Verifiable Privacy Preservation Scheme for Outsourcing Medical Image to Cloud Through ROI Based Crypto-Watermarking

Chuan Zhou *, Yi Zhou , Xinghan An , Yan Liu , Min Wang , XiangZhi Liu

Posted Date: 21 September 2023

doi: 10.20944/preprints202307.1435.v2

Keywords: sharing secret; data outsourcing; reversible watermarking; chaotic map

Article

Verifiable Privacy Preservation Scheme for Outsourcing Medical Image to Cloud through ROI Based Crypto-Watermarking

Chuan Zhou [1,*], Yi Zhou [2], Xinghan An [3], Yan Liu [4], Min Wang [5] and XiangZhi Liu [2]

[1] Tianjin University, Tianjin, China;
[2] Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan, China;
[3] College of Environmental Science and Engineering, Beijing Forestry University, Beijing
[4] Inspur software Co., Ltd.
[5] The party school of cpc jinan municipal committee
* Correspondence: zhouchuan@tju.edu.cn

Abstract: A novel verifiable privacy preservation scheme for outsourcing medical image to cloud through ROI based crypto-watermarking is proposed in the paper. In the proposed scheme, data owner firstly carries out substitution of S-box for the region of interest (ROI) of medical image, and then separates the image into 4 most significant bits (MSBs) plane and 4 least significant bits (LSBs) plane images. Secondly, the hash value of ROI is embedded into the two separated bit plane images using reversible watermarking algorithm. Lastly, some selected hash values are transformed into the initial parameters of chaotic maps, and the two sharing secrets, which are produced through chaos based encryption algorithm, are finally outsourced to two different cloud servers. For authorized users, they can get shares from different cloud servers, and then can losslessly recover the original medical image through a series of decryption operations and extraction of watermarking. Furthermore, the users can verify whether the original image is completely reconstructed or not, they even can locate the tampered parts inside ROI if anyone of the sharing secrets is damaged. Some experiments analyses and comparisons are given to show the security and effectiveness of proposed scheme.

Keywords: sharing secret; data outsourcing; reversible watermarking; chaotic map

1. Introduction

With the explosive growth in the amount of multimedia content, as one of the most important computing paradigms emerged in recent years, cloud computing has become an effective means for user to manage data. By outsourcing the data to the cloud server, the large enterprises as well as individual users can dynamically increase their storage space without buying any storage devices, and it also can reduce the costs for purchasing hardware equipment, managing enterprise data and maintaining the system [1–3].

While enjoying the abundant storage and computation resources for cost saving and flexibility, the security and privacy of outsourced data also become great concerns for people. Because the cloud service providers (CSPs) are considered ''honest but curious'' under cloud environment, and many popular social network providers also exploit the outsourced personal image data to conduct behavioral advertising and preference analyses for improving user experience, some attackers also want to find the valuable information from the network. To provide privacy and security guarantees, people have proposed many kinds of schemes to protect the sensitive multimedia data outsourced to the cloud [4–6].

At present, encryption and digital watermarking are two widely used means for protection of images such as medical images in the cloud [7–15]. For the encryption scheme, Kanso et al. proposed a full and selective chaos-based image encryption scheme suitable for medical image encryption applications [9]. Fu et al. proposed medical encryption based on bit plane permutation and pixel

 doi:10.20944/preprints202307.1435.v2

substation [10]. Lima proposed fast medical images encryption scheme based on the cosine number transform [11]. For the watermarking algorithms, people usually apply reversible watermarking algorithm to embed watermarking into the medical image, the original image can be totally restored when the watermarking is extracted [12–14]. Moreover, some schemes can detect the tampers inside region of interest and recover original region of interest [14]. Regarding the above algorithms, encryption algorithms are effective and have better performance for protection of medical images, but they can't identify and locate the tampered position when the encrypted image is modified; digital watermarking algorithms based scheme can offset the defects of encryption algorithm, but watermarked image is visually the same as the original image, it is not suitable for privacy protection, especially not suitable for outsourcing the images to the cloud.

Based on the characteristics of the encryption and digital watermarking algorithms, people have proposed crypto-watermarking scheme by combining watermarking and encryption algorithm to protect image [16–24]. One way of using crypto-watermarking scheme is that image is firstly encrypted, and then watermarking is embedded in encrypted domain [16–21]. For example, Priyanka et al. proposed a reversible information hiding scheme in encrypted domain, this scheme can securely transmit the media information over cloud architecture and prove rightful ownership of media using Chinese Remainder Theorem (CRT) based secret sharing algorithm [18]. Zhang et al. presented a reversible data hiding in reversible image transformation domain [19]. Priyanka recently gave a reversible data hiding scheme based on Shamir's secret sharing for color images over cloud, the scheme permits the rightful owner to extract the information either directly from the cloud servers or after recovery of the media [20].

Another kind of crypto-watermarking scheme is that watermarking is firstly embedded into the original image, and then watermarked image is encrypted [22–25]. For example, Dalel Bouslimi et al. proposed a joint encryption/watermarking system for protection of medical images based on substitutive watermarking algorithm, the quantization index modulation and an encryption algorithm. The scheme can verify integrity of restored image even though the image is stored in encrypted form [23]. Sangita Zope-Chaudhari et al. showed a crypto-watermarking scheme by combining wavelet-based watermarking and multiplicative-transposition-based encryption to protect multispectral images [24]. Xiang et al. studied a crypto-watermarking scheme for resource-limited client, in the scheme, the client is responsible for embedding information, while cloud server implements encryption based on chaotic systems [25]. Recently, Gao et al. presented random grid and reversible watermarking based verifiable secret sharing scheme for outsourcing image into the cloud, in the scheme, original secret image is divided into some sub-images, and reversible watermarking is used for embedding hash value of the secret image into the image itself, then encryption are implemented to generate some sharing secrets, which are outsourced into the cloud, the scheme can restore the original secret image without any loss, and can verify the integrity of the restored image[26].

