Hilbert convex similarity for Highly Secure Random Distribution of patient privacy steganography

Alzubaidy, Hussein K, Al-Shammary, Dhiah, Abed, Mohammed Hamzah, Ibaida, Ayman and Ahmed, Khandakar (2023) Hilbert convex similarity for Highly Secure Random Distribution of patient privacy steganography. IEEE Access, 11. pp. 115816-115826. ISSN 2169-3536

IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 1 October 2023, accepted 15 October 2023, date of publication 18 October 2023, date of current version 24 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3325754

RESEARCH ARTICLE

Hilbert Convex Similarity for Highly Secure Random Distribution of Patient Privacy Steganography

HUSSEIN K. ALZUBAIDY[1], DHIAH AL-SHAMMARY[1], MOHAMMED HAMZAH ABED[1,2], AYMAN IBAIDA[3], AND KHANDAKAR AHMED[3]

[1]Computer Science Department, University of Al-Qadisiyah, Al Diwaniyah 58002, Iraq
[2]Department of Telecommunication and Media Informatics, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, H-1111 Budapest, Hungary
[3]Intelligent Technology Innovation Laboratory, Victoria University, Melbourne, VIC 3011, Australia

Corresponding author: Mohammed Hamzah Abed (m.abed@edu.bme.hu)

This work was supported by Hungarian Electronic Information Service National Programme and the Intelligent Technology Innovation Laboratory (ITIL), Victorian University (VU), through the Digital Transformation of Small Medium Enterprises (SMEs) under Grant VUR20466.

ABSTRACT Based on Hilbert Random Secure Distribution, a novel data-hiding method for embedding secret information about the patient in a cover image MRI sample has been proposed. Least significant bit (LSB) and most significant bit (MSB) techniques are applied for the physical hiding. Medical images confidentiality suffers from potential attacks and tracing by an unauthorized access. Technically, distributing the secret text in a random way on the cover image is the core security function of the proposed model. In order to evaluate the performance of the proposed solution, three quality metrics: Peak signal to noise ratio (PSNR), Mean Square Error (MSE), percentage residual difference (PRD) and Structural Similarity Index measure (SSIM) were computed and compared on ten MRI images. Experimental results showed significant results in comparison with other models and reached average PSNR up to 61 db. Furthermore, the security analysis in case of 512 × 512 image samples show complex probability of distribution based on the Hilbert space model.

INDEX TERMS Patient privacy, steganography, LSB, MSB, MRI samples, Hilbert similarity.

I. INTRODUCTION

Secret text transfer over the network has increased significantly. Digital images represent the most cover material to hide secret text and send/receive over the networks [1]. This secure activity faces big challenges as a result of the potential number of hackers and organizations trying their best to intrude and obtain this private information [2], [3], [4]. Steganography technique is used to provide the protection of patient privacy and digital medical images [5], [6]. The basic components of steganography are covering image, secret text, and stego image [7], [8]. In addition, the main purpose of steganography avoids detection secret message and there are many algorithms in this fields [9], [10]. Least significant bit is one traditional method depend on spatial domain to hide secret information [11], [12]. Most significant bit (MSB) is an untraditional technique that targeting the high significant bits for hiding with low error [13]. To increase the efficiency of the steganography many researchers try to find the proper location to save the secret message for examples using the image edges [14], [15]. Furthermore, using health Images in such system are very interesting because they contain sensitive details to any change that may lead into false information [16].

The associate editor coordinating the review of this manuscript and approving it for publication was Yongjie Li.

A. MOTIVATION

With the great progress in information technology and communication sector Transmission of medicals, patient privacy is facing malicious attacks [17], [18]. Patient Privacy protection has been becoming an essential issue in the administration of Electronic Patient Records (EPRs) [19].

This paper discusses the problem of unauthorized access to medical images to provide high security for patient sensitive. In addition, we tried to find a mathematical space model to achieve a random distribution to increase the efficiency of the traditional steganography methods alongside a new model using the MSB location.

B. PROPOSED SOLUTION

In this paper, a new secure random distribution for the secret bits is proposed. Hilbert mathematical similarity is developed to provide secure random. This secure distribution would increase security and complicate the hacking process potentially. Furthermore, a key image is created based on a seed key exchanged between the sender and the receiver. Hilbert random distribution is completely based on the better similarity search between the cover and key images. Finally, both LSB and MSB are applied to physically hide the secret bits.

C. EVALUATION STRATEGY

In this paper, evaluation strategy has been developed for testing performance the proposed system. Technically, PSNR (Peak Signal to Noise Ratio), PRD (percentage residual difference) and MSE (Mean Squared Error) have been applied as quality metrics for evaluation and to investigate efficiency. In order to track the behavior of the proposed system and its outcomes, three MRI image sizes have been used. High results have been achieved by the proposed model especially when compared with other methods.

D. PAPER ORGANIZATION

The rest of this paper is organized as follow: section II presents the related works. proposed method is illustrated in section III. Furthermore, Experiments and results are demonstrated in section IV. Finally, the conclusion is explained in section V.

II. RELATED WORK

Rustad et al. [20] have addressed the improvement the stego image quality and minimize error rate to embed the message. An adaptive method has been proposed to choose the optimal pattern to reduce error bit that caused by embedding message and enhancement performance of the inverted LSB substitution method through use two bit and LSB pattern. Technically, PSNR, MSE, SSIM and Bit Error Rate (BER) have been computed and compared to investigate their results. This paper has used six container image like Lena and Baboon and ten MR samples image for evaluation. The best achieved result in this research are 56.053304 dB PSNR and 0.176664 MSE for hiding 8192 bytes' message. In addition, 58.197853 db. PSNR and 0.103816 MSE for hiding 5000 characters. On the other hand, although several of images have been tested, it's still the performance has not capacity on optimization is inefficiency to assist various of attacks on the stego image. Jayapandiyan et al. [21] have discussed hide secret text in cover image to improve cover image quality. In this paper, an enhanced Least Significant Bit (eLSB) embedding technique have been proposed to optimize secret message while embedding phase. The proposed algorithm has been used in spatial domain. In order to evaluate their proposed solution, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Root Mean Square Error (RMSE) have been computed and compared to investigate their results. This paper has used five sample of image like Lena and monalisa for evaluation. The best achieved result in this research are 77.2883 dB PSNR and 0.00122 MSE. On the other hand, few image samples are not enough to assure efficient the proposed algorithm. Abed [22] Have addressed problem unauthorized access of individual and organizations and secure transmission sensitive information patients over network from intruders. A highly efficient solution has been proposed based on fractal principle to protect patient's privacy and provide high secure via hiding information patient within MRI image by using steganography techniques such as LSB and MSB to prevent unauthorized entities access. Range and Domain is splited into blocks with same block size. fractal have been used as distribuer for secret messages into MRI host image. secret information has been done in random order depending on the fractal search. the original image blocks (Range) is calculated then search of block that is the most similar to the original and has the lowest root mean square error (RMS) in the domain blocks. The resulting block is the destination block in range that will be used to conceal sensitive information in the cover image. Moreover, indexes are used to hide block in appropriate location. In order to evaluate their proposed solution, PSNR and MSE have been computed and to investigate their results. Twenty-five image samples MRI have been used as main dataset for evaluation. The best obtained results in this research are 45.7097676 dB average PSNR and 1.74717184 average MSE for LSB steganography technique. in addition, 47.24152412 average PSNR and 1.22763264 average MSE for MSB steganography technique. Although images size in the mobile devices is small, the efficient proposed model may not be achieved when are applied on other fields and with larger sizes of image Because the stego image quality is affected significantly.

