Hindawi
Journal of Computer Networks and Communications
Volume 2018, Article ID 8695103, 9 pages
https://doi.org/10.1155/2018/8695103

Research Article

A Framework of Secured Embedding Scheme Using Vector Discrete Wavelet Transformation and Lagrange Interpolation

Maheswari Subramanian[1,2] **and Reeba Korah**[3]

[1]*Department of Electronics and Communication Engineering, Sathyabama University, Chennai, India*
[2]*St. Joseph's College of Engineering, Chennai, India*
[3]*Alliance University, Bangalore, India*

Correspondence should be addressed to Maheswari Subramanian; maheswari.mani@gmail.com

Received 19 May 2017; Revised 13 September 2017; Accepted 26 October 2017; Published 1 March 2018

Academic Editor: Rui Zhang

Information hiding techniques have a significant role in recent application areas. Steganography is the embedding of information within an innocent cover work in a way which cannot be detected by any person without accessing the steganographic key. The proposed work uses a steganographic scheme for useful information with the help of human skin tone regions as cover image. The proposed algorithm has undergone Lagrange interpolation encryption for enhancement of the security of the hidden information. First, the skin tone regions are identified by using YC_bC_r color space which can be used as a cover image. Image pixels which belong to the skin regions are used to carry more secret bits, and the secret information is hidden in both horizontal and vertical sequences of the skin areas of the cover image. The secret information will hide behind the human skin regions rather than other objects in the same image because the skin pixels have high intensity value. The performance of embedding is done and is quite invisible by the vector discrete wavelet transformation (VDWT) technique. A new Lagrange interpolation-based encryption method is introduced to achieve high security of the hidden information with higher payload and better visual quality.

1. Introduction

The two major fast emerging trends of information hiding are steganography and watermarking. Steganography is the art and science of invisible communication. The main goal of steganography is to hide secret data into the other innocent digital media. It is a novel way of secret communication used in recent times. A majority of the existing steganography techniques use digital multimedia files as cover media to hide secret data. Using steganography, information can be hidden in different embedding media, known as carriers. These carriers can be images, audio files, video files, and text files. The concealment is accomplished by hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1–3], and by definition, it may be called as "covered writing." Cover image refers to the image used for carrying the embedded bits. Embedded data are known as payload, and the image with embedded data is called stego image [4].

Digital watermarking [5] is the process of embedding or hiding digital information called watermark into a multimedia product, and the embedded data can later be extracted or detected from the watermarked product, for protecting digital content copyright and ensuring tamper resistance, which is indiscernible and hard to remove by unauthorized persons. The visible and invisible types are major watermarking techniques, but steganography is always done in invisible manner. Hence, the demand for security is increasing day by day, leading to the use of steganography for information security [6].

Figure 1 shows the basic schematic of the steganography process. Here, the sender sends the secret message which

remains confidential. It can be texts, images, videos, audios, or any other information. The cover is the channel in which the message is embedded and it serves to hide the existence of the message. The message embedding method solidly depends on the structure of the cover [3].

Cover image is the original image into which the wanted secret message is embedded. It is also named as innocent image or host image. The secret message should be embedded to ensure the absence of any significant variation in the statistical properties of the cover image. Hence, cover image is an original unaltered message.

Stego image is the conclusive image obtained after embedding the payload into a given cover image. It should have similar statistical properties to that of the cover image. So, the cover image with the secret message embedded is called the "stego image." Hiding information may involve a stego key which is additional secret information. The stego image obtained should be securable and retrievable by the recipient alone [7–9].

El Rahman [10] describes the study of discrete cosine transform-based steganography for hiding secret bits sequentially in least significant bits (LSBs). The method indicates that the larger hiding capacity is achieved in the middle frequency band which relatively gives better PSNR and MSE. Here, confidential information associated with nuclear control system and related to nuclear reactor is used for embedding process. The spatial to frequency domain transformation using DCT is achieved here and quantization is taken place using quantization tables after the transformation. Standard images like Baboon and Lena are taken as the cover image. The author used a different size of cover image and a different message size for hiding. The DCT method gives low PSNR with a high MSE value.

