Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.035307
Article

Tech Science Press

An Improved Steganographic Scheme Using the Contour Principle to Ensure the Privacy of Medical Data on Digital Images

R. Bala Krishnan[1], D. Yuvaraj[2], P. Suthanthira Devi[3], Varghese S. Chooralil[4], N. Rajesh Kumar[1], B. Karthikeyan[5] and G. Manikandan[5,*]

[1]Srinivasa Ramanujan Centre, SASTRA Deemed University, Kumbakonam, Tamil Nadu, India
[2]Department of Computer Science, Cihan University–Duhok, Kurdistan Region, Iraq
[3]Department of Information Technology, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India
[4]Department of Computer Science & Engineering, Rajagiri School of Engineering & Technology, Kakkanad, Kerala, India
[5]School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India
*Corresponding Author: G. Manikandan. Email: manikandan@it.sastra.edu
Received: 16 August 2022; Accepted: 23 November 2022

Abstract: With the improvement of current online communication schemes, it is now possible to successfully distribute and transport secured digital Content via the communication channel at a faster transmission rate. Traditional steganography and cryptography concepts are used to achieve the goal of concealing secret Content on a media and encrypting it before transmission. Both of the techniques mentioned above aid in the confidentiality of feature content. The proposed approach concerns secret content embodiment in selected pixels on digital image layers such as Red, Green, and Blue. The private Content originated from a medical client and was forwarded to a medical practitioner on the server end through the internet. The K-Means clustering principle uses the contouring approach to frame the pixel clusters on the image layers. The content embodiment procedure is performed on the selected pixel groups of all layers of the image using the Least Significant Bit (LSB) substitution technique to build the secret Content embedded image known as the stego image, which is subsequently transmitted across the internet medium to the server end. The experimental results are computed using the inputs from "Open-Access Medical Image Repositories (aylward.org)" and demonstrate the scheme's impudence as the Content concealing procedure progresses.

Keywords: Contouring; secret content embodiment; least significant bit embedding; medical data preservation; secret content congregation; pixel clustering

1 Introduction

One of the classic demands of the contemporary world of the internet with digital communication is the term "secure communication." The method of hiding secret/confidential Content in a cover image is the theme of the phrase "digital image steganography" to produce the stego image, which would be transmitted to the receiver over the internet medium. The primary goal of the steganography principle is to protect the secret substance from intruders over the internet medium. New strategies and venues for

content concealing have emerged due to the availability of cutting-edge computing system facilities. To achieve the content confidentiality feature over the internet medium, the principles of Steganography and Cryptography are utilized, and Table 1 shows the main differences between the two principles.

Table 1: Difference between the terms "Cryptography" and "Steganography"

S. NO	Key elements	Cryptography	Steganography
1	Key	Required	Required
2	Base	Scrambled data	Obscured communication
3	Output	Cipher Text	Stego image
4	Detection	Easy	Complex
5	Main Concern	Robustness	Capacity and imperceptibility
6	Detection through	Cryptanalysis	Steganalysis

While both cryptography and steganography are concerned with the secure transmission of information using covert methods, there is a distinction between the two classes. Cryptography utilizes a key and a transformation to encrypt the data into a disguised form. It will have a key for the decryption of the transformed message back into its original state. In steganography, the Content is disguised into a cover object, which is then transmitted and analyzed by the receiver to acquire a secret content-embedded image known as a stego image. Both the stego and the cover image must be protected against deterioration. Steganography is a technology that hides hidden Content in a trustworthy medium, such as digital photos of grayscale or color, digital films/audio, and then pretends that it exists.

Steganography algorithms interpose a large amount of secret Content into many métiers to hide the confidential Content from attackers. The models' main conducts are the quality of the cover and stego images and their secrecy. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are two examples of steganography based on spatial and transformed domains (DWT). The goal of steganography principles is to hide a large amount of secret or confidential information on a large amount of media. The level of increasing imperceptibility, payload capacity, robustness against multiple attacks, and security are the main criteria for evaluating steganographic algorithms. Other qualities such as reversibility, encryption, and computational complexity are used in diverse applications to increase the stego object's security or communication. Steganography can be used in a variety of fields, according to current trends, and is dependent on the type of carrier. Steganography curves have been promoted due to recent technological advancements, and some of the trends include medical photographs, multimedia data, network contents, DNA patterns, and so forth. Most hidden content embodiment strategies use the famous Least significant bit (LSB) replacement strategy or the spatial orbit's pixel-value differencing scheme. One of the commonly established principles for hidden Content concealing on images is the LSB assignment method, which limits the steganographic models. Because any intruder could extract the secret data from the LSB content of the images. To improve the chaotic level of secret content extraction, authors deputize a rigid or variable length of bits in these approaches; the confidential material has been embedded into a digital image. Only if the secret stream for the embodiment procedure is large in quantity does one of the proficient methods, "Pixel-value differencing," yield more favorable results. The clustering scheme "K-Means" is based on the theory of vector quantization and aids the data mining process of cluster analysis. The K-Means clustering principle leads the sectionalization of the available 'n' reflections into 'K' clusters, with all observances processed to arrive at a cluster based on its skinniest mean value.