III. PROPOSED MODEL

This section is presented the description of the main concepts that are employed for the proposed models. Moreover, the Explanation of embedding and extracting information techniques.

A. HILBERT SIMILARITY MEASUREMENTS

The Hilbert similarity measurements are applied for two vectors (X, Y). The maximum similarity measurement between two vectors are considered popular problem in many applications such as steganography [23]. In this paper, Hilbert similarity is proposed to find the better similarity as a way to assure random selection to hide the secret bits at. Therefore, and in order to solve this problem, the maximum similarity is measured between the cover image corresponding block of pixels with a selected block in the randomly generated image key [24]. Technically, block size is proposed to be eight pixels each. The distance is inverse of the similarity, if the distance increases, the similarity decreases. The purpose of this measurement is to determine the indexes of blocks from the image key (i, j). Hilbert convex similarity is defined by the following equations:

$$\mathrm{Sim}(X, Y) = ((X.Y) - \mathrm{Max}(X))/(\|X\|.\|Y\|) \tag{1}$$

$$(X.Y) = x1 \times y1 + x2 \times y2 \ldots\ldots\ldots xn \times yn \tag{2}$$

$$\|X\| = \sqrt{x1^2 + x2^2 + x3^2 \ldots\ldots\ldots + xn^2} \tag{3}$$

$$\|Y\| = \sqrt{y1^2 + y2^2 + y3^2 \ldots\ldots\ldots + yn^2} \tag{4}$$

where:

X and Y: - vectors, Max (X): - Maximum value in vector X.

$\|X\|$: - square root for summation of element X, $\|Y\|$: - square root for summation of element Y.

B. HILBERT RANDOM SECURE DISTRIBUTION

A random secure distribution of secret text has been proposed based on Hilbert similarity to protect patient privacy from unauthorized access. Cover image is split into RGB bands. We used the Red band as a map in Hilbert similarity search and the Green or Blue band as cover to hide secret text. The Red band is to determine the secret locations of block in the key image (i, j) – generated previous to the random distribution - based on Hilbert Convex set then start search in Key image of the block which is the most similar to original.

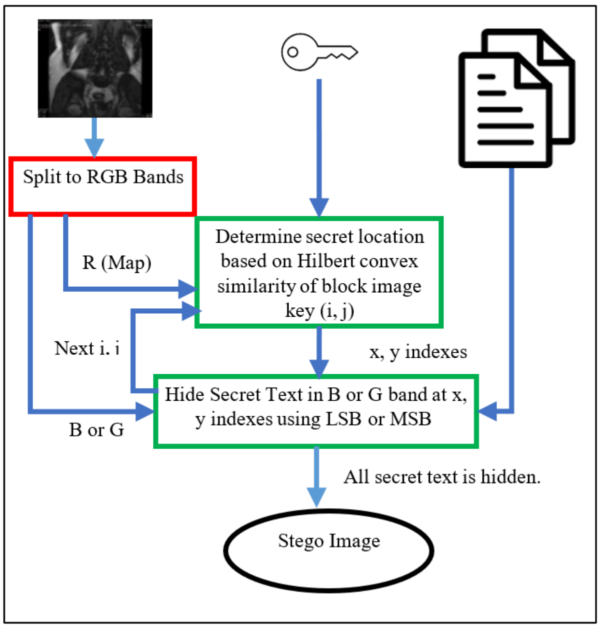

FIGURE 1. Proposed system for hiding operation.

The resulting block is called the destination block. Finally, indexes are taken and used to hide the secret text in Blue band that represent cover image. Fig 1. illustrates the hiding of secret text into cover image based on Hilbert similarity. Fig 2. illustrates the Extracting of secret text from stego image based on Hilbert similarity.

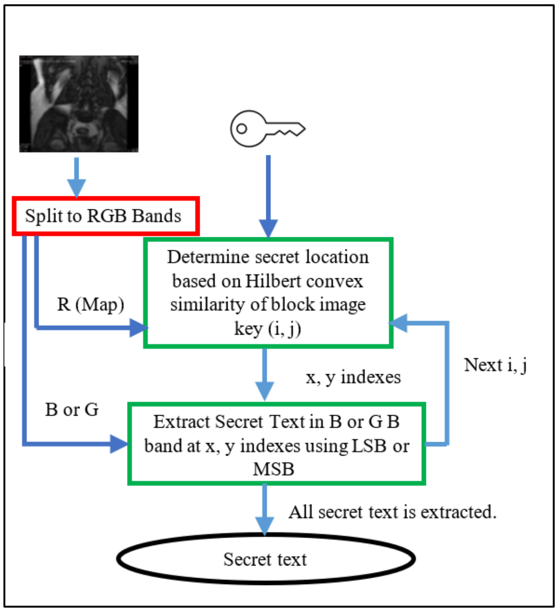

FIGURE 2. Proposed system for extracting operation.

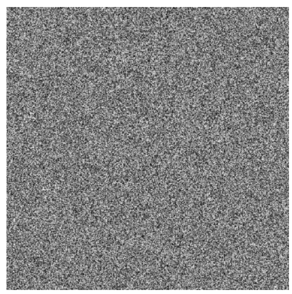

FIGURE 3. Key image samples of 250 ×250 dimension.