In [11, 12], the basic spatial domain method is used for steganography. Bai et al. [11] said that a steganography approach is discussed based on the combination of LSB substitution mechanism and edge detection. In this paper, the cover image is classified into edge and non-edge areas using various detection techniques. Here, the authors say that the edge area pixels are carrying secret data with 5 LSBs of the stego image cleared. Hence, this methodology achieves larger embedding length with the usage of 3 MSBs for edge detection. The drawback is that the cover image and stego image are not much similar by using various edge detections. The authors achieve the average PSNR as 45 dB which shows that the quality of the image is distorted. The usage of edge detection also takes more computational time for embedding. In [12], generating a pseudorandom value of each pixel value of the cover image is introduced for embedding process. Random pixel embedding is achieved using the LSB method. Standard images are taken as a cover image and secret message as a binary number in bits.

Ramalingam and Mat-Isa [13] maintain the security of hidden data and minimizes distortions in the stego image. They proposed a hiding technique using discrete cosine transform (DCT) with minimum distortions achieved by discrete wavelet transform (DWT) coefficients. The secret messages were embedded in the transform domain of the video sequences. By combining two different transform

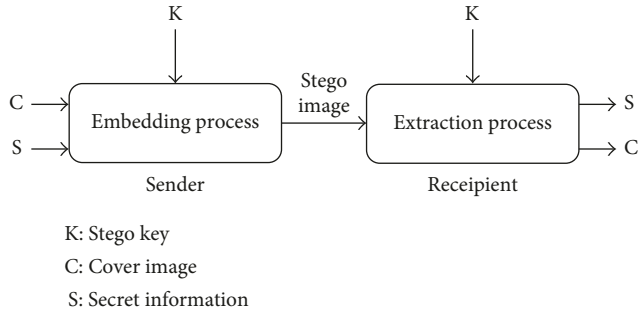

Figure 1: Basic schematic of the steganography technique.

domain methods, more number of coefficients arise which takes more space and processing time. Since DWT has four numbers of coefficients, the authors could not conclude which coefficient is used for reducing distortions.

In [14], a steganographic scheme is proposed using different edge detectors like Canny, Sobel, and Fuzzy. The edge image is generated by clearing the last 5 LSBs operation to the original image called MSB image. Here, the embedding capacity is calculated by the maximum number of embedding bits used per pixel (bpp). This method may reduce the computational time complexity.

In this paper [15], two new steganography methods in spatial domain are discussed. The idea behind this is the substitution of a group of bits in a pixel by another group of bits of the same length, and hiding of one or two bits of secret data is achieved. The first method known as 1 bit group of bits substitution (1-bit GBS) method hides one bit per pixel, whereas the second method (2-bit GBS) is used to hide two bits per pixel. Again two different spatial methods are used here to make the system complex.

Indra Sena Reddy and Siva Kumar [16] proposed a combination of steganography and cryptography together for the improvement of security. The most common wavelet method is used for data embedding in low coefficient band. The main drawback here is the need of more computational time and poor embedding process with an average PSNR of 49 dB.

In the field of secret information hiding, researchers should concentrate on three requirements which are payload, imperceptibility, and robustness. Among the three, payload and imperceptibility are interrelated. The main requirement in steganography is embedding capacity or payload. It is defined as the total number of secret bits which one can hide into the cover image. Achieving higher capacity should mean that more secret messages will be carried by the cover image. The imperceptibility is used to measure the quality of the image by attaining the high peak signal-to-noise ratio (PSNR) [17]. The minimum distortion is introduced by embedding operation which will guarantee that it cannot be identified by the human visual system (HVS). In the proposed method, capacity of embedding is higher than that in the existing methods. Similarly, imperceptibility or image quality is tested by achieving high PSNR values.

The main aspect of steganography is to achieve high security and robustness. Security in steganography refers to the eavesdropper's inability to detect the hidden information,

whereas robustness refers to the ability of the embedded data to remain intact when the stego image undergoes any transformation like cropping, scaling, filtering, and addition of noise.

The rest of the paper is organized as follows: Section 2 discusses an overview of image steganography techniques. Section 3 presents the methodology of the proposed work. Image quality and performance evaluation measures are illustrated in Section 4. Section 5 concludes the paper.