Medical images are a class of special images with specific characteristics and requirements. Any imperfects in image, especially in the region of interest (ROI) will result in misdiagnosis [27–29]. These strict specifications regarding the quality of medical images must be met when security and privacy are considered. In this paper, a novel verifiable privacy preservation scheme for outsourcing medical image to cloud through region of interest (ROI) based crypto-watermarking is proposed. In the scheme, data owner firstly calculates the hashes of the ROI blocks of medical image, and executes substitution of S-box for ROI and separation of bit plane. Secondly, data owner embeds the hashes into the separated bit plane images. Lastly, some hashes are transformed into the initial value and parameters of chaotic maps, and encryption for two bit plane images is implemented to get two sharing secrets, which are outsourced to the different cloud servers. For any authorized user who wants to access the image, he firstly gets secret key from the data owner, downloads the corresponding sharing secrets; and then he can decrypt the sharing secrets and extract the data embedded in the sharing secrets. Thus he can confirm whether the restored image is the same as the original one, and moreover, he can also locate the tampered parts if the sharing secrets are damaged. Large numbers of experiments show the effectiveness of proposed scheme.

 doi:10.20944/preprints202307.1435.v2

The highlights of the paper lie in the following points:

(1) Compared with state-of-the-art schemes, the proposed crypto-watermarking scheme for medical image can verify the integrity of recovered image; it can also identify the tampered blocks inside ROI. This is especially suitable for the application of outsourcing medical image to the cloud.

(2) In the proposed scheme, the sharing secrets have good performance of privacy protection. Attackers can't get any available information from the sharing secrets.

(3) The secret key of the scheme depends on image itself; different images use different secret keys. Damages to anyone of sharing secrets will affect the recovery of original image.

The rest of the paper is organized as follow: Section 2 introduces the reversible watermarking and S-box. Section 3 presents the proposed method in detail. The simulations and analyses are reported in Section 4. The conclusion is given in Section 5.

2. Preliminaries

In this section, some concepts and knowledge such as S-box and reversible watermarking used in the proposed scheme are first reviewed.

2.1. Reversible watermarking

Digital watermarking can be used for the copyright protection, tamper detection, traitor tracing of multimedia through embedding some specific data into the image [30–33]. Reversible watermarking, also known as lossless watermarking is a technique to embed the watermark into a digital content in a reversible way, the original multimedia can be totally restored when the digital watermarking is extracted, this characteristic makes it suitable for the protection of important multimedia data such as medical and military images. One of the most widely used algorithms is histogram shifting-based methods (HS) [32]; it is reviewed in the following.

For a gray image, the histogram of the image is first presented. Then the data pair (h_z, h_p) is found, where, h_p is a peak point of histogram, and h_z is a zero point in the histogram. The histogram shifting based watermarking algorithm can be implemented in the following steps.

(1) Scan all the pixels of the image, if the pixel value satisfies the condition

$$h_z + 1 \le p \le h_p - 1 \tag{1}$$

then, let $p = p - 1$, where, p is the value of the pixel.

(2) Watermarking embedding. Scan all the pixels, if the pixel value is equal to h_p, the watermarking is embedded according to formula (2)

$$\begin{cases} h_p = h_p - 1 & if\ w = 1 \\ h_p = h_p & if\ w = 0 \end{cases} \tag{2}$$

where, w is watermarking bit.

The process of watermarking extraction and restoration of the original image are given in the following.

(1) Watermarking extraction. Scan all the pixels of the watermarked image, if the pixel value is equal to h_p, then extracted watermarking bit is 0; if the pixel value is equal to $h_p - 1$, then bit 1 is extracted;

(2) Restoration of the original image. Scan all the pixels of the watermarked image, if the value of pixel is equal to $h_p - 1$, then, let add the pixel value by 1, this operation restores the peak point of the image. Next, the original image will be lossless restored by formula (3)

$$p = p + 1 \ \ if\ h_z \le p \le h_p - 2 \tag{3}$$

Figure 1 illustrates the process of HS based watermarking embedding. The distribution of pixels of image is given in the Figure 1(a). It can be seen that pixel value 133 is the peak point, and the 234 is the zero point. Then, shift the pixels between 134 and 233 to the right and it results in distribution of pixel as described in Figure 1(b). After the shifting, the adjacent pixel value (134) of peak point is changed into the zero point, as shown in Figure 1(c). Thus, the watermarking embedding can be

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

conducted through pixel value 133 and 134. Further, Figure 1(d) displays the histogram information embedding process more intuitively.

Pixel value	…	132	133	134	135		232	233	234	…
Quantity		356	457	356	244		123	12	0	…

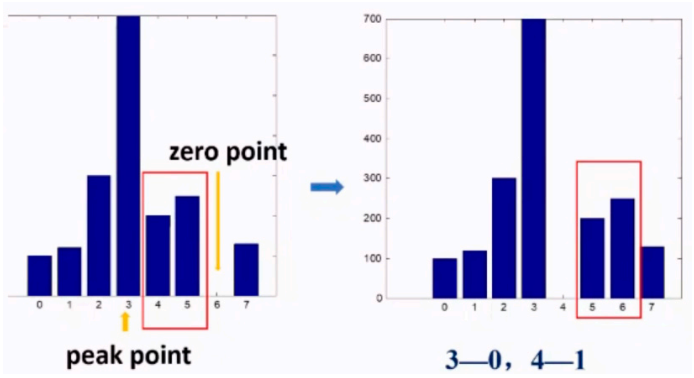
(a)

Pixel value	…	132	133	134	135	…	232	233	234	…
Quantity		356	457	0	356	244	…	123	12	…

(b)

Pixel	…	132	133	134	135	…	232	233	234	…
Quantity		356	457	0	356	244	…	123	12	…

(c)



(d)

Figure 1. Example of HS based watermarking embedding (a) Example of find the peaks and zeros (b) Example of histogram translation (c) Example of histogram embedding (d) Histogram embedding method diagram.

2.2. S-boxes

Substitution boxes (S-boxes) are the most essential parts of modern cryptographic applications. S-boxes are multi-input and multi-output boolean functions that map binary input to binary output values [34]. S-boxes with high cryptographic features have been used in encryption to resist differential cryptanalysis. The Rijndael S-box shown in Table 1 is a square matrix, which the Advanced Encryption Standard (AES) crptographic algorithm is based on. In order to enhance the security of algorithm, the Rijndael S-box is used for substitution of pixel in the proposed scheme.

Table 1. Rijndael S-box with the size of 16 × 16.