C. KEY IMAGE CREATION

Key image is created with the same dimensions of the original image. The key image matrix is applied as a random searching area for Hilbert in matching with the cover image in order to randomly locate secret positions for hiding information. Key image is constructed on two sides for sender and receiver in unpredictable way. Two secret Seeds are random numbers that predefined on the sender side and sent to the receiver sides using asymmetric encryption. Both sender and receiver have seed1 and seed2 in the same time. One-dimension array of Raw key(RK) mod 256 is generated using random generating function set by seed1. Another one-dimension array of Template Key(TK) mod TN (Total Number of pixels: WxH) is generated using the random generating function set by seed2. The Raw Key items (numbers) are swapped within the key itself by applying the Template items (numbers) as indexes for the RK items swap operations. The swapping process would probably change items positions twice or more that increase security significantly. Finally, the resultant RK array is transformed into two- dimensional array. Fig3 illustrate key image samples furthermore, Fig4 shows key image generation process for the sender and the receiver.

D. LEAST SIGNIFICANT BIT STEGANOGRAPHY TECHNIQUE LSB

It is the most common steganography method to embed the information bits into the cover image's least-significant-bit usually in a sequential order [25]. Due to the amplitude of the change is small, manipulating the least-significant bit does not produce a discernible difference. It is easily expected to the hackers to investigate secret bits from the cover least sequentially. This is the general weakness of steganography methods. In order to obtain secret bits, least significant bits are extracted from cover bands by binary masking operation.

E. MOST SIGNIFICANT BIT STEGANOGRAPHY TECHNIQUE MSB

MSB technique is considered as strong security, low computational complexity and causes little distortion to the host signal. This method is able to hide secret bit in a high significant bit with a resultant distortion that is equivalent to LSB. Initially, the cover high significant location values in fact belong to a special range of values selected by the method. Then, the value of the cover byte is mathematically shifted by Eq. 5.

$$S = Rmin + (M \ mod \ n) \tag{5}$$

where S is the resultant shifted value, Rmin is the starting value of the target special range, n is the length of the special range. Experimentally, we used Rmin = 127, Rmax = 129 and n = 3. The secret bit B will be hidden using S by Eq.6.

$$M_n = \begin{cases} M_o + (R_{max} - S) & if \ B = 1 \\ M_o - (S - R_{min}) & if \ B = 0 \end{cases} \tag{6}$$

where Mn is the new resultant value of the host byte, Mo is the original host byte, Rmin is the minimum value of the selected special range, Rmax is the maximum value of the selected special range and B is the secret bit. The fundamental idea behind of hiding process is to use the shifted value as a host to conceal the secret bit. Technically, the resulting value would be shifted back to its original level with little possible distortion. In order to extract the secret bit in the case of MSB, Eq. 5 is applied with the parameter Mn instead of Mo. Then, the secret bit would be extracted from the resultant Shift value (S) by the binary masking operation that targeting the secret cover bit position [26].

F. EMBEDDING MODEL

A steganography technique is applied either Least Significant Bit with Hilbert Random secure distribution (LSBHRSD) or

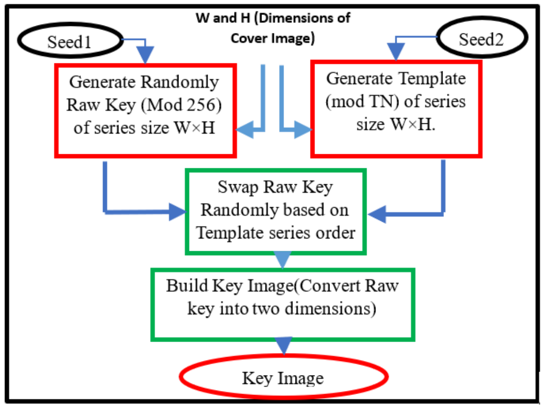

FIGURE 4. Key image generation using seed1 and seed2.

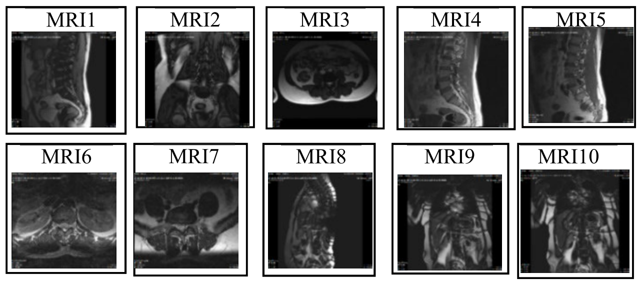

FIGURE 5. Original image MRI samples.

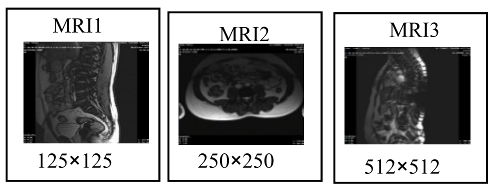

FIGURE 6. Stego-images obtained using (LSBHRSD) model.

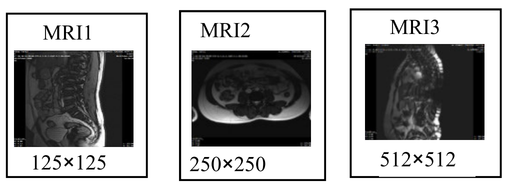

FIGURE 7. Stego-images obtained using (MSBHRSD) model.

Most Significant Bit with Hilbert Random secure distribution (MSBHRSD). Hiding locations for both approaches are randomly selected by the Hilbert similarity search inside the key image in matching with the cover block of pixels. Technically, the proposed model hides one bit in a byte at a time using either LSB or MSB. Therefore, each secret character (8 bits) would be hidden in 8 bytes. In Least significant bit and in order to hide one bit in byte, the cover byte would be binary masked with 254 (11 11 11 10) if the secret bit=0 otherwise it would be binary masked with 1 (00 00 00 01). In Most significant bit and in order to hide one bit in a byte, the cover

TABLE 1. Comperative performance of proposed method (LSBHRSD) and S. N. Abed et al [22] method of stego images with dimentions 125 × 125 and 1870 embeded characters.