2. Related Work

The major image steganography techniques are spatial domain and transform domain techniques. Spatial domain techniques embed information in the intensity of the original image pixels directly. The simplest and the most widely used spatial domain steganography method is the least significant bit (LSB) method where it replaces the least significant bit of the original pixel with the message bit. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is the embedding of confidential data at the rightmost bits which may have the smallest weighting. Therefore, the embedding procedure does not affect the original pixel value greatly. An ability of handling noises by the LSB method is not in a high level. Though it is an easy and straightforward technique, it cannot maintain the quality of a cover image and secret data can be easily stolen by extracting the whole LSB plane. For a color image model, each color layer may be decomposed into 8 bits. The secret message may be hidden by altering the least significant bit in a particular layer. More bit planes can be obtained by other bit plane decomposition algorithms in order to embed more information [18]. The most widely used uncompressed file formats are bitmap (BMP) and TIFF in image steganography. The other technique is called the substitution technique, which substitutes the redundant part of the cover object with a secret message.

In transform domain techniques [3], the images are first transformed or distorted and then the secret message is embedded in a transform space of the image. Transform domain steganography methods hide data in the image coefficients of the represented domain. After mapping to another domain such as discrete Fourier transform, cosine transform, curvelet transform, and wavelet transform, the obtained coefficients are altered or replaced. These transform methods are more robust than spatial domain embedding techniques while maintaining better quality of the image [18].

Digital multimedia content, in the form of images, audios, and videos, is widely used in electronic commerce, national security, forensics, networked communications, social networking websites, and other fields [5, 6].

In [7], wavelet transform (WT) converts spatial domain information to frequency domain information. In this method, a mother wavelet is selected with a nonzero function in a small interval and used for exploring the properties of the function in that interval. The mother wavelet is then translated to another interval of time. Wavelets are used in the image steganography model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel-by-pixel basis. The various transforms are discrete cosine transform (DCT), discrete wavelet transform (DWT), Hadamard transform, dual-tree DWT, double density dual-tree DWT (DD DT DWT), ridgelet transform, curvelet transform, and so on. Embedding is then done in suitable transform coefficients. As transform domain methods are more immune to image processing operations and are less susceptible to stego attacks, they are usually preferred to spatial domain methods. Various techniques can be employed for optimal choice of the transform coefficients to hide data in.

Other steganography techniques are spread-spectrum techniques and distortion techniques [6].

Spread-spectrum techniques embed secret messages which adopt ideas from spread-spectrum communications. Spread-spectrum transmission in radio communications transmits messages below the noise level for any given frequency. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image. For permitting the transmission of more than one bit, the cover image has to be broken into subimages [4, 19, 20]. When these subcover images are tiles, the technique is referred to as direct sequence spread-spectrum steganography. When the subcover images consist of separate points distributed over the cover image, the technique is referred to as frequency hopping spread-spectrum steganography. These techniques require searching of the image for the carrier in order to retrieve the data. A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This implies that there is a significant change in the channel capacity of the image. Thus, in practice, the difficulty in recovering a real number decreases the value to a single bit. It is a blind scheme as the original image is not required during extraction. This method outperforms in terms of payload capacity and invisibility. Spread-spectrum steganography involves embedding in noise inherent to image acquisition process. Image restoration and error control techniques can be used while extracting the data at the decoder side.

Distortion techniques store secret messages by signal distortion and measure the deviation from the original cover in the extraction step [2].

3. Methodology

The proposed method introduces a method of embedding secret information into the high-intensity layer of detected and extracted skin tone regions using YC_bC_r [21]. The extracted skin tone region is used as a cover image in this methodology. Any information like digital images, old handwritten documents [22], and logos can be chosen for secret information. The embedding process is carried through the technique called VDWT using random stego key. After embedding, it is necessary to obtain the system in a secured way. Hence, encryption has been performed using the Lagrange interpolation technique, and the secret information is recovered

using correlated information of the embedded image and stego key. Finally, the decryption process is carried out for recovering the original cover image.

Most of the researchers have chosen cover images such as standard images like Lena image and Baboon image and secret images such as standard internet images of a cup and rose. In the proposed mechanism, extracted skin regions are chosen as the cover image that carry secret information. Hence, a new method is proposed for embedding the secret information in horizontal and vertical sequences of the skin areas using VDWT algorithm which allocates the secret information as a column vector. The high intensity skin pixels carry the secret bits which cannot be recovered by the third party without the stego key.