Sbox	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
1	202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
2	183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
3	4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
4	9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
5	83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
6	208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
7	81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
8	205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

9	96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
10	224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
11	231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
12	186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
13	112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
14	225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
15	140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

3. Proposed scheme

In order to protect privacy of the data, data owner often encrypts data before it is outsourced to the cloud. Some roles based on real application for outsourced data management are data owner, authorized user and cloud server, as depicted in Figure 2.

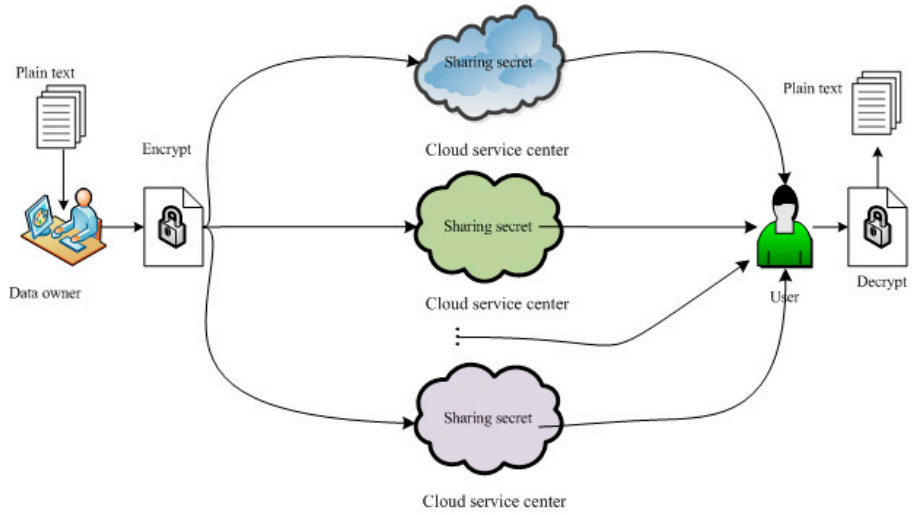


Figure 2. System model for outsourcing data.

Data owner: He has some set of files $C = (F_1, F_2, \cdots, F_n)$. He wants to outsource these files to the cloud server in the encrypted form. And he also hopes that these files can be searched by a series of keywords $= (w_1, w_2, \cdots, w_m)$. In order to protect the file from attacks, he hopes to create secure ranked searchable index from keyword and store them on the cloud server.

Authorized user: He hopes to get the files relevant to certain or some keywords submitted to cloud server, the cloud server selects the corresponding files, and he can download the files from the cloud, and then decrypt it.

Cloud server: It stores the files and keyword index. When it receives the request from the user, it can inquiry index and return the search results according to some ranked relevance criteria.

In this paper, what we concern is how to outsource the image to the cloud safely, such that for authorized user, he can verify the integrity of the file when he downloads the file. The detailed scheme is given in next subsections.

3.1. Generation of sharing secret

To generate the sharing secret, the following steps are followed to achieve the goal.

(1) Manually partition the original image into ROI and non-ROI sections, and the coordinate of upper left of the ROI is given by (x_1, y_1), and the coordinate in lower right is recorded by (x_2, y_2).

(2) Divide ROI into some no overlapping sub-blocks with the size of 16×16, the corresponding number of block is $m = \frac{(y_2 - y_1) \times (x_2 - x_1)}{256}$. Next, the 256-bits hash is calculated for every block. These hashes are represented by $H_1, H_2, \cdots, H_m$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

(3) Transform every $H_i, (i = 1,2,\cdots,m)$ expressed by $\hbar_1, \hbar_2, \cdots, \hbar_{256}$ into 128-bits by formula (4).

$$h_i' = h_i \otimes h_{i+128}, i = 1,2,\cdots,128 \tag{4}$$

(4) Conduct substitution of pixels value for the ROI using S-box. Firstly, for every pixel value p in ROI, extract its high 4-bits and low 4-bits, respectively, they can be named H_{bits} and L_{bits}. Next, replaces the pixel value of ROI with the value of S-box in the coordinate position of (H_{bits}, L_{bits}). H_{bits} stands for the row, and L_{bits}stands for column in the S-box. The generated image after S-box substitution is expressed by I_{SROI}.

(5) Bit plane separation. Separate the image I_{SROI} into two images $I_{SROI-MSB}$ and $I_{SROI-LSB}$, where, $I_{SROI-MSB}$ is generated by the most significant bits (MSBs), which is the high 4-bits of the I_{SROI}, and $I_{SROI-LSM}$ is generated by the least significant bits (LSBs), which is the low 4-bits of the I_{SROI}. The process of bit plane separation is depicted in Figure 3.

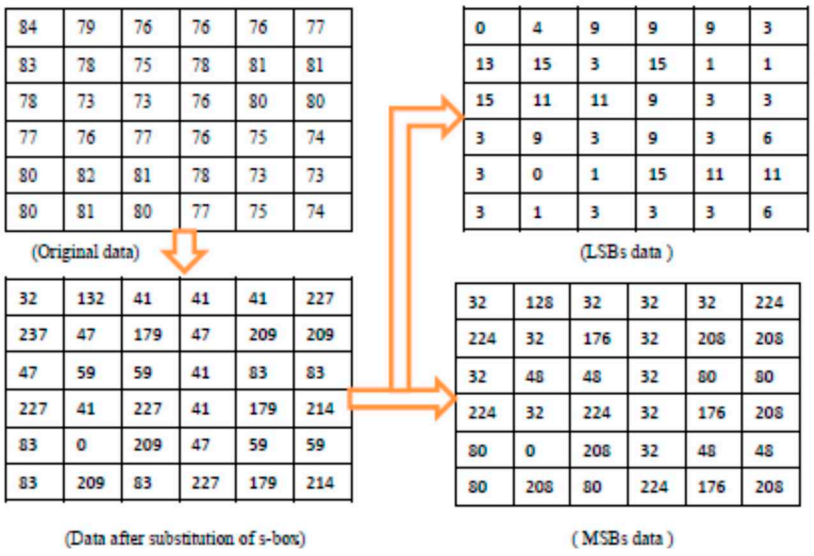


Figure 3. Example of separation for bit plane.

(6) Embed the hashes $H_i, i = 1,2,\cdots,m$ of 128 bits into the two images, $I_{SROI-LSB}$ and $I_{SROI-MSB}$ based on HS method. The produced images are labeled by $I_{SROI-LSB-HE}$ and $I_{SROI-MSB-HE}$.