The suggested model has two stages that deal with the secret content embodiment process. With the help of the secret key value, a contour pattern is provided and constituted to a distinct domain in all layers of the

digital color image to traverse the pixels of the image. In the resulting contour of the layers, pixel blocks are generated and classified into 'K' separate clusters. The secret data embodiment is performed on the contour clusters using the LSB substitution approach in the next phase. As a result, the suggested approach aims to achieve efficient data privacy via pixel values on all image levels and retain secret Content via digital images. After the embodiment procedure, the freshly created stego image is subjected to communication channel transfer. After successfully detecting contour clusters at the receiver end, a reverse method might be used with the shared stego image to extract the original secret data. The proposed model's public presentation is compared to the results of many previous approaches. The trials' findings indicate that the nominated secret content embodiment practice on digital photographs is both graceful and reliable.

The proposed scheme perch comprises the following elements: The literature review is covered in segment 2, and the nominated scheme's primary idea and capabilities are presented in detail in segment 3. In segment 4, the experimental findings and analysis of the nominated scheme are presented. Finally, the nominated scheme's conclusion is provided in Section 5.

2 Literature Survey

The process of capturing digital photos has never been easier, thanks to digital cameras. Huang et al. [1] presented an approach for reversible and high-capacity data hiding in high-quality cover images. The authors nominated a model for deciding the pixels over the image by dividing the image into tiles and shifting the histograms of each image tile between its minimum and maximum frequency. Raghupathy et al. [2] demonstrated a new pattern for pixel embodiment on a grayscale image using the bishop tour pattern from the chess game. In this work, the authors thoroughly examined modern steganography concepts and provided an FEC-based double security system based on encrypted image Steganography [3]. The research proposed a model for detecting noise in transmitted images and different types of attacks. Another method proposed by the author's Prasad et al. [4] for implementing RGB color image steganography and the models is to use overlapping block-based pixel-value differencing methods. On the content concealing process, Sathish Shet et al. [5] proposed a competent paradigm for the design and development of reconfigurable architectures. The LSB and multi-bit based steganography principles were used in work mentioned above. Naqvi et al. [6] describe a methodology for steganography implementation based on the multilayer partiality homographic encryption concept. The paper demonstrates that the model provides secure text content transmission with the cover image through communication channels. Authors Manikandan et al. [7] have presented a lossless steganography system that generally adheres to clustering and contouring principles on grayscale photos. Hua et al. [8] an image encryption scheme using value-differencing transformation and modified zigzag transformation. This scheme encrypts different types of images with high level security. The method uses a partial encryption scheme for confidential Content hiding in medical photographs. Konyar et al. [9] offer a clever medical image-based data-hiding strategy for achieving content secrecy and promoting secure data transmission over the communication medium in this work. The secret content embodiment procedure in the study mentioned above employs Reed Solomon coding in conjunction with the salt and pepper noise principle. Another approach for embodiment proposed by Aziz et al. [10] for achieving protected content embodiment on images. The model described above is concerned with reversible data concealment strategies with a large secret content embedding capacity in images. The author Li et al. [11] proposed a method based on the ideas of reversible data concealment and quick response codes. The method uses a partial encryption scheme for confidential Content hiding in medical photographs. Various steganography methods and appropriate steganalysis schemes that have a high level of applicability in the field of digital forensics have been presented in work stated by the authors Dalal et al. [12], and the same authors [13] have compiled a survey for the efficient implementation of video steganography. The researchers Patel et al. [14] presented a full review of the inquiry of video steganography in the uncompressed and compressed

domains, in which several compressed and uncompressed mediums with their advantages and disadvantages in terms of information concealing were presented. The authors Lin et al. [15] demonstrated feature-based steganalysis for Pixel-Value Differencing Steganography, and the model demonstrates the significance of statistical features-oriented embodiment and detection techniques. Authors Kordov et al. [16] have proposed another implementation of the steganography principle based on color photos medium images with random order pixel selection and encrypted text message embedding. The author AbdelRaouf [17] proposed a new approach for hiding secret Content on color images, in which the pixel values for the secret content embodiment are chosen based on the visual color sensitivity of the pixels. Manikandan et al. [18] proposed a new method for achieving concealed content embodiment on sensitive medical images. The mentioned works with DICOM pictures. For pixel pattern identification, several chess-based approaches are used to explore the pixel paths, and experimental observations show that the offered model is effective. Another model proposed by authors Krishnan et al. [19] for data hiding on images works by encrypting the image and then applying the secret material to the appropriate pixel channels, with the image being descrambled after the embodiment process to return to its original form. The experimental results demonstrate the model's chaotic degree and uniqueness. It might be more powerful for detecting the places where content embodiment has been performed. Those regions must be correctly detected at the receiver end to achieve lossless content extraction. Another model suggested by the authors Yassin et al. [20] for the attainment of information hiding in digital images with the help of wavelets. The above-stated model deals with the content concealment process by following the most significant bit substitution methodology for attaining confidentiality. The authors Sabeti et al. [21] presented an adaptive image steganography method for content concealment through integer wavelet transformation. The model utilizes a genetic algorithm for pixel detection on images to perform the secret data concealment process. The authors, Pilania et al. [22], suggested an ROI-based video steganography scheme in the wavelet domain using the SVD mechanism. The above-stated model offers an efficient Steganographic model for attaining a secret stream hiding in video frames.