Samples	S. N. Abed et al [22] method				The proposed method (LSBHRSD)			
	MSE	PSNR	PRD	SSIM	MSE	PSNR	PRD	SSIM
MRI1	1.809728	45.55467	–	–	0.04960370	61.17566	0.003273440	0.981199
MRI2	1.717120	45.78280	–	–	0.04926247	61.20564	0.003455198	0.986074
MRI3	1.750400	45.69943	–	–	0.04554437	61.54646	0.003641183	0.985122
MRI4	1.773376	45.64280	–	–	0.05315119	60.87567	0.002936438	0.987380
MRI5	1.812928	45.54700	–	–	0.05213461	60.95954	0.003004709	0.978780
MRI6	1.534400	46.27142	–	–	0.05302335	60.88613	0.003077421	0.999999
MRI7	1.712512	45.79447	–	–	0.05214886	60.95835	0.002909565	0.981118
MRI8	1.817792	45.53536	–	–	0.04972468	61.16508	0.003936846	0.982296
MRI9	1.739776	45.72587	–	–	0.04903502	61.22574	0.003390534	0.980221
MRI10	1.762048	45.67063	–	–	0.04971751	61.16571	0.003262279	0.999999
Avg	1.743008	45.72245	–	–	0.05033500	61.11640	0.003289000	0.986219

TABLE 2. Comparative performance of proposed method (LSBHRSD) and S. N. Abed et al [22] method of stego images. with dimentions 250 × 250 and 7500 embeded characters.

Samples	S. N. Abed et al [22] method				The proposed method(LSBHRSD)			
	MSE	PSNR	PRD	SSIM	MSE	PSNR	PRD	SSIM
MRI1	1.977360	45.16994616	–	–	0.04662550	61.44457	0.003154056	0.992342059
MRI2	1.887008	45.37306620	–	–	0.04665039	61.44225	0.003349906	0.990883344
MRI3	1.926112	45.28398824	–	–	0.04567461	61.53405	0.003619436	0.992545672
MRI4	1.896288	45.35176064	–	–	0.05345755	60.85071	0.002925908	0.988431678
MRI5	2.029440	45.05704145	–	–	0.05319807	60.87185	0.003013199	0.988766028
MRI6	1.699856	45.82668228	–	–	0.05363532	60.8363	0.003073508	0.999999492
MRI7	1.870224	45.41186735	–	–	0.05375794	60.82638	0.002937083	0.981298896
MRI8	1.948480	45.23384408	–	–	0.04636779	61.46864	0.003761495	0.991888482
MRI9	1.918208	45.30184663	–	–	0.04617405	61.48682	0.003278387	0.999999305
MRI10	1.942992	45.24609348	–	–	0.04643177	61.46265	0.003146021	0.999999416
Avg	1.909597	45.32561	–	–	0.04919700	61.22242	0.003226000	0.992615437

byte would be shifted first using Eq.5 and hiding the secret bit using Eq.6.

G. INFORMATION EXTRACTION

In order to extract secret bits from the cover image, the receiver requires initially the values of seed1 and seed2. Then, the Key Image is generated by implementing the same technique applied on the sender side. Furthermore, the cover blocks of pixels are searched for the similarity with the key image using Hilbert measurements to locate the secret random order of the cover blocks. Finally, steganography bit extraction is applied by either LSB or MSB.

IV. EXPERIMENTS AND RESULTS

In this section, a dataset has been obtained by communicating the author Abed et al. [22]. Technically, the proposed model is tested and evaluated on ten image MRI samples of sizes 125 × 125, 250 × 250 and 512 × 512 as explained in Fig. 5. The stego image of LSBHRSD model is illustrated in Fig 6. Finally, Fig.7 shows the stego image of MSBHRSD model.

As Figure 8 illustrates a sample of the histogram in the case of MSBHRSD, clearly change are not notable.

In fact, payload capacity has not affected by applying Hilbert models alongside with LSB and MSB methods. Maximum payload capacity embedding size has been targeted in order to have fair quality evaluation. However, system complexity would be increased for both embedding and extracting secret message.

A. EVALUATION METRICS

In this section, several evaluation metrics are applied to evaluate our proposed system performance such as PSNR, PRD and MSE. The results of the evaluation include comparisons for the proposed model with other techniques. The metric quality is determined by computing Peak signal to noise ratio(PSNR), Mean Square Error (MSE) and

TABLE 3. Comperative performance of proposed method (LSBHRSD) and S. N. Abed et al [22] method of stego images with dimentions 512 × 512 and 32000 embeded characters.

Samples	S. N. Abed et al [22] method				The proposed method(LSBHRSD)			
	MSE	PSNR	PRD	SSIM	MSE	PSNR	PRD	SSIM
MRI1	2.036514282	45.04192901	–	–	0.04478258	61.61971	0.003051654	0.999999937
MRI2	1.877239227	45.39560740	–	–	0.04467173	61.63047	0.003235901	0.999999937
MRI3	1.924274445	45.28813349	–	–	0.04405297	61.69105	0.003496561	0.999999924
MRI4	1.911251068	45.31762620	–	–	0.05481656	60.74169	0.002937118	0.999999932
MRI5	1.943630219	45.24466718	–	–	0.0545953	60.75925	0.003024283	0.999999946
MRI6	1.737731934	45.73097579	–	–	0.05402113	60.80517	0.003058007	0.99999992
MRI7	1.914749146	45.30968476	–	–	0.05485563	60.73859	0.002941099	0.999999936
MRI8	1.941310883	45.24985272	–	–	0.04404915	61.69143	0.003603053	0.999999943
MRI9	1.932186127	45.27031401	–	–	0.04410266	61.68616	0.003161734	0.99999993
MRI10	1.937366486	45.25868578	–	–	0.04418293	61.67826	0.003033824	0.999999937
Avg	1.915625	45.3107500	–	–	0.048413	61.30418	0.003154	0.999999934

TABLE 4. Comparative performance of proposed method (MSBHRSD) and S. N. Abed et al [22] method of stego images with dimentions 125 × 125 and 1870 embeded characters.

Samples	S. N. Abed et al [22] method				The proposed method(MSBHRSD)			
	MSE	PSNR	PRD	SSIM	MSE	PSNR	PRD	SSIM
MRI1	1.21856	47.27233443	–	–	0.1730302	55.74958	0.006113760	0.999998092
MRI2	1.20576	47.31819488	–	–	0.1682519	55.8712	0.006385499	0.999998627
MRI3	1.213568	47.29016245	–	–	0.1527259	56.29168	0.006667783	0.999998839
MRI4	1.220288	47.26618020	–	–	0.1807513	55.55999	0.005415082	0.999997556
MRI5	1.150400	47.52231488	–	–	0.1868587	55.41567	0.005688478	0.999997865
MRI6	1.13728	47.57212959	–	–	0.1791579	55.59845	0.005656805	0.999998608
MRI7	1.2416	47.19098657	–	–	0.1778001	55.63148	0.005372441	0.999998205
MRI8	1.249024	47.16509577	–	–	0.1729732	55.75101	0.007342633	0.999997823
MRI9	1.241344	47.19188211	–	–	0.1700507	55.82502	0.006313993	0.999998015
MRI10	1.239232	47.19927741	–	–	0.1679534	55.87892	0.005995989	0.999997985
Avg	1.211706	47.29886	–	–	0.172955	55.7573	0.006095	0.999998162

TABLE 5. Comparative performance of proposed method (MSBHRSD) and S. N. Abed et al [22] method of stego images with dimentions 250 × 250 and 7500 embeded characters.