In our methodology, handwritten documents and logos are used as secret information. According to available literature, this may be the first method to hide secret images like old handwritten documents and logos in skin regions which are used as a cover image. Here, the skin pixels are highly used to hide the secret information.

In addition, after the embedding process, the embedded image is converted to a RGB color image rather than to a grayscale image. This embedded image taken as a stego image is the color space converted image in this work.

Even after embedding, the quality of the stego image is good, which is proved by achieving better a PSNR value, and the stego image does not give much variation irrespective of different imaging conditions in the proposed VDWT mechanism.

More than the DWT method and spatial domain methods in the existing approach, the integration of VDWT embedding and Lagrange interpolation gives a secured way of information embedding. The proposed method achieves high PSNR than the existing methods, and nominal computational time is achieved for retrieving the secret information. It is necessary to preserve and prevent the secret information with better quality. Hence, a method is proposed to hide the secret information in the skin tone regions using VDWT mechanism and it is encrypted to improve the security. The proposed method achieved better image quality by means of focusing on information hiding in skin pixels in a secured manner.

The flow diagram of the proposed method is shown in Figure 2.

In the proposed method, the skin regions are detected by color space transformation using heuristic thresholding and embedding the secret information using VDWT. The following section deals with skin tone detection and extraction of skin tone regions.

3.1. Skin Tone Detection and Extraction. The classification of skin pixels and non-skin pixels in a color digital image plays a vital role in this methodology. Detection of human skin tone regions using YC_bC_r color space is a preprocessing step of the proposed approach. An approach of color space transformation is achieved using heuristic thresholding to detect skin tone regions by the suitable YC_bC_r color space. Since Y is a luminance component, C_b and C_r are

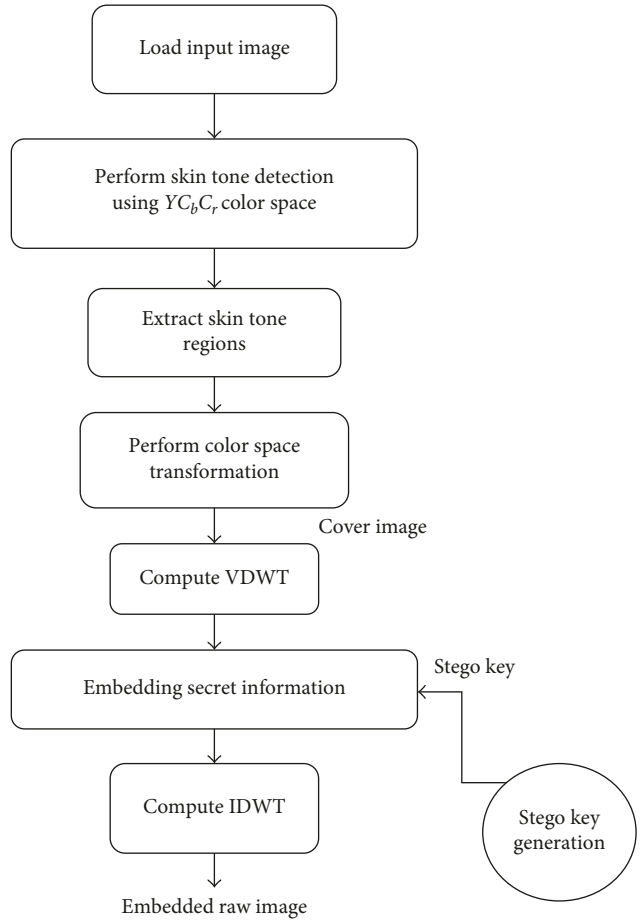

Figure 2: Flow diagram of the embedding process.

chrominance components. This method requires the choice of a heuristic thresholding as chrominance C_b should present between 77 and 127 and the value of C_r should be between 133 and 173. This predefined thresholding classifies skin regions effectively. Secondly, the detected skin tone regions alone are extracted using morphological processing. It is proved that skin regions are highly detected by this YC_bC_r color space with a high detection rate. The high-intensity layer is chosen for hiding secret information on the basis of different intensity layers of the extracted color image. The extracted high-intensity skin tone layer is used as a cover image for the proposed methodology. Extracted skin tone can be evaluated by various important measures such as F-measure, specificity, and accuracy, and the detection rate of a sample of four images is shown in Figure 3. A high detection rate is achieved by using YC_bC_r color space with heuristic thresholding.