3 Proposed System

The proposed model has been designed to effectively combine Geodesic active Contour Algorithms, often known as Snake Algorithms, K-Means Clustering principles, and steganography's Least Significant Bit (LSB) replacement technique. The proposed novel steganographic model is concerned with layering the digital image into Red, Green, and Blue layers. The system flow begins with the contour generation principle, followed by the process of pixel clustering on picture layers such as Red, Green, and Blue, and finally, the process of identifying pixels within the contour on the previously mentioned layers to attain the secured content transmission over the communication channel partners.

The suggested model works by turning the secret Content from the medical client on an internet medium for transmission into a binary stream that may be used in the embedding process. The conversion would be carried out using the standard ASCII-based stream creation method. It generates a secret binary stream, which is then divided into three parts for the purpose of embedding practice on all of the color image's available channels or layers. The embodiment process' confidential material, or secret binary stream, has been divided into three variable length stream arrays: Red Stream, Green Stream, and Blue Stream. The kinship between the stream arrays is:

Red_Stream = Secretstream_count/2, Green_Stream = Secretstream_count/8, and Blue_Stream = (3 × Secretstream_count)/8. Where Secretstream_count is the length of the binary stream of the secret code for the embodiment process.

During the content embodiment process, the user must indicate the coordinate position in the digital image for the development of contours, and the Mapping-Key will determine the relevant cluster for the embodiment process (MK). The cluster for the embodiment process would be based on the MK value, and the secret contents of the stream array would be embedded in all three layers of the image using the

LSB replacement technique. K-Means uses the LSB approach to channel the clusters on the image layers, resulting in the stego image, a hidden binary stream-embedded image. The stego image would then be shared with the recipient through the internet medium. The secret stream from the shared stego image is recovered using the exact reverse technique at the receiver end (Medical practitioner) for offering services to the client who requested services/suggestions. The workflow of the proposed model scheme at the sender side is shown in Fig. 1, and the workflow at the receiver end is presented in Fig. 2.

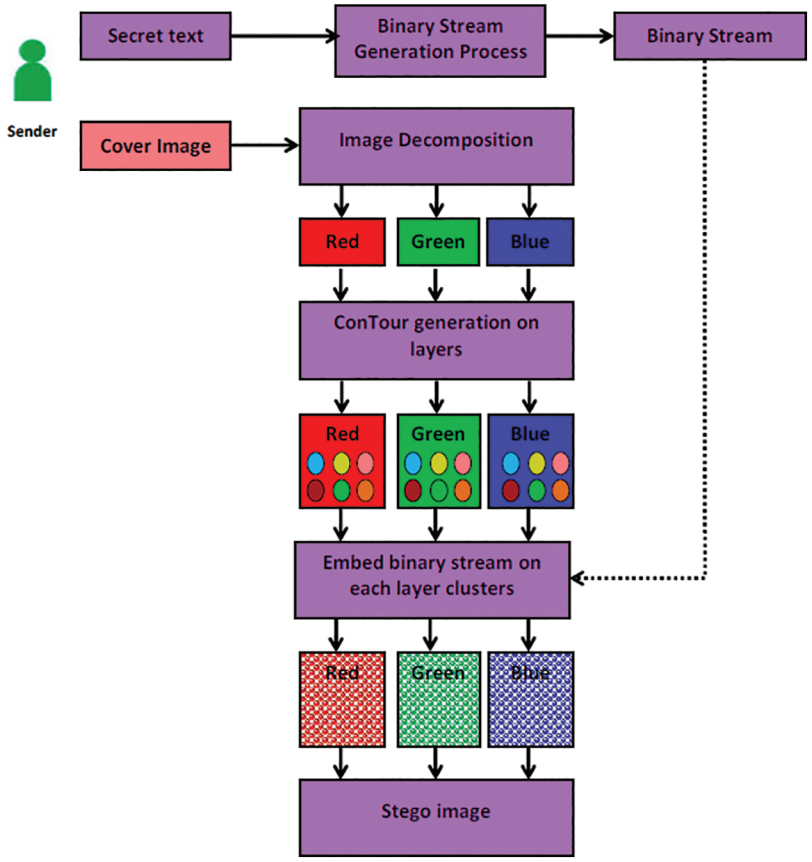

Figure 1: Secret content embodiment process at the sender side (Medical Client)

Algorithm 1 and Algorithm 2 provide a secret content embedding procedure and its corresponding extraction procedure.