(7) Select secret key for image diffusion. Select the number $t = \frac{(y_2-y_1)\times(x_2-x_1)}{512}$, the following steps are used to generate two sharing secret images.

1) Divide $H_{1,\ldots,t}$ of 128-bits, expressed by $h_1h_2\cdots h_{128}$ into two sections, every section has 64 bits, then convert $h_1h_2\cdots h_{64}$ into some integers, respectively.

$$\begin{cases} u = \hbar_1\hbar_2\hbar_3 \\ k = \hbar_4\hbar_5\hbar_6\hbar_7 \\ N_0 = \hbar_8\hbar_9\hbar_{10}\hbar_{11}\hbar_{12}\hbar_{13}\hbar_{14}\hbar_{15}\hbar_{16}\hbar_{17}\hbar_{18}\hbar_{19} \\ x_0 = 10^{-14} \times \hbar_{20}\hbar_{21}\cdots\hbar_{64} \end{cases} \tag{5}$$

Obviously,$u \in [0,7], k \in [0,15], N_0 \in [0,4095], x_0 \in [0,\ 0.35184372088831]$.Then, u, N_0 and k are transformed with the following constraints.

$$\begin{cases} u = u + 0.5212882 \ \text{ if } u = 0 \\ k = \begin{cases} k & 8 \le k \le 15 \\ k + 12 & 0 \le k < 8 \end{cases} \\ N_0 = \begin{cases} N_0 & 3000 \le N_0 \le 4096 \\ N_0 + 1000 & N_0 < 3000 \end{cases} \end{cases} \tag{6}$$

Next, iterate chaotic Sine-Sine system (SSS) defined in the formula (7) for $N_0 + N$ times, and then dispose these elements by formula (8).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

$$x_{n+1} = u \times sin(\pi \times x_n) \times 2^k - floor(u \times sin(\pi \times x_n) \times 2^k) \quad (7)$$

$$x_i = mod(\left(abs(x_i) - floor\left(abs(x_i)\right)\right) \times 10^{14}, 256), i = 1,2,\cdots, N_0 + N \quad (8)$$

Here, N is the number of pixel in image. $abs(x)$ stands for the absolute value of x. $floor(x)$ is equal to the value of x to the nearest integers less than or equal to x, $\mathrm{mod(x,y)}$ generates the remainder after division.

Lastly, arrange the last N integers from $N_0 + 1$ to $N_0 + N$ into a matrix A with the same size as that of the image to be diffused, where $A(i,j) = reshape[(N_0 + 1: N_0 + N), \sqrt{N}, \sqrt{N})$, here, $reshape$ represents the conversion of a one-dimensional array into a two-dimensional matrix *with size of* $\sqrt{N} \times \sqrt{N}$. For example, N=9 and one-dimensional array is (1,2,3,4,5,6,7,8,9), the matrix A=[1,2,3;4,5,6;7,8,9] with size of 3×3 is generated by the reshape process.

2) For other 64-bits $h_{65}h_{66}\cdots h_{128}$ of H_i, use the procedures as the same of 1) to generate a matrix B, here, the chaotic map used is Chebyshev-Chebyshev system (CCS) defined in formula (9)

$$x_{n+1} = cos(\,(u+1) \times arccos(\,x_n) \times 2^k - floor(cos(\,(u+1) \times arccos(\,x_n) \times 2^k) \quad (9)$$

The better performances of chaotic CCS and SSS for encryption can be found in Reference [35,36].

3) Obtain sharing secret from the diffusion of the $I_{SROI-MSB-HE}$ by the following diffusion equation.

$$I'_{\text{SROI-MSB-HE}}(i,j) = mod(\,I_{SROI-MSB-HE}(i,j) \oplus A(i,j),256) \otimes B(i,j) \quad (10)$$

where,$i = 1,2,\cdots L, j = 1,2,\cdots W$. W and L are the length and width of image, respectively. $\oplus$ is the arithmetic plus operator, and $\otimes$ is the bit-level XOR operator. The generated $I'_{SROI-MSB-HE}$ is one of the sharing secrets.

In the same way, the second sharing secret image can be derived using $H_{t+1,\ldots,m}$and $I_{SROI-LSB-HE}$. Then, the tow shares are outsourced to different cloud servers.

Figure 4. shows the detailed flowchart of generation of sharing secret.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

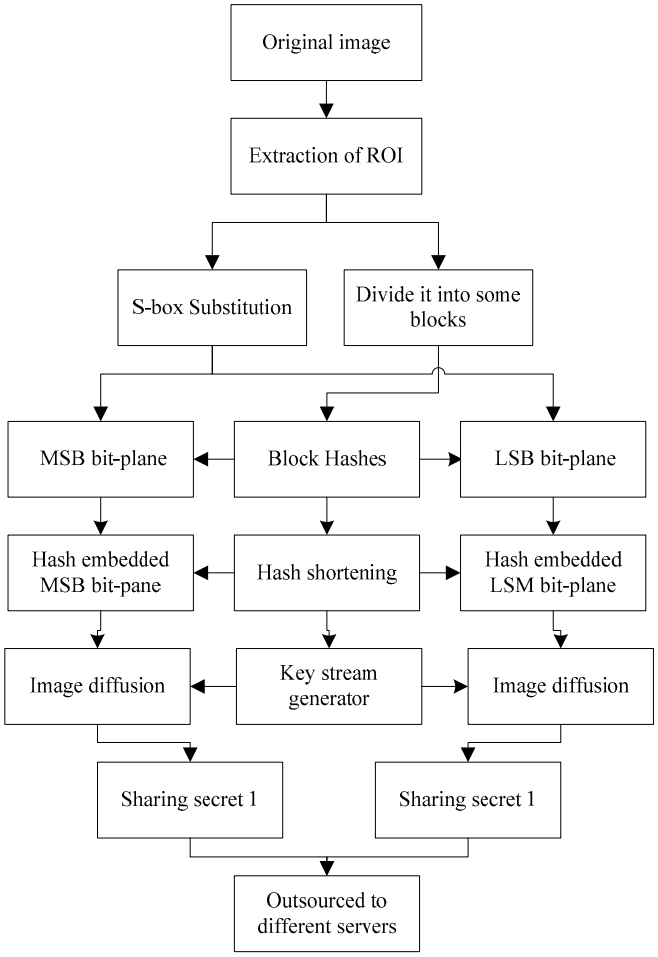


Figure 4. The flowchart of generation of sharing secret.