The cover image is the high-intensity skin tone layer whose size is considered as "M" number of rows and "N" number of columns.

3.2. Embedding Using Vector Discrete Wavelet Transform (VDWT). Transform domain steganography methods are used to hide messages in new remarkable areas of the cover image. It is necessary to split the cover image into high-, middle-, and low-occurrence mechanisms. Most of the

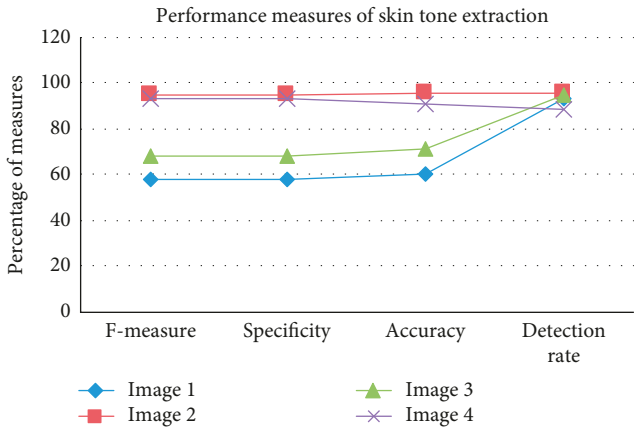

Figure 3: Curve of various measures.

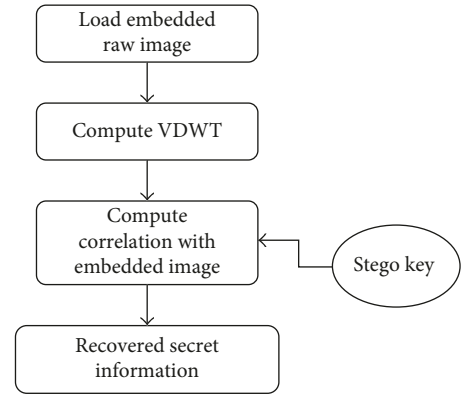

Figure 4: Flow diagram of the extraction process.

signal energy is concentrated in the inferior frequencies that contribute to visibility. Therefore, secret data are embedded in superior frequencies for eliminating chances of image deformation. Hence, the cover image has undergone frequency transformations using VDWT. These transformations compute four coefficient matrices, namely, approximation coefficient matrix (CA) and detailed coefficient matrices horizontal (CH), vertical (CV), and diagonal (CV) matrices of the cover image.

In the proposed algorithm, the secret information or an image is considered in the form of column vector. This secret information is added to the horizontal and vertical information of the cover image

3.2.1. Algorithm for Embedding Process. The algorithm to obtain an embedded raw image has been presented in this section.

Step 1: The size of the cover image as $M*N$ is taken.

Step 2: Perform VDWT of the cover image.

Step 3: Generate a random stego key sequence which is obtained by key = (KS)/256, where KS is the key sequence with the minimum and maximum value as 0 and 255, respectively.

Step 4: Generate a pseudo-noise sequence as the interblock sequence separately for horizontal and vertical information of the cover image with the respective length of the column vector of the secret image.

Iteration = 1: length (vector)

{

PN Sequence for horizontal = (2∗(rand (M/2, N/2)))

PN Sequence for vertical = (2∗(rand (M/2, N/2)))}

Iteration == 0, obtain stego image with horizontal and vertical information by embedding the secret information into the transformed cover image.

Step 5: Perform inverse VDWT to get the embedded raw image.

The embedded raw image is subjected to color space conversion in order to obtain the stego image. The advantage of vector DWT transform domain techniques over LSB and DCT techniques is that they hide information in areas of the image that is less exposed to compression, cropping, and image processing [20]. The JPEG file format is the most common image file format on the internet owing to the small size of resultant images obtained by using it. The discrete wavelet transform (DWT) method is favored much than discrete cosine transform (DCT) method, owing to the resolution, WT provides to the image at various levels. To maintain image quality, discrete wavelet transform is used for embedding process. The next section brings the method of extracting secret information from the embedded raw image.

