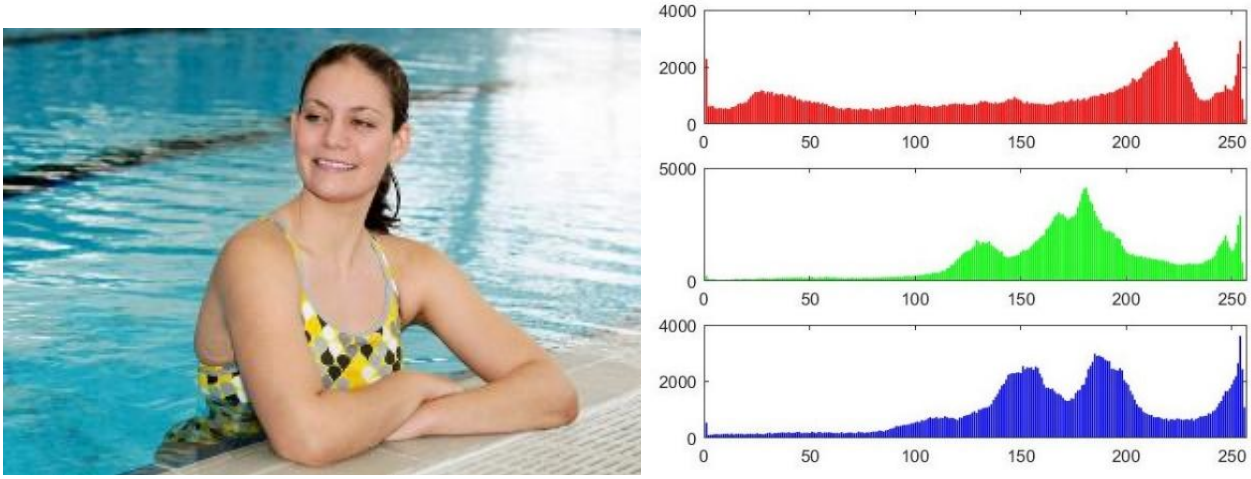


Figure 4. The cover-image and its corresponding histograms of the three color channels (i.e., Red, Green, and Blue).

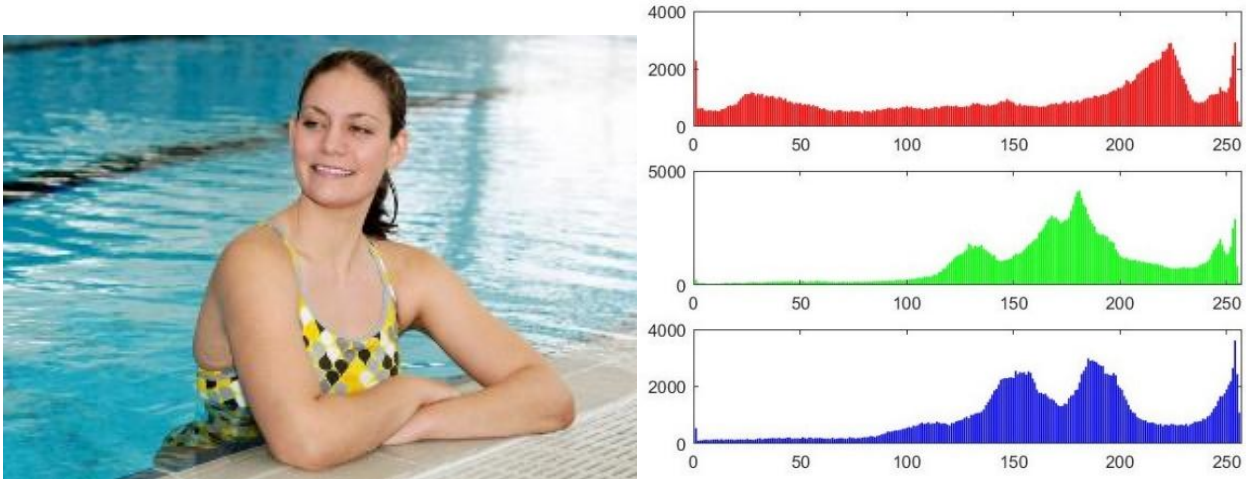


Figure 5. The stego-image and its corresponding histograms of the three color channels (i.e., Red, Green, and Blue).

Another measure that can be employed to show the quality of the steganographic technique is the image histogram. Figure 4 shows the cover image and its corresponding histograms of the three color channels (i.e., Red, Green, and Blue). Figure 5 shows the stego-image and the corresponding histograms of its three color channels after embedding a message of 52 characters. As shown in these figures, the histograms of the stego-image are highly similar to their corresponding histograms.

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, to the best of our knowledge, this is the first attempt that employs skin detection in application to steganography which considers the pictorial information in the input image and consequently 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. Applying randomization to hide message bits rather than storing them on a systematic basis makes the system more secure. Compared to standard RSA and LSB techniques, the proposed system achieves minimum visual defects with double level of security.

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] R. S. Ankit Uppal, Renuka ngapal, Aakash gupta, "Merging Cryptography and Steganography Combination of Cryptography: RC6 Enhanced Ciphering and Steganography: jpeg," *International Journal of Advanced Computational Engineering and Networking*, vol. 2, Oct. 2014.
[16] S. Saraireh, "A Secure Data Communication system using cryptography and steganography," *International Journal of Computer Networks & Communications,* vol. 5, p. 125, 2013.
[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] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, and M. Mamat, "A New Model for Hiding Text in an Image Using Logical Connective," *International Journal of Multimedia and Ubiquitous Engineering,* vol. 10, pp. 195-202, 2015.
[21] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," presented at the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.
[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] K. D. Patel and S. Belani, "Image encryption using different techniques: A review," *International Journal of Emerging Technology and Advanced Engineering,* vol. 1, pp. 30-34, 2011.

[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] 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.
[32] 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.
[33] 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.
[34] K. Gautam and S. K. Thangavel, "Video analytics-based intelligent surveillance system for smart buildings," *Soft Computing*, vol. 23, pp. 2813-2837, 2019.
[35] 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.
[36] 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.
[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.
[42] 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.
[43] 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.
[44] 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.
[45] 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.
[46] M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques," *International Journal of Advanced Science and Technology*, vol. 54, 2013.
[47] 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.

[48] 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.
[49] The USC-SIPI image database [Online] [Online].