3.2. Restoration of original secret image

For authorized users, when they want to access the image from the cloud, the data owner will give them the secret key in a secret way. Then, the following steps are used to restore the original secret image.

(1) Download two sharing secrets S_1 and S_2 from two cloud servers.

(2) Use the same key as that used in the generation procedures of sharing secrets to generate matrices using chaotic maps (7) and (9). Then implements the inverse operation of formula (10) between the matrices and sharing secret, thus two images $I_i''', i = 1, 2$ with the size of $L \times W$ are produced.

(3) Extract the watermarking $H_1', H_2', \cdots, H_m'$ from $I_i''', i = 1,2$ using HS based reversible watermarking algorithm to get two images $I_i'', i = 1,2$, and then produce one image I''using the formula $I'' = I_1'' + I_2''$.

(4) Implement inverse S-box replacement of ROI for image I'' to produce image *I*.

(5) Use the same method as Step 2 in the phase of generation of sharing secret to obtain $H_1'', H_2'', \cdots, H_m''$. And then compare these hash values with the watermarking data extracted in Step 3, thus, we can locate whether the corresponding block in ROI is tampered. Moreover, the position of tampered parts can be located.

4. Experimental results and discussions

The experiment was conducted by MATLAB version 12b. The medical data from 6,970 fully sampled brain MRIs obtained on 3 and 1.5 Tesla magnets. In this section, six 256-grey scale test images with the size of 512×512 are given in Figure 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

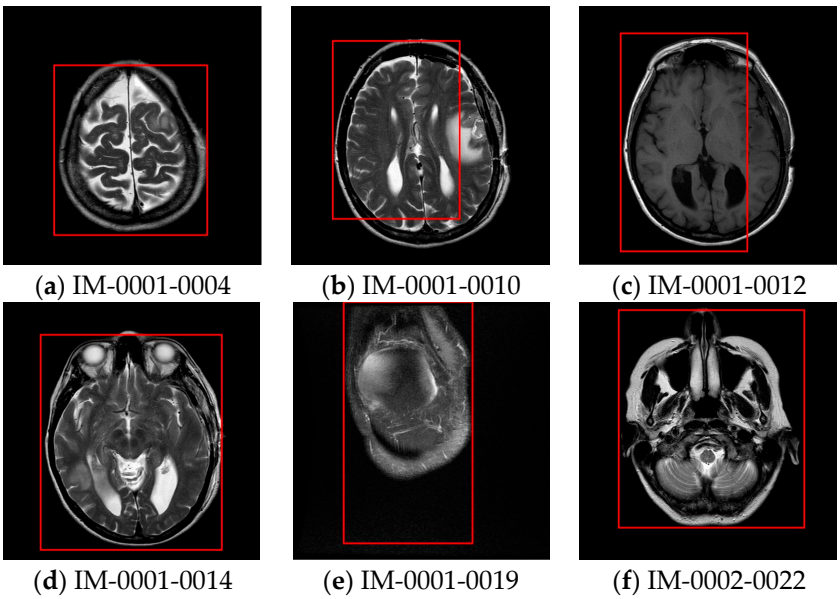


Figure 5. 256-grey scale test images and the corresponding ROI.

4.1. Experimental results

Firstly, the ROI is described for every test image, the coordinates of upper left and lower right of test image are given in Table 2. As an example, for image IM-0001-0012, the separated bit plane image of MSBs and LSBs following the S-box substitution are given in Figure 6 (a-b). Figure 6(c-d) displays the two sharing secrets outsourced to the cloud.

Table 2. The coordinate of ROI for different test images.

Images for test	Coordinate of upper left of ROI	Coordinate of lower right of ROI
IM-0001-0004	(102,118)	(405,453)
IM-0001-0010	(83,70)	(434, 469)
IM-0001-0012	(83,55)	(434,486)
IM-0001-0014	(75,66)	(426,481)
IM-0001-0019	(102,1)	(357,480)
IM-0002-0022	(81,17)	(448,448)

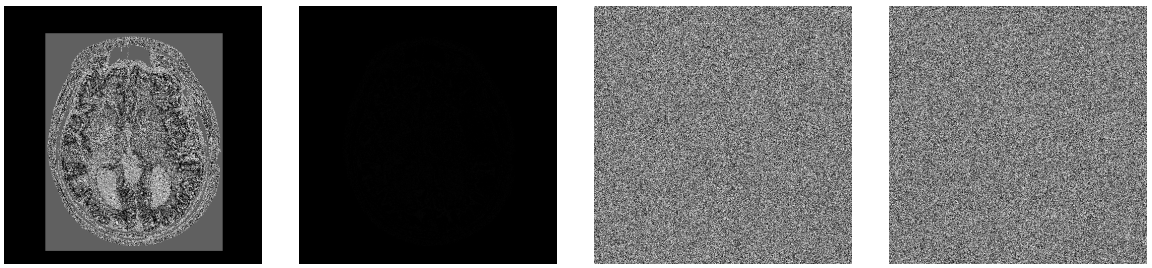


Figure 6. Experimental results (a) MSBs plane image (b) LSBs plane image. (c) Sharing secret generated from MSBs (d) Sharing secret generated from LSBs.

4.2. Security analysis of the proposed scheme

A good encryption algorithm should have large key space to resist brute force attacks, and also should be sensitive to key. In this section, some security analyses are presented.

1) *Key space analysis*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

It can be seen from the scheme that the medical image is safely outsourced to the cloud. Because different sharing secret is outsourced to the different cloud server, anyone, including cloud server itself can't obtain useful information about the image, and different sharing secret can only be decrypted by specific secret key. For example, the 128-bit secret key "50192EC81EFD534ED830D3BE68F0B53F" is used to generate sharing secret Figure 6(c); another secret key used for generating sharing secret Figure 6(d) is "8437EBF46D99CB55A00D77FCDF143369". In the meantime, the secret key highly depends on the image itself. Moreover, based on the characteristic of hash function, for any two different images, the secret keys used for generating sharing secret are different. This is a one-time pad from the point of encryption. The coordinate of the ROI, S-boxes, and hash of the image constitute the secret space of the scheme, combining to form the secret key with the size of more than 2^{512}. This ensures the security of the scheme.