3.2.2. Algorithm for Extraction of Secret Information. The flow diagram of extraction process is shown in Figure 4.

The algorithm for extraction of secret information is given below.

Step 1: Embedded raw image is taken as input image for extraction.

Step 2: Perform VDWT of embedded image.

Step 3: Generate a random stego key sequence.

Step 4: Generate a pseudo-noise sequence as the interblock sequence. This sequence is correlated with the embedded image to reconstruct the cover work.

The capacity of secret information embedded in the proposed and existing methods is compared and shown in Table 1.

The proposed methodology gives high payload than the existing methods. After embedding, it is necessary to secure the secret information. Hence, the next section deals with the method of encryption using Lagrange interpolation.

3.3. Encryption Using Lagrange Interpolation Using Adaptive Encryption Key. Security requirement is that a third person who notices such a communication should not be able to find out whether the sender has been active. At the same time, he or she might sense that the person really embedded a message in the cover image. Hence, encryption algorithm is implemented to make the information securable. The

Table 1: Comparison of the payload used and its capacity.

Embedding techniques	Payload	Payload capacity
Proposed method using VDWT	Handwritten document and logo	High
Horizontal band of DWT [23]	Ordinary image like cups and rose images	High
LSB method [24]	Digital data	Low
DCT-based method (hiding in LSB) [10]	Text message	Low
LSB with edge detection [11]	Information as bit	Low
LSB method [12]	Information as bit	Low

adaptive encryption key is generated in this proposed method.

Step 1: Obtain the size of embedded raw image as R and C.

Step 2: According to the size ($R*C$) of the embedded image, generate adaptive encryption key.

∗Allocate the buffer for key generation with new value $n = n*$unit 8, where minimum and maximum values of n are 0 and 255, respectively.

∗Choose the initial threshold to be less than 1.

∗Replace new threshold instead of initial threshold as per the following condition.

{

For ind = 2: n, $X\hat{}N = 1\text{-}2*T*T$; T is initial threshold.

If ($X\hat{}N > 0.0$)

Bin_X (ind) = 1

else

New threshold $T\_N = X\hat{}N$

For ind1 = 1: n/8

For ind2 = 1: 8, key (ind1) = 0 initially.

Encryption key (ind1) = key (ind1) + Bin_X (ind2∗ind1)∗ 2ˆ(ind2)}

Step 3: Interpolate the adaptive key and embedded image using bit xor operation with the following condition.

For ind1 = 1: length of embedded image

For ind2 = 1: width of embedded image

Interpolation of (ind1, ind2) = bitxor (Img (ind1, ind2), adaptive key (ind1, ind2));

Step 4: Perform decryption using encrypted image and the key.

4. Results and Discussion

The proposed method uses different handwritten documents and logo images as secret information. The different set of images is taken as an input image from the FEI face database which contains more than 500 images of various gender and illumination conditions. Nearly 50 various poses of human face images are tested for the proposed methodology, which detects skin region efficiently, and more than 50 images are tested under various illumination conditions. Samples of results acquired for different images are depicted in Figure 5, where (a) represents the original images (Image 1–Image 4), (b) represents high-intensity layer as cover image, (c) represents secret information hidden into skin tone regions, (d) represents color space converted stego image, (e) the encrypted image, and (f) the decrypted output image. The performance of embedding process is discussed in the following section.

4.1. Performance Evaluation. While designing the steganography system, the things that need to be considered are invisibility, payload capacity, computational time, security, robustness against rotation, different imaging conditions, and so on.

PSNR is used to evaluate quality of the stego image after embedding the secret message. A kind of mathematical measure of image quality is based on the pixel difference between two images [9]. It is a quality estimation of the stego image compared to a cover image. PSNR is calculated by using (1), whereas MSE stands for mean square error. The maximum possible pixel value of the image is taken as 255. If the PSNR value is greater than 36 DB, then good visibility of the stego image is obtained like that of the cover image [19].

$$\text{PSNR} = 10 * \log_{10}\left(\frac{255^2}{\text{MSE}}\right). \tag{1}$$

Equation (2) is used to calculate MSE which is computed by averaging the squared intensity of the cover and stego image pixels:

$$\text{MSE} = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - Y_{ij}\right)^2, \tag{2}$$

where X and Y are the image coordinates and M and N are the dimensions of the image (X_{ij}–Y_{ij}).