Samples	S. N. Abed et al [22] method				The proposed method(MSBHRSD)			
	MSE	PSNR	PRD	SSIM	MSE	PSNR	PRD	SSIM
MRI1	1.326784	46.9028	–	–	0.1632809	56.00145	0.005902356	0.999998764
MRI2	1.315040	46.94141	–	–	0.1595647	56.10143	0.006195459	0.999999065
MRI3	1.320816	46.92238	–	–	0.1532035	56.27811	0.006628844	0.999999101
MRI4	1.320208	46.92438	–	–	0.1859117	55.43774	0.005456443	0.999998198
MRI5	1.246896	47.1725	–	–	0.1842818	55.47598	0.00560817	0.999998036
MRI6	1.247680	47.16977	–	–	0.1789682	55.60305	0.005614317	0.999998633
MRI7	1.379920	46.73226	–	–	0.1791608	55.59837	0.005361871	0.999998243
MRI8	1.357824	46.80237	–	–	0.1634848	55.99603	0.007063029	0.999998499
MRI9	1.373456	46.75266	–	–	0.1590756	56.11477	0.006085034	0.999998614
MRI10	1.370688	46.76142	–	–	0.1603907	56.07901	0.005847141	0.999998653
Avg	1.325931	46.9082	–	–	0.168732	55.86859	0.005976	0.999998581

percentage residual difference (PRD) after hiding as follow: Peak signal to noise ratio(PSNR)is commonly used to measure the quality of stego image. The higher value of PSNR is considered higher quality of image and can be calculated

TABLE 6. Comperative performance of proposed method (MSBHRSD) and S. N. Abed et al [22] method of stego images with dimentions 512 × 512 and 32000 embeded characters.

Samples	S. N. Abed et al [22] method				The proposed method(MSBHRSD)			
	MSE	PSNR	PRD	SSIM	MSE	PSNR	PRD	SSIM
MRI1	1.3358383	46.87326	–	–	0.1552551	56.22034	0.005682033	0.999999827
MRI2	1.3401718	46.85920	–	–	0.1534092	56.27229	0.005996593	0.999999784
MRI3	1.3202171	46.92435	–	–	0.1469943	56.4578	0.006387101	0.999999817
MRI4	1.3250885	46.90835	–	–	0.1901397	55.34008	0.005470184	0.999999869
MRI5	1.2719269	47.08618	–	–	0.1901526	55.33978	0.005644117	0.999999861
MRI6	1.3478355	46.83443	–	–	0.1838030	55.48728	0.005640699	0.99999985
MRI7	1.3976898	46.6767	–	–	0.1819690	55.53083	0.005356706	0.999999884
MRI8	1.3824539	46.7243	–	–	0.1523289	56.30298	0.00670028	0.999999804
MRI9	1.3937263	46.68903	–	–	0.1522143	56.30625	0.00587382	0.999999788
MRI10	1.3832588	46.72177	–	–	0.1529645	56.2849	0.00564493	0.999999827
Avg	1.349821	46.82976	–	–	0.165923	55.95425	0.00584	0.999999831

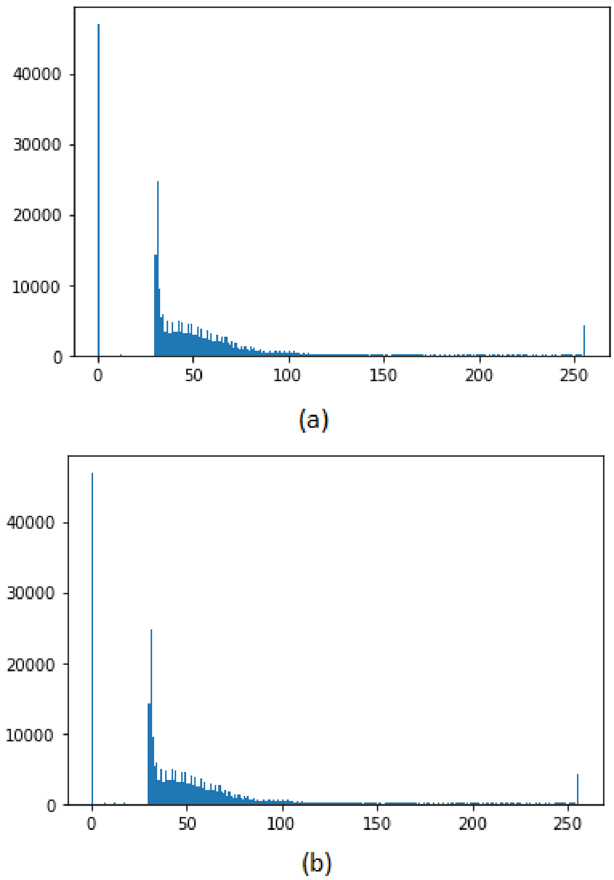

FIGURE 8. Histogram of (a) original image (b) Stego-images obtained using (MSBHRSD) model 512 ×512 dimension.

by the formula:

$$PSNR = 10.log_{10}(\frac{Max^2}{MSE}) \tag{7}$$

where Max: the maximum possible pixel value of the image.

MSE represents the Mean Square Error between cover image and stego image. Lower value of MSE implies lower error and lower distortion in the stego image and is defined as:

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i=0}}^{\mathrm{M-1}} \sum_{\mathrm{j=0}}^{\mathrm{N-1}} [\mathrm{I(i, j)} - \mathrm{I'(i, j)}] \tag{8}$$

where M, N represent the dimensions of the image (number of rows and columns of the original MRI of input image sample).

I‘ (i, j) represented A stego MRI sample

I(i,j)-I‘(i,j): is the difference between MRI image sample before and after the steganography

Percentage Residual Difference (PRD) is used to evaluate the different between the original image and image after hiding,where it is used to assess the image quality after embedding text and it is computed by equation number 9.

$$PRD = \sqrt{\frac{\sum_{i=1}^{N} (xi - yi)\, 2}{\sum_{i=1}^{N} xi^2}} \tag{9}$$

where x is original image, and y is the stego image. This metric has been used to assess the accuracy of images after hiding. It measures the discrepancy between the original cover image and the steganographic image by calculating the percentage difference between their pixel values. In other words, this metric is computed to indicate how much distortion has affected images by the hiding process.