2) *Key Sensitivity Analysis*

Here, we test the key sensitivities in the process of generation of sharing secret. For this test, the secret key is changed only one bit, and then conducts encryption. Result of this encryption is compared with the sharing secret generated by correct key. Key sensitivity is measured by NPCR (number of pixels change rate) and UACI (unified average changing intensity), which are expressed by formula (11). W and L are the width and length of the sharing secret, $c_k(i,j), \mathrm{k} = 1,2$ are pixel values of two sharing secrets generated by different secret keys.

$$NPCR = \frac{1}{W \times L}\sum_{i=0}^{L}\sum_{j=0}^{W} D(i,j) \times 100\%$$

$$D(i,j) = \begin{cases} 0 & c_1(i,j) = c_2(i,j) \\ 1 & c_1(i,j) \neq c_2(i,j) \end{cases} \tag{11}$$

$$UACI = \frac{1}{W \times L}\sum_{i=0}^{L}\sum_{j=0}^{W} \frac{|c_1(i,j) - c_2(i,j)|}{255}$$

All the tests are implemented based on modification of the last bit of the secret key. The corresponding values of NPCR and UACI for test images are summarized in Table 3. In reference [37], the expected values of NPCR and for a 256-Grayscale image are 99.6094% and 33.4635%. Obviously, the average values of UACI and NPCR are 33.465% and 99.61%, the proposed scheme has high sensitivity to the secret key in the encryption process.

Table 3. UACI and NPCR of test images.

Image	IM-0001-0004	IM-0001-0010	IM-0001-0012	IM-0001-0014	IM-0001-0019	IM-0002-0022
UACI	0.3355	0.3339	0.3348	0.3343	0.3343	0.3351
NPCR	0.9961	0.9960	0.9959	0.9961	0.9961	0.9964

3) *Analysis against Known-Plaintext Attack and Chosen Cipher text Attack*

In the known-plaintext attack, attackers attempt to find secret keys by obtained plaintext and the corresponding cipher text. For chosen-cipher text, attackers try to find plain text information by obtaining the decryption of chosen cipher texts. In the proposed scheme, attackers can't obtain any plain image in the cloud, and they also can't decrypt anyone of the sharing secret using incorrect keys. Even if the attacker knows the correct keys, owing to he does not know how to implement the encryption/decryption operations, he also cannot decrypt the image correctly.

4) *Analysis against collude attack*

Obviously, it can be seen from the scheme that the sharing secrets are in the different cloud servers, and they use different keys for generating sharing secret. The final verification and acknowledgement of the original image can be achieved by data owner or user. So, even if different servers can collude to use false sharing secret to act as real one, the data owner can also distinguish the true from the false of the restored original image, because only the owner possesses the private key for restoring original image. This makes it difficult for several servers to collude to cheat data owner or user.

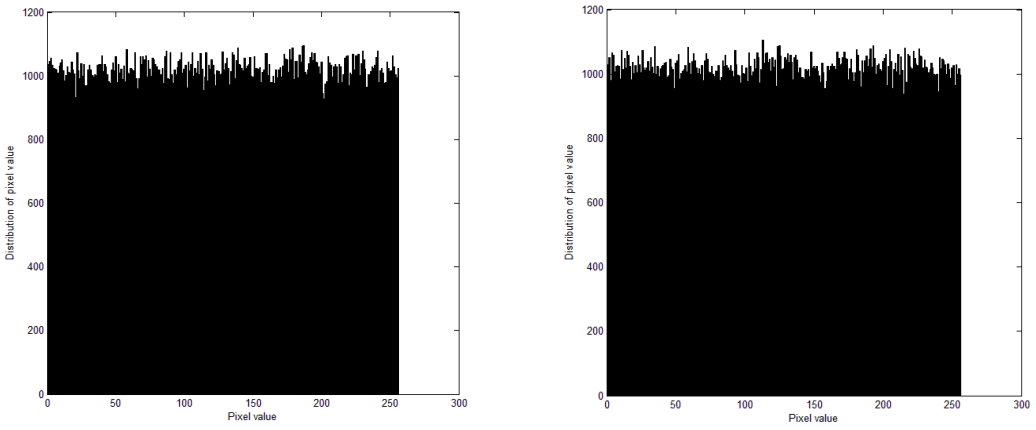
Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

4.3. Privacy protection analysis

Privacy in the cloud includes data privacy, index privacy and keyword and enquiry privacy. Here, we only discuss data privacy; others are outside of the paper.

Data privacy means the data in the cloud is secure and anyone including CSPs can't obtain the plaintext of the data.

In the proposed scheme, medical images are stored in the cloud in the encrypted sharing secret form. The histograms of the sharing secrets generated by image IM-0001-0012 are shown in Figure 7. Obviously, the histograms of the sharing secrets are nearly distributed uniformly; they don't provide any clues to statistical attack. On the other hand, adjacent pixels of a meaningful image have high correlation. In order to test the correlation between two adjacent pixels, 16384 pairs of two adjacent pixels for sharing secret are randomly selected to calculate the correlation coefficient by the following formulas (12).



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

Figure 7. Histogram of sharing secrets (a) The histogram of the sharing secret generated from MSB (b) The histogram of the sharing secret generated from LSB.

$$
\begin{aligned}
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
D(x) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))^2 \\
cov(x,y) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))\,(y_i - E(y_i)). \\
r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}
\end{aligned}
\tag{12}
$$

where x and y are grey values of two adjacent pixels in the image. The outcomes of sharing secret images are listed in Table 4. It can be seen that the correlation of adjacent pixels in the sharing secret images are very low. One can't obtain any useful information from the sharing secrets. The scheme has better performance of privacy protection.

Table 4. Coefficients of different grey encrypted images.