Algorithm 1: Secret content embedding process

Step 1: Identify the Cover image (DICOM format) from the repository
Step 2: Generate the image coordinate position along with the value for contour size in
Step 3: each of the image layers, such as Red, Green, and Blue
Step 4: Select the Mapping-Key (MK) value for locating the contour region in the
Step 5: layers of the image, such as Red, Green, and Blue
Step 6: Perform the Clustering process on the image pixels on the Red, Green and
Step 7: Blue layers based on the generated contour stated in Step 3

(Continued)

Algorithm 1 (continued)

Step 8: Perform the LSB substitution process to hide the Red_Stream,
Step 9: Green_Stream and Blue_Stream on the corresponding clusters in Red,
Step 10: Green and Blue layers of the image (starting with cluster A, B, C… on Red
Step 11: Layer, Green Layer, and Blue Layer)
Step 12: The secret stream of the medical client from the client end through the internet medium has
Step 13: been embedded, and Stego Image is generated and shared with the receiver (Medical
Step 14: Practitioner)

Algorithm 2: Secret content extraction at receiver zone (Medical Practitioner)

Step 1: Received the Stego Image from the sender zone
Step 2: Split the received stego image into layers such as Red, Green, and Blue
Step 3: Specify the image coordinate position along with the value for contour size in
Step 4: each of the image layers, such as Red, Green, and Blue, to yield the contour
Step 5: The shared Mapping-Key (MK) from the sender is used to exemplify the
Step 6: contour region on the Red, Green, and Blue layers of the image
Step 7: Detect the clusters on the Red, Green, and Blue layers on the contour regions
Step 8: of the stego image
Step 9: Secret Content from the LSB positions on the Red, Green, and Blue layers
Step 10: are extracted, and the secret stream is cumulated.
Step 11: Secret Content for the communication is extracted from the Secret stream
Step 12: generated in Step 6.

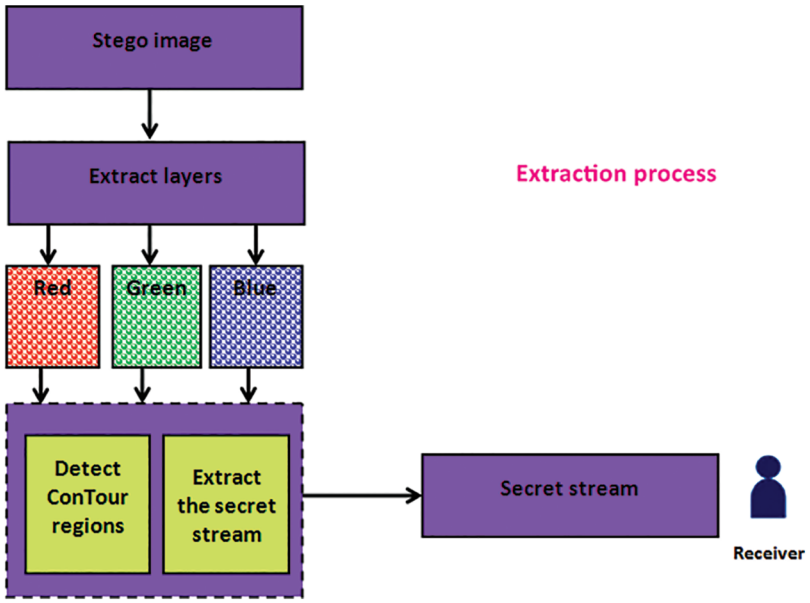

Figure 2: Secret content extraction process at the receiver side (Medical Practitioner)

The proposed model holds the pixel clusters for the embedding process with better intelligence using Mapping-Key (MK). On the contours of the image layers, the K-Means clustering principle is imposed, resulting in K-Clusters. In each contour, a minimum of 6 clusters can be found based on the dimension of the input cover image, with each cluster holding 6 pixels for the embedding process. As a result, six clusters are formed in each layer of the cover image 'K' for the secret content embodiment procedure.

On a color image, the secret stream embodiment phase works by picking out pixels in each cluster one by one, and the emergence can be completed after the embodiment of Red Stream, Green Stream, and Blue Stream content. The secret stream count on the relevant layers might be used to determine the size of the contour zone on the cover works. If the image's size is insufficient for the embodiment process, the image will be processed by increasing the size of the contour region on the image layers. Fig. 3 shows a sample of the pixel selection process and alternate region selection and clusters.