Furthermore, Structural Similarity Index Measure (SSIM) utilities to measure the similarity between original images and stego images.

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_x\sigma_y + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{10}$$

Empirically, all the computed metrics have clearly shown significant efficiency of the proposed model. Furthermore, evaluation metrics have provided potential analysis in comparing the proposed model performance with previous models.

TABLE 7. Comparisons of results on PSNR and MSE of proposed model versus other techniqueS (LSB and MSB) OF SET different of images in 128*128 size and 1870 embeded characters.

Samples	The proposed method(LSBHRSD)		LSB		The proposed method(MSBHRSD)		MSB	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
MRI1	0.0496037	61.17566	0.0506045	60.2365	0.1730302	55.74958	0.18301	53.786
MRI2	0.04926247	61.20564	0.0492689	62.2454	0.1682519	55.8712	0.171934	54.321
MRI3	0.04554437	61.54646	0.04654468	61.87971	0.1527259	56.29168	.016321	55.567
MRI4	0.05315119	60.87567	0.054143	61.54371	0.1807513	55.55999	0.189793	55.2326
MRI5	0.05213461	60.95954	0.0534232	61.2354	0.1868587	55.41567	0.19124	55.3421
MRI6	0.05302335	60.88613	0.053897	61.2871	0.1791579	55.59845	0.18765	55.6901
MRI7	0.05214886	60.95835	0.052967	61.1534	0.1778001	55.63148	0.186801	55.7321
MRI8	0.04972468	61.16508	0.048456	61.7898	0.1729732	55.75101	0.179852	55.6321
MRI9	0.04903502	61.22574	0.0502345	61.8954	0.1700507	55.82502	0.17987	54.7632
MRI10	0.04971751	61.16571	0.0499123	61.98651	0.1679534	55.87892	0.17783	55.9876

TABLE 8. Comparisons of results on PSNR and MSE of proposed model versus other techniques (LSB and MSB) of set different of images in 256*256 size and 7500 embeded characters.

Samples	The proposed method(LSBHRSD)		LSB		The proposed method(MSBHRSD)		MSB	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
MRI1	0.0466255	61.44457	0.047531	61.1237	0.1632809	56.00145	0.160921	54.9852
MRI2	0.04665039	61.44225	0.048123	61.2151	0.1595647	56.10143	0.16098	55.87331
MRI3	0.04567461	61.53405	0.046761	60.5985	0.1532035	56.27811	0.15945	55.7832
MRI4	0.05345755	60.85071	0.054451	61.0971	0.1859117	55.43774	0.19573	55.7432
MRI5	0.05319807	60.87185	0.052171	61.6535	0.1842818	55.47598	0.192316	55.5463
MRI6	0.05363532	60.8363	0.053122	60.8363	0.1789682	55.60305	0.189762	55.45632
MRI7	0.05375794	60.82638	0.054944	60.8438	0.1791608	55.59837	0.181768	55.5672
MRI8	0.04636779	61.46864	0.0473791	60.9764	0.1634848	55.99603	0.17489	54.7864
MRI9	0.04617405	61.48682	0.04751	61.2382	0.1590756	56.11477	0.165645	55.6753
MRI10	0.04643177	61.46265	0.045972	60.9865	0.1603907	56.07901	0.162071	55.0987

TABLE 9. Comparisons of results on PSNR and MSE of proposed model versus other techniques (LSB and MSB) of set different of images in 512∗512 size and 32000 embeded characters.

Samples	The proposed method(LSBHRSD)		LSB		The proposed method(MSBHRSD)		MSB	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
MRI1	0.04478258	61.61971	0.0453258	60.9713	0.1552551	56.22034	0.16523	55.45221
MRI2	0.04467173	61.63047	0.0467332	60.9303	0.1534092	56.27229	0.155421	56.8983
MRI3	0.04405297	61.69105	0.0469721	61.9351	0.1469943	56.4578	0.159313	56.2351
MRI4	0.05481656	60.74169	0.053891	61.2934	0.1901397	55.34008	0.196521	54.8921
MRI5	0.0545953	60.75925	0.056598	61.05413	0.1901526	55.33978	.0203912	55.7682
MRI6	0.05402113	60.80517	0.0530642	60.70316	0.183803	55.48728	0.193502	54.1234
MRI7	0.05485563	60.73859	0.0558431	60.78545	0.181969	55.53083	0.182971	55.6532
MRI8	0.04404915	61.69143	0.043521	61.53143	0.1523289	56.30298	0.152458	55.7832
MRI9	0.04410266	61.68616	0.045198	60.6176	0.1522143	56.30625	0.1554124	55.1235
MRI10	0.04418293	61.67826	0.046284	60.97651	0.1529645	56.2849	0.1589632	56.01912

B. ANALYSIS AND COMPARISONS

According to the results shown in Tables 1,2,3,4,5 and 6, the proposed model has shown a high performance when compared with [S.N. Abed method]. These results have illustrated the comparisons with the measurements of PSNR, MSE and PRD for the proposed model with

[S.N. Abed method]. This evaluation has been applied for both LSB with Hilbert Random Secure Distribution (LSBHRSD) and MSB with Hilbert Random Secure Distribution (MSBHRSD). Technically, 1870, 7500 and 32,000 characters of data have been hidden into BMP image samples MRI for three dimensions 125 × 125, 250 × 250 and 512 × 512 respectively. Moreover, Table 10 illustrates the comparisons for proposed model with five recent different steganography. approaches using various images with size 512 × 512. Potentially, the proposed model has outperformed the other models with 61.30418 average of PSNR value and 0.048413 average of MSE.

TABLE 10. Comparisons of results on PSNR and MSE of proposed model versus other techniques of set different of images in 512*512 size.

Method	Average PSNR	Average MSE
Karakus et al.(2020) [27]	56.3936	0.149202
U. Subramaniyam et al .(2020) [28]	53.7713	0.2729
S. Heidari et al.(2017) [29]	55.61042	0.090322
R. Shanthakumari et al. (2020) [30]	47.92	0.845916
G. F. Siddiqui et al. (2020) [16]	49.33	0.77
Proposed model	61.30418	0.048413

C. SECURITY ANALYSIS

With the aim to evaluate the security strength of the suggested system, probability for each function in the system are computed. Probability for each stage of the system has been calculated as:

- Possibility of the first step of the key image creation is (seed).
- The data type of seed in our proposed system is 4 bytes, then the Possibility of seed1 is $2^{32} = 4294967296$, Possibility of seed2 is $2^{32} = 4294967296$.
- Total probability of seed=4294967296 × 4294967296 =1.84467441E+19

To compute the possibility of the key image creation, we tested the large image.