Image	Sharing secret	Horizontal	Vertical	Diagonal
IM-0001-0004	Sharing secret 1	-0.0056	-0.0073	-0.0024
	Sharing secret 2	-0.0011	-0.0096	-0.0107
IM-0001-0010	Sharing secret 1	-0.0105	-0.0128	0.0198
	Sharing secret 2	-0.01232	0.0016	0.0110
IM-0001-0012	Sharing secret 1	-0.0085	-0.0131	0.0011
	Sharing secret 2	-0.0016	0.0044	0.0001

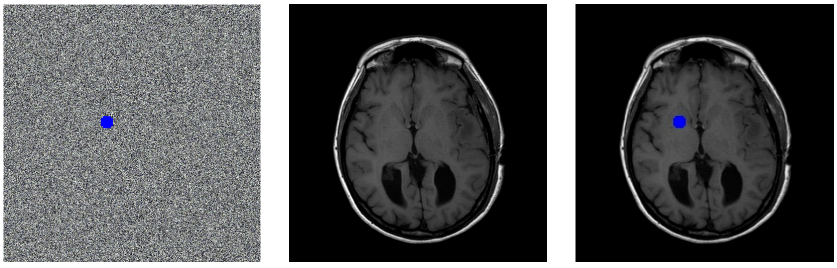
Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2

IM-0001-0014	Sharing secret 1	-0.0217	0.0031	-0.0026
	Sharing secret 2	-0.0067	0.0088	-0.0028
IM-0001-0019	Sharing secret 1	0.0073	-0.0022	-0.0053
	Sharing secret 2	0.0021	0.0039	0.0011
IM-0001-0022	Sharing secret 1	0.0018	-0.0213	0.0016
	Sharing secret 2	0.0026	-0.0136	-0.0029

4.4. Tampers localization of restored image.

From the description of the proposed scheme, we know that the user can verify the integrity of ROI for the restored image, and locate the position of the tampered image. In order to give a total understanding of tampers localization, the example illustrates the verification process for the restored image.

For example, for the second sharing secret image generated from image IM-0001-0012, see the image block in blue color in Figure 8(a), the first pixel value is changed to 111 from the original value 106; the second pixel is changed to 100 from 97. Obviously, the sharing secret is tampered. Next the tampered image block will be located.



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

Figure 8. Example of tampers localization of restored image. (a) The tampered secret image (b) Original medical image (c) Tamper with location image.

Firstly, the two sharing secrets are decrypted, and then hashes of the original image blocks are extracted, the data is represented by $H_i, i = 1,2,\cdots N$. N is the total number of block.

Secondly, conduct the superposition of two sharing secret to produce one image by plus the pixels of the corresponding position, and then carry out the reversible substitution of S-box for the ROI. The restored image is shown in Figure 8(b).

Lastly, for the restored image, calculate the hashes of every block in ROI, these values are marked by $H_i^r, i = 1,2,\cdots N$

It is found that the hash value of H_{253} is different from the value of $H_{253}^{'}$ by comparing $H_i, i = 1,2,\cdots N$ and $H_i^r, i = 1,2,\cdots N,$:

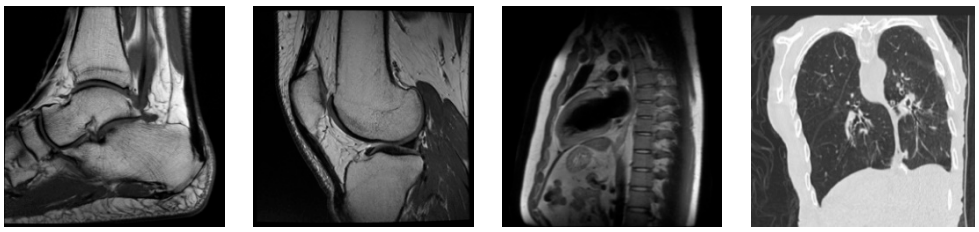
$$H_{253} = \text{2A6692938C21F29A8351F6CEAD689398}$$
$$H_{253}^{'} = \text{69C19839984065D2A0D4DFFF776629CB} \quad (13)$$

Thus, the tampered part is located, which is shown in blue color in Figure 8(c).

It can be seen that although there is no distinct difference between restored image and the original one visually, the original image is not lossless restored.

In order to test the effectiveness of the proposed scheme, some images with large ROI in COVID-19 images [38–40] are used for test. Some typical images are shown in Figure 9.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 September 2023 doi:10.20944/preprints202307.1435.v2



(a) (b) (c) (d)

Figure 9. Examples of medical images with large ROI.

Similarly, the proposed scheme can perform well on these medical images with large ROI. It should be noted that, large ROI means time-consuming for the proposed scheme. As it need calculate hashed of more image blocks.

4.5. Comparison Analysis of Performance

Up to now, people have proposed many effective ways to protect medical image. Some comparisons with other state-of-art methods on integrity verification, tampers localization and error in image recovery (ROI) are given in Tables 5 and 6.

Table 5. Comparisons with existing encryption algorithms.

The scheme	Integrity verification	Tamper localization
Ali Al-Haj [8]	Yes	No
Hua [9]	No	No
A. Kanso [10]	No	No
Chong Fu [11]	No	No
J.B. Lima [12]	No	No
Ping [28]	No	No
Proposed scheme	Yes	Yes

Table 6. Performances comparisons with the crypto-watermarking schemes.

The scheme	Integrity verification	Tamper localization	Error in image recovery (ROI)
Priyanka [19]	No	No	/
Zhang [20]	No	No	No
Priyanka [21]	No	No	Yes
Wu [22]	No	No	No
Sangita [24]	No	No	Yes
Xiang [25]	No	No	No
Ping [28]	No	No	No
Liu [29]	No	No	No
Proposed scheme	Yes	Yes	No

(1) Comparison with the existing encryption algorithms

Most of available encryption schemes for medical images have no integrity verification ability for restored one from the encrypted image. When the encrypted image is tampered, even if the secret key is correct, one can't make sure whether the restored image is the same as the original one. This will affect the application of medical images. Some comparisons in integrity verification and tamper localization are summarized in Table 5.

(2) Comparison with the existing Crypto-Watermarking algorithms

Digital watermarking can provide performance of integrity verification, especially for reversible watermarking based crypto-watermarking schemes, but some methods can't achieve totally reversibility. The comparison results are done in Table 6.

(3) Comparison with newly proposed verifiable secret sharing for outsourcing images into cloud

Different from the scheme proposed in [30], the scheme in this paper aims at ROI in medical image, and the hashes of blocks in ROI are embedded into the two bit planes, we can verify the integrity of the restored image, and moreover, the tampered sections in ROI can also be located, this is the better performance that reference [30] has not.