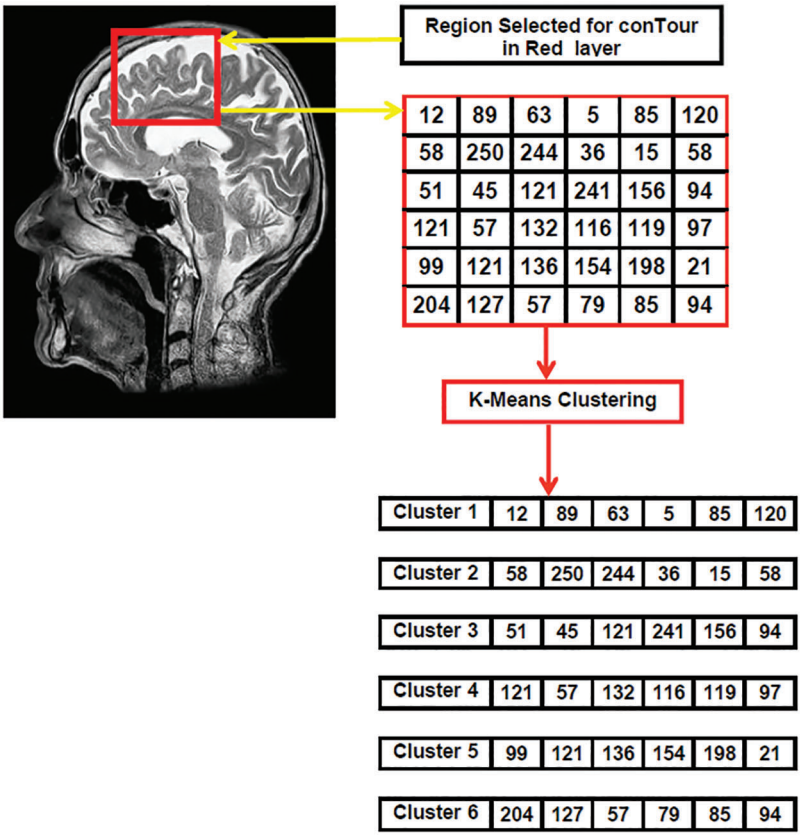

Figure 3: Clusters generation process for red layer in cover image

The initial values of the pixels in the clustered regions are adjusted after the secret stream embodiment process on the pixels of the Red, Green, and Blue layers of the image. Table 2 shows the initial cluster values, the secret stream in natch of bits, the secret bits embedded cluster value, and the cluster similarity percentage.

Table 2: Similarity between the initial and updated cluster values

Cluster	Value before embodiment	Binary stream	Value after embodiment	Cluster similarity percentage
Cluster 1	12	11	15	33%
	89	01	89	
	63	11	63	
	5	10	7	
	85	10	86	
	120	10	122	
Cluster 2	58	10	58	33%
	250	11	251	
	244	00	244	
	36	00	36	
	15	10	14	
	58	11	59	
Cluster 3	51	10	50	16.66%
	45	11	46	
	121	01	121	
	241	10	242	
	156	10	158	
	94	00	92	
Cluster 4	121	00	120	16.66%
	57	10	58	
	132	11	135	
	116	11	119	
	119	10	118	
	97	01	97	
Cluster 5	99	01	97	49.98%
	121	01	121	
	136	11	139	
	154	10	154	
	198	10	198	
	21	10	22	
Cluster 6	204	11	207	16.66%
	127	11	127	
	57	10	58	
	79	00	76	
	85	00	84	
	94	01	93	

4 Experimental Observations

The proposed LSB-based embedding model with Contour and K-Means clustering strategy was developed in MATLAB R2021a software, input DICOM images with layers (Red, Green, and Blue) are taken from the source "Open Access Medical Image Repositories (aylward.org)" [23] and output snapshots of the processed inputs are presented below. The proposed model works with six contour clusters on each layer of the image, and each cluster holds six-pixel values. So that it is possible to hide 12 bits of data using LSB substitution on each cluster, a maximum of 216 bits of private data would be permitted to hide in an image with dimensions 512 × 512. The proposed model's resilience has been tested with various dimensional values of the input images (as shown in Fig. 4) and varied dimensions of the contours (as shown in Fig. 5). The following four input color images are considered for processing in the experimental outgrowth: (i) Head (ii) Skull (iii) Chest and (iv) Hand. The color images are used as input cover images, and the secret stream has been inserted in the images, resulting in the stego images shown in Fig. 6.

Figure 4: Clusters generation process for red layer in cover image

Figure 5: Various contour sizes generated on various image dimensions

The metrics Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Number of Pixels Change Rate (NPCR), and Unified Averaged Changed Intensity (UACI) are determined to assess the compatibility of the stego picture with the corresponding cover image. The process for computing MSE, PSNR, NPCR, and UACI for a N × N cover picture and stego scale image is described in Eqs. (1)–(4).

$$\begin{aligned} MSE(colorimage) = \frac{1}{p \times q} \sum_{i=1}^{p} \sum_{j=1}^{q} \Big[& \left(C_{Image}Red_{Layer}(i,j) - S_{Image}Red_{Layer}(i,j)\right)^2 \\ & + \left(C_{Image}Green_{Layer}(i,j) - S_{Image}Green_{Layer}(i,j)\right)^2 \\ & + \left(C_{Image}Blue_{Layer}(i,j) - S_{Image}Blue_{Layer}(i,j)^2\right) \Big] \end{aligned} \tag{1}$$

where C_{Image} and S_{Image} represents the cover and stego images, respectively. The symbols $Red_{Layer}(i, j)$, $Green_{Layer}(i, j)$ and $Blue_{Layer}(i, j)$ denote the pixels (Red, Green, and Blue) in locations (i, j) of the C_Image and S_Image. The parameters p x q denote the image dimensions.