The similarity measure between the cover image and stego image has been evaluated by a parameter termed as normalized correlation N_C. The performance measure N_C is calculated by the equation given below. In (3), C (i, j) and S (i, j) are the cover image pixels and stego image pixels. The maximum value of N_C as 1 indicates that the cover image and stego image are identical and N_C value as 0 indicates that both the images are not identical [25].

$$N_C = \frac{\sum_i\sum_j C(i,j) * S(i,j)}{\sum_i\sum_j C(i,j)^2}. \tag{3}$$

The quantitative analysis of embedding process is shown in Table 2. Calculated normalized correlation N_C nearer to 1 shows the good similarity between the cover and

Figure 5: Simulation results of the embedding scheme using V-DWT and Lagrange interpolation encryption using different imaging conditions and different poses of an input image. (a) Original images (image 1 to image 4), (b) high-intensity layer as the cover image, (c) embedded raw image, (d) color space converted stego image, (e) encrypted image, and (f) decrypted output image.

Table 2: Quality measures of the proposed methodology.

Cover image	Secret information	PSNR	CT of embedding process	CT of recovering process	N_C
Image 1	Handwritten document	50.92	15.2101	1.1388	0.9988
Image 2	Logo image	52.34	11.7781	0.9516	0.9989
Image 3	Handwritten document	53.41	17.8161	1.1238	0.9990
Image 4	Logo image	51.46	16.7061	1.2214	0.9994

CT: computational time; N_C: normalized correlation.

stego image. The high measure of PSNR shows the quality of the image. The proposed method achieves a quite reasonable computation time for embedding and recovering process.

In addition, after the embedding process, the embedded image converts back to the RGB color image (Figure 5(d)) rather like a grayscale image. This embedded image is mentioned as the stego image which is a color space converted image in this process. So, the cover image in Figures 5(b) and 5(d) is visually equal. Even after embedding, the quality of the stego image is good, which is proved by achieving a better PSNR value. Moreover, the stego image does not give much variation irrespective of different imaging conditions in the proposed VDWT mechanism.

The proposed method is compared with other stego methods of [10–12, 23, 24]. Table 3 shows the comparative analysis of PSNR of the proposed method and the existing methods. It is observed that better PSNR is achieved by the VDWT scheme comparable to other schemes. In the existing approach, integration of VDWT embedding and Lagrange

Table 3: Comparison of the proposed and existing approaches.

Embedding techniques	Cover image	Payload	Average PSNR
Proposed method using VDWT	Extracted skin tone region	Handwritten document and logo	52.0325 (image 1 to image 4)
Horizontal band of DWT [23]	Standard database image like garden and house images	Ordinary image like cups and rose images	50.25
LSB method [24]	Standard image like cameraman image	Digital data	46.23
DCT-based method (hiding in LSB) [10]	Flower image	Text message	42
LSB with edge detection [11]	Edge-detected standard database image like Leena and Baboon image	Information as bit	37 to 43
LSB method [12]	Standard database image like Leena and Baboon image	Information as bit	47.23

interpolation gives a secured way of information embedding. The proposed method achieves high PSNR than the existing methods and nominal computational time is achieved for retrieving the secret information.

5. Conclusion

A steganography scheme is proposed for hiding useful secret information using human skin tone regions as cover image. YC_bC_r color space is used for accurate detection of skin tone regions in which the information is hidden. Information like digital image, handwritten documents, and logos is used as a secret image for information embedding. The proposed algorithm has undergone Lagrange interpolation encryption for achieving security for the secret information. The performance of embedding with useful information is quite invisible for the vector discrete wavelet transformation (VDWT) technique. High security of the hidden information in human skin regions is achieved by encryption. It is decrypted for getting the cover image.

Better PSNR is achieved by the VDWT scheme comparable to other schemes. The reasonable computational time is achieved by the proposed method. Maximum normalized correlation is attained using the proposed methodology.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] A. Z. Al-Othmani, A. A. Manaf, and A. M. Zeki, "A survey on steganography techniques in real time audio signals and evaluation," *IJCSI International Journal of Computer Science Issues*, vol. 9, no. 1, 2012.