- N_1 is supposed for large image, if the image being used is 512 × 512, then $N_1 = 262144$.
- Each sample in large image has the possibility of changing index of 262144, therefore: Total probability of this case would be:

$$PN1 = N_1 * N_1 \tag{11}$$

PN1=68719476736.

- To compute the probability of first array and second array.

$$S_1 = (s_a * img_{size}) + (s_b * img_{size}) * (img_{size} * img_{size}) \tag{12}$$

where s_a, s_b is seed 1 and seed 2 respectively, and img_{size} is the image size from height * weight.

$$S1 = (4294967296 \times 262144) + (4294967296 \times 262144) * (262144 * 262144) = 1.54742504910672E + 26$$

Furthermore, the analysis of key image possibility as we consider the large sample of 512 × 512, can by calculated as following:

$$\begin{aligned} key_{img} &= S_1 + PN1 \\ \text{Key img} &= 1.54742504910672\text{E} + 26 + 68719476736 \\ &= 1.55E + 26 \end{aligned} \tag{13}$$

The calculation of possibility for Hilbert model based on 512 × 512 image dimension $N_1 = 262144$, Possibility generated by Hilbert similarity distribution is depend on the total number of segmented blocks. each block has the potential to match any position or any other block found inside the key image. Therefore, the possibility for each Hilbert block is equal to the total number of blocks. The block size in our suggested approach is 8, making number of block (T) is based on size of image.

$$\begin{aligned} T &= N_1/8 \\ \text{T} &= 262144/8 = 32,768 \end{aligned} \tag{14}$$

Finally, the total system possibility will be multiplication of key image possibility by Hilbert possibility. In same context by using Hilbert's distribution the complexity of find the hiding place are increased in high manner.

D. HIDING SECRET TEXT ANALYSIS

The same medical document file has been used for each image dimension to evaluate the proposed model and compare it with the traditional steganography methods (LSB). These files contain the patient records and all the examination results. This document is generated randomly to fit the maximum capacity of the MRI images to investigate the worst scenario. MRI dataset consist of set of images in different dimensions starting from 128*128, 256*256 and 512*512. For each dimension set, there is a specific document to achieve the maximum embedding capacity. Table 1, 2, 3, 4, 5 and 6 shows the comparison between the proposed model and Abed [22] method by using same document file that include (1870 characters) in case of 128*128, (7500 characters) in 256*256 MRI images while the maximum number of characters was 32000 in 512*512 images set. Technically, embedding document size have changed several times in order to investigate the value of MSE at different stages.

V. CONCLUSION

In conclusion, a new and efficient data hiding method based on Hilbert Random secure distribution has been presented. Two steganography techniques are implemented: most significant bit (MSB) and least significant bit (LSB) to hide sensitive patient information into a cover image. The key

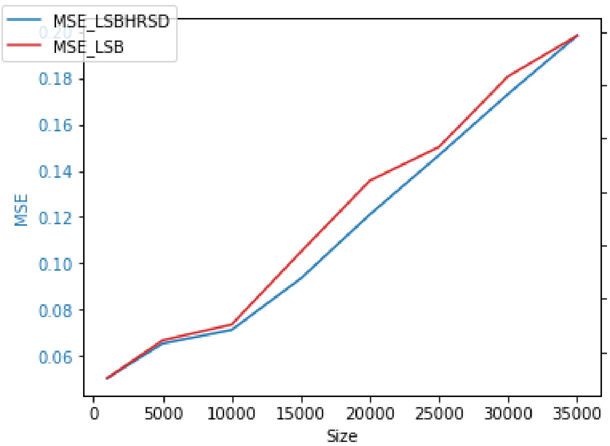

FIGURE 9. **MSE value according different document size of 512∗512 image dimension for LSB and LSBHRSD.**

image is constructed to be unexpected and support distributing secret bits in such a random and secure way to prevent the intruder's access. Technically, PSNR, MSE and PRD are computed for analysis and comparison process. Moreover, Ten MRI samples of 125 × 125, 250 × 250 and 512 × 512 dimensions are used as main dataset for evaluation. Evidently, the proposed model has shown better performance and security in comparison with other models.