$$PSNR = 10\ log_{10}\ \frac{255^2}{\text{MSE}} \tag{2}$$

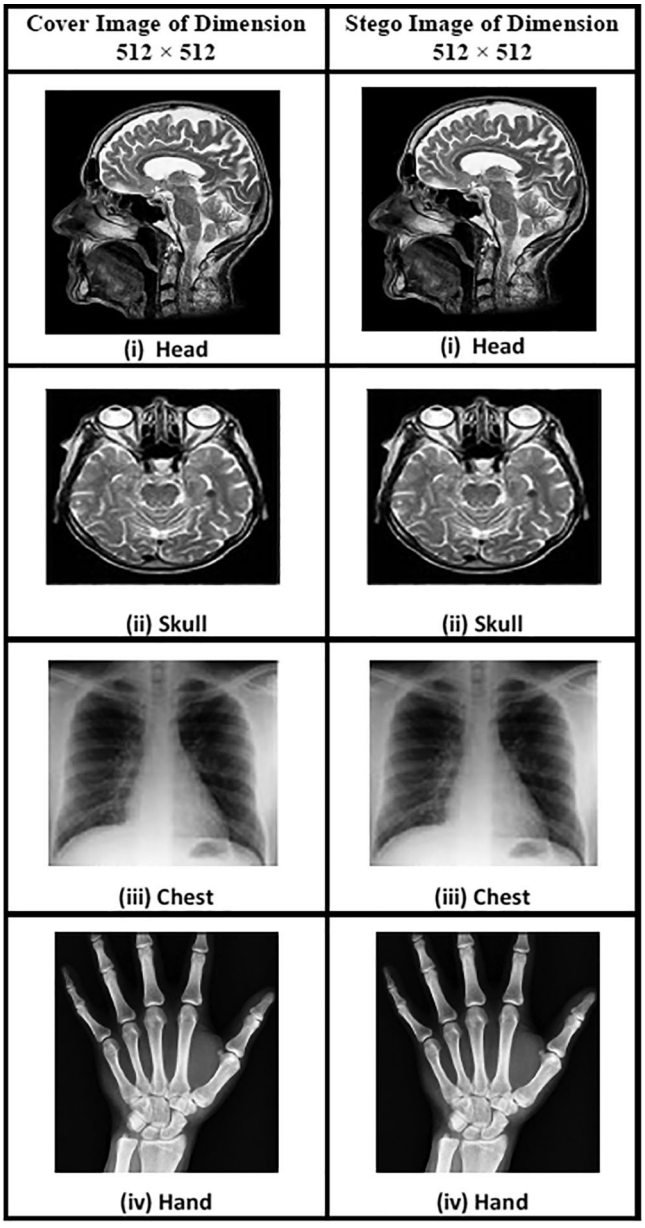

Figure 6: Input cover images *vs.* stego images

where MSE represents Mean Squared Error.

$$UACI = \frac{1}{p\ x\ q}\sum p, q \frac{|C\_Image(i,j) - S\_Image(i,j)|}{255} * 100\%, \tag{3}$$

$$NPCR = \frac{\sum p, q\ D(p,\ q)}{p\ x\ q}, \tag{4}$$

$$D(p,\ q) = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

$$D(p,\ q) = \{1 \text{ if C\_Image (i, j)} \neq \text{S\_Image(i, j)} | 0 \text{ if C\_Image (i, j)} = \text{S\_Image(i, j)}\} \quad (5)$$

where C_Image and S_Image represent the Cover and Stego images, respectively, the symbols 'p' and 'q' represent the images' dimensions. The parameters 'i' and 'j' represents the pixel locations on the images.

The metrics MSE, PSNR, NPCR, and UACI for different cover and stego image dimensions with varying contour sizes are computed to prove the efficiency of the chosen approach. The MSE and PSNR values for the collection of input cover images with different dimensions are shown in Tables 3–5 shows the results of the NPCR and UACI tests that were performed. Figs. 7 and 8 show the evolution of the nominated method's MSE and PSNR values on various image sizes. The proposed approach was compared with various existing steganography models [7] for embedding secret Content, which is listed in Table 6, and graphical Content is shown in Fig. 9. According to the findings, the observed experimental values are close to the theoretical ideal values. As a result, the suggested embedding approach can effectively shield the hidden Content from ordinary perception.