[2] T. Morkel, J. H. P. Eloff, and M. S. Olivier, *An Overview of Image Steganography*, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, Pretoria, South Africa, 2005.

[3] T. Moerland, *Steganography and Steganalysis*, Leiden Institute of Advanced Computing Science, Leiden, Netherlands, 2003.

[4] M. S. Subhedara and V. H. Mankarb, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13-14, pp. 95–113, 2014, in press.

[5] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: a review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014.

[6] C. Ling and O. Ur-Rehman, *Watermarking for Image Authentication, Robust Image Authentication in the Presence of Noise*, N. Živic, Ed., Springer International Publishing Switzerland, Base, Switzerland, 2015.

[7] S. Hemalatha, "Wavelet transform based steganography technique to hide audio signals in image," *Procedia Computer Science*, vol. 47, pp. 272–281, 2015.

[8] B. Saha and S. Sharma, "Steganographic techniques of data hiding using digital images," *Defence Science Journal*, vol. 62, no. 1, pp. 11–18, 2012.

[9] A. Cheddad, "Digital image steganography: survey and analyses of current methods," *Signal processing*, vol. 90, no. 3, pp. 727–752, 2010.

[10] S.A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Computers and Electrical Engineering*, 2016, in press.

[11] J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, and Y. Liu, "A high payload steganographic algorithm based on edge detection," *Displays*, vol. 46, pp. 42–51, 2017.

[12] M. M. Emam, "An improved image steganography method based on lsb technique with random pixel selection," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 3, 2016.

[13] M. Ramalingam and N. A. Mat-Isa, "A data-hiding technique using scene-change detection for video steganography," *Computers and Electrical Engineering*, vol. 54, pp. 423–434, 2016.

[14] A. Malik, G. Sikka, and H. K. Verma, "A high capacity text steganography scheme based on LZW compression and color coding," *Engineering Science and Technology, an International Journal*, vol. 20, no. 1, pp. 72–79, 2017.

[15] G. Swain, "Digital image steganography using variable length group of bits substitution," in *Procedia Computer Science*, vol. 85, pp. 31–38, 2016.

[16] M. Indra Sena Reddy and A. P. Siva Kumar, "Secured data transmission using wavelet based steganography and cryptography by using aes algorithm," *Procedia Computer Science*, vol. 85, pp. 62–69, 2016.

[17] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and*

Countermeasures, Kluwer Academic Publishers, Boston, MA, USA, 2001.

[18] Parul, Manju, and H. Rohil, "Optimized image steganography using Discrete Wavelet Transform (DWT)," *International Journal of Recent Development in Engineering and Technology*, vol. 2, no. 2, 2014, ISSN 2347–6435.

[19] Y. A. Y. Al-Najjar and D. C. Soong, "Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI," *International Journal of Scientific & Engineering Research*, vol. 3, no. 8, 2012, ISSN 2229-5518.

[20] A. Mittal, "A highly secure skin tone based optimal parity assignment steganographic scheme using double density discrete wavelet transform," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, no. 9, 2012.

[21] P. Kakumanu, S. Makrogiannis, and N. Bourbakis, "Asurvey of skin-color modeling and detection methods," *Pattern Recognition*, vol. 40, no. 3, pp. 1106–1122, 2007.

[22] U. V. Marti and H. Bunke, "The IAM-database: an English sentence database for off-line handwriting recognition," *International Journal on Document Analysis and Recognition*, vol. 5, no. 1, pp. 39–46, 2002.

[23] H. S. Manjunatha Reddy, "Wavelet based non LSB steganography," *International Journal Advanced Networking and Applications*, vol. 3, no. 3, pp. 1203–1209, 2011.

[24] S. Gupta, "Information hiding using least significant bit steganography, using least significant bit steganography and cryptography," *International Journal of Modern Education and Computer Science*, vol. 4, no. 6, pp. 27–34, 2012.

[25] N. I. Yassin, N. M. Salem, and M. I. El Adawy, "QIM blind video watermarking scheme based on Wavelet transform and principal component analysis," *Alexandria Engineering Journal*, vol. 53, no. 4, pp. 833–842, 2014.