REFERENCES

[1] P. Panwar, S. Dhall, and S. Gupta, "A multilevel secure information communication model for healthcare systems," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 8039–8062, Feb. 2021.
[2] R. F. Mansour and S. A. Parah, "Reversible data hiding for electronic patient information security for telemedicine applications," *Arabian J. Sci. Eng.*, vol. 46, no. 9, pp. 9129–9144, Sep. 2021.
[3] A. Abd and E. Hussein, "Design secure multi-level communication system based on duffing chaotic map and steganography," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 25, no. 238, pp. 238–246, 2022, doi: 10.11591/ijeecs.v25.i1.
[4] N. A. Zebari, D. A. Zebari, D. Q. Zeebaree, and J. N. Saeed, "Significant features for steganography techniques using deoxyribonucleic acid: A review," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, p. 338, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp338-347.
[5] S. Kaur, S. Bansal, and R. K. Bansal, "Image steganography for securing secret data using hybrid hiding model," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7749–7769, Feb. 2021.
[6] N. Ayub and A. Selwal, "An improved image steganography technique using edge based data hiding in DCT domain," *J. Interdiscipl. Math.*, vol. 23, no. 2, pp. 357–366, Feb. 2020.
[7] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity," *Multimedia Tools Appl.*, vol. 80, no. 15, pp. 23393–23417, Jun. 2021.
[8] A. H. Khaleel and I. Q. Abduljaleel, "Secure image hiding in speech signal by steganography-mining and encryption," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, p. 1692, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1692-1703.
[9] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Process.*, vol. 206, May 2023, Art. no. 108908.
[10] L. Yang, H. Deng, and X. Dang, "A novel coverless information hiding method based on the most significant bit of the cover image," *IEEE Access*, vol. 8, pp. 108579–108591, 2020.
[11] K. Praghash, C. Vidyadhari, G. NirmalaPriya, and R. Cristin, "WITHDRAWN: Secure information hiding using LSB features in an image," *Mater. Today, Proc.*, vol. 2021, p. 1, Jan. 2021.
[12] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K.-H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimedia Tools Appl.*, vol. 80, no. 13, pp. 20381–20401, May 2021.
[13] S. A. Mahdi, "An improved method for combine (LSB and MSB) based on color image RGB," *Eng. Technol. J.*, vol. 39, no. 1, pp. 231–242, Mar. 2021.
[14] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Graded fuzzy edge detection for imperceptibility optimization of image steganography," *Imag. Sci. J.*, vol. 2023, pp. 1–13, Jun. 2023.
[15] S. Rustad, I. M. S. De Rosal, P. N. Andono, and A. Syukur, "Optimization of cross diagonal pixel value differencing and modulus function steganography using edge area block patterns," *Cybern. Inf. Technol.*, vol. 22, no. 2, pp. 145–159, Jun. 2022.
[16] G. F. Siddiqui, M. Z. Iqbal, K. Saleem, Z. Saeed, A. Ahmed, I. A. Hameed, and M. F. Khan, "A dynamic three-bit image steganography algorithm for medical and e-Healthcare systems," *IEEE Access*, vol. 8, pp. 181893–181903, 2020.
[17] D. Wang, D. Chen, B. Ma, L. Xu, and J. Zhang, "A high capacity spatial domain data hiding scheme for medical images," *J. Signal Process. Syst.*, vol. 87, no. 2, pp. 215–227, May 2017.
[18] M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Med. Imag. Graph.*, vol. 29, no. 5, pp. 367–383, Jul. 2005.
[19] B. Suma and G. Shobha, "Privacy preserving association rule hiding using border based approach," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 23, no. 2, p. 1137, Aug. 2021, doi: 10.11591/ijeecs.v23.i2.pp1137-1145.
[20] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3559–3568, Jun. 2022.
[21] J. R. Jayapandiyan, C. Kavitha, and K. Sakthivel, "Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization," *IEEE Access*, vol. 8, pp. 136537–136545, 2020.
[22] S. N. Abed, "Mobile patients privacy protection by fractals secure distribution for LSB and MSB steganography," M.S. thesis, Mod. Univ. Bus. Sci. (MUBS), Lebanon Univ., Beirut, Lebanon, 2019.
[23] Y. C. Sagala, S. Hariyanto, Y. D. Sumanto, and T. Udjiani, "The distance between two convex sets in Hilbert space," in *Proc. AIP Conf.*, 2021, pp. 1–12.
[24] G. S. Yadav and A. Ojha, "Improved security in the genetic algorithm-based image steganography scheme using Hilbert space-filling curve," *Imag. Sci. J.*, vol. 67, no. 3, pp. 148–158, Apr. 2019.
[25] H. K. Alzubaidy, D. Al-Shammary, and M. H. Abed, "A survey on patients privacy protection with steganography and visual encryption," in *Expert Clouds and Applications*. Singapore: Springer, 2022, pp. 491–504.
[26] A. Ibaida, I. Khalil, and D. Al-Shammary, "Embedding patients confidential data in ECG signal for healthcare information systems," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol.*, Aug. 2010, pp. 3891–3894.
[27] S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," *Med. Hypotheses*, vol. 139, Jun. 2020, Art. no. 109691.
[28] G. V. K. Murugan and R. U. Subramaniyam, "Performance analysis of image steganography using wavelet transform for safe and secured transaction," *Multimedia Tools Appl.*, vol. 79, nos. 13–14, pp. 9101–9115, Apr. 2020.
[29] S. Heidari and E. Farzadnia, "A novel quantum LSB-based steganography method using the gray code for colored quantum images," *Quantum Inf. Process.*, vol. 16, no. 10, Oct. 2017.
[30] R. Shanthakumari and S. Malliga, "Retraction note: Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools Appl.*, vol. 82, no. 20, p. 31865, Aug. 2023.

HUSSEIN K. ALZUBAIDY was born in Shamiya, Al-Qādisiyyah, Iraq, in 1992. He received the B.S. and M.S.C. degrees in computer science from Al-Qadisiyah University, Iraq. His research interests include information security and networks, cryptography, digital communications, and computer networks.

DHIAH AL-SHAMMARY received the Ph.D. degree in computer science from RMIT University, in 2014. He was with several universities in both Iraq and Australia. He was with some silicon valey based companies, such as Optcts and AgilePQ. He has published with his Australian-USA Team a potential patent for designing new post-quantum data encryption with high performance. He has several publications at highly reputed venues. His research interests include data security and privacy, clustering techniques, classifications methods, optimization, and networking.

MOHAMMED HAMZAH ABED was born in Al Diwaniyah, Iraq. He received the B.Sc. degree in computer science from the University of Al-Qadisiyah, Iraq, in 2008, and the M.Sc. degree in computer science from B.A.M. University, India, in 2011. He is currently pursuing the Ph.D. degree in informatics with the Budapest University of Technology and Economics (BME). Alongside his academic pursuits, he is also an Assistant Professor with the Department of Computer Science, University of Al-Qadisiyah. His current research interests include medical image processing, speaker verification, machine learning, applying deep learning techniques to medical image analysis, and forensic voice comparison.

AYMAN IBAIDA received the Ph.D. degree in computer science and IT from RMIT University, Australia, in 2014. He was a Lecturer with the Computer College, Dubai, from 2006 to 2008. He was a Technical Lead with AgilePQ Australia Ltd., and a Co-Founder of EyeCura Pty Ltd. He is currently a Lecturer with Victoria University. His research interests include AI and machine learning in biomedical applications, diagnoses, patient health records security, and cyber security in healthcare systems.

KHANDAKAR AHMED received the bachelor's degree, the M.Sc. degree in networking and e-business centred computing (NeBCC) under the joint consortia of the University of Reading, U.K.; the Aristotle University of Thessaloniki, Greece; and the Charles III University of Madrid (UC3M), Spain, in 2011, and the Ph.D. degree from RMIT, in 2015. He started his career as a Full-Stack Developer and later switched to the academy by joining his alma mater as a Lecturer, in 2007. He taught at several universities in Europe and Australia and was a Postdoctoral Research Fellow with RMIT, in 2015 and 2016, before joining Victoria University, in 2017. He is currently a Senior Lecturer in IT with the College of Engineering and Science, Victoria University. He has extensive industry engagement as a Chief Investigator in multiple research projects related to the Internet of Things, smart cities, machine learning, cybersecurity, and biomedical informatics. He received substantial industry funding over the last five years collaborating with industries and local, state and federal governments in solving contemporary social problems using intelligent technologies.