Table 3: MSE for various stego image dimensions with different contour sizes

Input image	MSE		
	128 × 128	256 × 256	512 × 512
Head	0.0540	0.0669	0.0880
Skull	0.0601	0.0687	0.0876
Chest	0.0549	0.0643	0.0780
Hand	0.0573	0.0691	0.0796

Table 4: PSNR for various stego image dimensions with different contour sizes

Input image	PSNR (dB)		
	128 × 128	256 × 256	512 × 512
Head	61.18	67.03	68.69
Skull	60.29	65.91	67.31
Chest	59.57	66.74	63.62
Hand	57.46	62.10	65.98

Table 5: NPCR and UACI computation between the cover and stego Images

Cover image (512 × 512)	Stego image (512 × 512)	NPCR (%)	UCI (%)
Head	Head	99.8062	32.7691
Skull	Skull	99.8120	32.8918
Chest	Chest	99.7925	33.3701
Hand	Hand	99.8012	33.5728

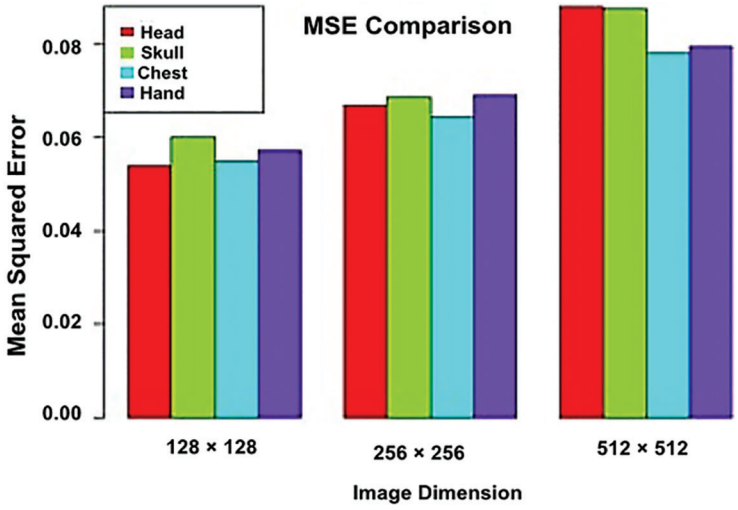

Figure 7: MSE of the anticipated scheme with distinct image dimensions

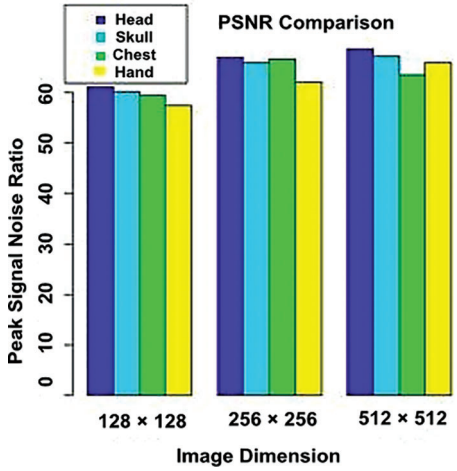

Figure 8: PSNR of the anticipated scheme with distinct image dimensions

Table 6: Comparison of secret stream embedding practices

Input Image 512 × 512	PSNR VALUES [7]			
	Manikandan et al. scheme [7]	Manikandan et al. scheme [7]	Manikandan et al. scheme [7]	Proposed Method
Head	54.23	61.89	62.14	68.69
Skull	53.92	59.32	63.29	67.31
Chest	53.56	63.46	61.65	63.62
Hand	57.46	60.56	62.72	65.98

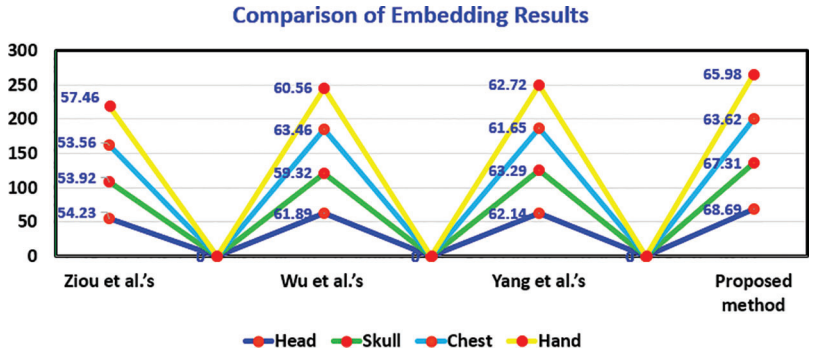

Figure 9: Comparison of the nominated scheme with existing outcomes

5 Conclusion

The nominated steganographic model gives an ameliorated scheme using Contours and K-Means clustering on digital images to accomplish secret Content (from a medical client) hiding on all levels of the color image with dimension 512 * 512, according to our provided method and its investigational observations to generate a stego image for transmission. The model generates a stego image with the secret Content, and the novelty of the proposed scheme is evaluated using the metrics Peak Signal Noise Ratio, Number of Pixels Change Rate (NPCR), and Unified Averaged Changed Intensity (UACI). Comparing the proposed model with existing schemes is encouraging to learn that the proposed scheme consistently outperforms existing standard schemes in terms of quality and other security-related activities. The proposed principle is very effective and ideal for information concealment in telemedicine applications. In simple terms, the proposed system satisfies all the requisites necessary for information security-related applications and efficiently performs the desired function. The future path of this study work would be to incorporate the presented model on videos with the deployment of Privacy preservation techniques.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. C. Huang, M. S. Hwang and L. Y. Tseng, "Reversible and high-capacity data hiding in high quality medical images," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 7, no. 1, pp. 132–148, 2013.

[2] B. K. Raghupathy, N. R. Kumar and N. R. Raajan, "An enhanced bishop tour scheme for information hiding," *International Journal of Applied Engineering Research*, vol. 9, no. 1, pp. 145–151, 2014.

[3] M. A. El-Bendary, "FEC merged with double security approach based on encrypted image steganography for different purpose in the presence of noise and different attacks," *Multimedia Tools and Applications*, vol. 76, no. 24, pp. 26463–26501, 2017.

[4] S. Prasad and A. K. Pal, "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing," *Royal Society Open Science*, vol. 4, no. 4, pp. 1–14, 2017.

[5] K. Sathish Shet, A. R. Aswath, M. C. Hanumantharaju and X. Z. Gao, "Design and development of new reconfigurable architectures for LSB/multi-bit image steganography system," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13197–13219, 2017.

[6] N. Naqvi, A. T. Abbasi, R. Hussain, M. A. Khan and B. Ahmad, "Multilayer partially homomorphic encryption text steganography (MLPHE-TS): A zero steganography approach," *Wireless Personal Communications*, vol. 103, no. 2, pp. 1563–1585, 2018.

[7] G. Manikandan, R. Bala Krishnan, N. Rajesh Kumar, D. Narasimhan, A. Srinivasan *et al.,* "Steganographic approach to enhancing secure data communication using contours and clustering," *Multimedia Tools and Applications*, vol. 77, no. 24, pp. 32257–32273, 2018.

[8] Z. Hua, J. Li, Y. Li and Y. Chen, "Image encryption using value-differencing transformation and modified ZigZag transformation," *Nonlinear Dynamics*, vol. 106, no. 6, pp. 3583–3599, 2021.

[9] M. Z. Konyar and S. Öztürk, "Reed solomon coding-based medical image data hiding method against salt and pepper noise," *Symmetry*, vol. 12, no. 6, pp. 1–16, 2020.

[10] F. Aziz, T. Ahmad, A. H. Malik, M. I. Uddin, S. Ahmad *et al.,* "Reversible data hiding techniques with high message embedding capacity in images," *PLoS One*, vol. 15, no. 5, pp. 1–24, 2020.

[11] J. Li, Z. Zhang, S. Li, R. Benton, Y. Huang *et al.,* "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology," *BMC Medical Informatics and Decision Making*, vol. 20, no. 14, pp. 1–16, 2020.

[12] M. Dalal and M. Juneja, "Steganography and steganalysis (in digital forensics): A cybersecurity guide," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5723–5771, 2021.

[13] M. Dalal and M. Juneja, "A survey on information hiding using video steganography," *Artificial Intelligence Review*, vol. 54, no. 8, pp. 5831–5895, 2021.

[14] R. Patel, K. Lad and M. Patel, "Study and investigation of video steganography over uncompressed and compressed domain: A comprehensive review," *Multimedia Systems*, vol. 27, no. 5, pp. 985–1024, 2021.

[15] W. B. Lin, T. H. Lai and K. C. Chang, "Statistical feature-based steganalysis for pixel-value differencing steganography," *EURASIP Journal on Advances in Signal Processing*, vol. 2021, no. 1, pp. 1–18, 2021.

[16] K. Kordov and S. Zhelezov, "Steganography in color images with random order of pixel selection and encrypted text message embedding," *PeerJ Computer Science*, vol. 7, pp. 1–21, 2021.

[17] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity," *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 23393–23417, 2021.

[18] G. Manikandan, R. Bala Krishnan, E. Preethivi, K. R. Sekar, R. Manikandan *et al.,* "An approach with steganography and scrambling mechanism for hiding image over images," *International Journal on Emerging Technologies*, vol. 10, no. 1, pp. 64–67, 2019.

[19] R. B. Krishnan, M. M. Raj, N. R. Kumar, B. Karthikeyan, G. Manikandan *et al.,* "Scrambling based riffle shift on stego-image to channelize the ensured data," *Intelligent Automation and Soft Computing*, vol. 32, no. 1, pp. 221–235, 2022.

[20] N. I. Yassin and E. M. El Houby, "Image steganography technique based on integer wavelet transform using most significant bit categories," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 1, pp. 499–508, 2022.

[21] V. Sabeti, M. Sobhani and S. M. H. Hasheminejad, "An adaptive image steganography method based on integer wavelet transform using genetic algorithm," *Computers and Electrical Engineering*, vol. 99, no. 107809, pp. 1–16, 2022.

[22] U. Pilania, R. Tanwar and P. Gupta, "An ROI-based robust video steganography technique using SVD in wavelet domain," *Open Computer Science*, vol. 12, no. 1, pp. 1–16, 2022.

[23] M. McCormick, S. Gerber, T. Czernuszewicz, R. Gessner, D. R. Chittajallu *et al.,* "Image-based methods for phase estimation, gating, and temporal superresolution of cardiac ultrasound," *IEEE Transactions on Biomedical Engineering*, vol. 66, no. 1, pp. 72–79, 2019. [Online]. Available: https://www.aylward.org/.