In addition to, the generation process of sharing secrets are different between the proposed scheme and reference [30], and the proposed scheme needs some secret keys to recover the original secret image, but the secret keys are located on the sharing secrets in reference [30].

Obviously, because the special characteristics and requirements of medical images must be met, any compromise on the quality of medical images could result in misdiagnosis. The proposed scheme has better privacy protection, and it can restore the original medical image in reversible operation, verify the integrity of ROI and locate the tampers inside ROI. These better performances outperform many protection schemes for medical images. The proposed scheme can be used for outsourcing medical image to the cloud.

5. Conclusions

Medical images are more typical than any other ordinary images, since it can be used for diagnosis purpose. Such images need security and confidentiality; it also needs to be totally restored when it is used. Region of interest (ROI) are the most important parts for diagnostic in medical image. A novel verifiable privacy preservation scheme for outsourcing medical image to cloud through ROI based crypto-watermarking is proposed in the paper. In the proposed scheme, data owner carries out substitution of S-box for the ROI, separation the image, watermarking embedding and image diffusion based on chaotic maps, and outsources to generated two sharing secrets to the cloud servers. For any authorized user, he can download shares from cloud server, and can lossless recover the original medical image through a series of decryption operations. Furthermore, the user can verify whether the original image is completely reconstructed, and even can locate the tampered parts inside ROI if anyone of the sharing secrets is damaged. Large numbers of experiments show the effectiveness of proposed scheme and better performances compared with most existing methods.

Next, under the condition that the tampers are located in restored image, the restoration technology of the tampered parts inside ROI in medical image by using crypto-watermarking, will be researched.

Funding: This research received no external funding.

Data Availability Statement: : The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Keying Li and Hua Ma: Outsourcing decryption of multi-authority ABE cipher texts, *International Journal of Network Security*, 16(4) (2014) 286-294.
2. Arpita Banik, Zeba Shamsi, Dolendro Singh Laiphrakpam, An encryption scheme for securing multiple medical images, Journal of Information Security and Applications 49 (2019) 102398
3. Praveen Kumar P, Syam Kumar P, Alphonse P.J.A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions Journal of Network and Computer Applications, 108(15) (2018) 37-52.
4. D. Agrawal, A. A. El, F. Emekci, A.Metwally and S. Wang: Secure data management service on cloud computing infrastructures, Proceedings of Service and Application Design Challenges in the Cloud, (2011) 57-80.
5. J. L. Dautrich and C. V. Ravishankar: Security limitations of using secret sharing for data outsourcing, in Proc. of Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, Paris, France, (2012) 145-160.

6. Hui Zhu, Rongxing Lu, Cheng Huang et.al: An efficient privacy-preserving location-based services query scheme in outsourced cloud, IEEE Transactions on Vehicular Technology, 65(9) (2016).7729-7739
7. Qin Zou, Jianfeng Wang, Jun Ye et.al: Efficient and secure encrypted image search in mobile cloud computing. Soft Computing, 4 (2016) 1-11.
8. Ali Al-Haj, Gheith Abandah, Noor Hussein, Crypto-based algorithms for secured medical image transmission, IET Information Security, 9(6) (2015) 365–373.
9. Zhongyun Hua, Shuang Yi, Yicong Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, Signal Processing 144 (2018) 134-144.
10. A. Kanso, M. Ghebleh, An efficient and robust image encryption scheme for medical applications, Communication in Nonlinear Science and Numerical Simulation, 24 (2015) 98-116.
11. Chong Fu, Wei-hong Meng, Yong-feng Zhan, An efficient and secure medical image protection scheme based on chaotic maps, Computers in Biology and Medicine 43(2013)1000-1010.
12. J.B. Lima, F.Madeiro, F.J.R.Sales, Encryption of medical images based on the cosine number transform, Signal Processing: Image Communication 35 (2015) 1-8.
13. Li-Chin Huang, Lin-Yu Tseng, Min-Shiang Hwang, A reversible data hiding method by histogram shifting in high quality medical images, The Journal of Systems and Software 86 (2013) 716-727.
14. Nazir A. Loan, Shabir A. Parah, Javaid A. Sheikh, Hiding Electronic Patient Record (EPR) in medical images: A high capacity and computationally efficient technique for e-healthcare applications, Journal of Biomedical Informatics 73 (2017) 125-136.
15. Rayachoti Eswaraiah, Edara Sreenivasa Reddy, Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest, IET Image Process., 9(8) (2015) 615-625.
16. Amit Kumar Singh, Mayank Dave, Anand Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images, Multimedia Tools and Applications, 75(14) (2016) 8381-8401.
17. Chih-Wei Shiu, Yu-Chi Chen, Wien Hong, Encrypted image-based reversible data hiding with public key cryptography from difference expansion, Signal Processing: Image Communication 39 (2015) 226-233.
18. Jiantao Zhou, Weiwei Sun, Li Dong, et al. Secure reversible image data hiding over encrypted domain via key modulation, IEEE Transactions on Circuits and Systems for Video Technology, 26(3) (2016) 441-452.
19. Priyanka Singh, Balasubramanian Raman, Reversible data hiding for rightful ownership assertion of images in encrypted domain over cloud, International Journal of Electronics and Communications (AEÜ) 76 (2017) 18-35.
20. Weiming Zhang, Hui Wang, Dongdong Hou, Reversible data hiding in encrypted images by reversible image transformation, IEEE Transactions on Multimedia, 18(8) (2016) 1469.
21. Priyanka Singh, Balasubramanian Raman, Reversible data hiding based on Shamir's secret sharing for color images over cloud, Information Sciences 422 (2018) 77-97.
22. Han-Zhou Wu, Yun-Qing Shi, Hong-Xia Wang, Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification, IEEE Transactions on Circuits and Systems for Video Technology, 27(8) (2017) 1-1.
23. Bouslimi D, Coatrieux G, A crypto-watermarking system for ensuring reliability control and traceability of medical images, Signal Processing Image Communication, 47 (2016) 160-169.
24. Sangita Zope-Chaudhari, Parvatham Venkatachalam, Krishna Mohan Buddhiraju, Secure dissemination and protection of multispectral images using crypto-watermarking, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 8(11) (2015) 5388-5394.
25. Tao Xiang, Jia Hu, Jianglin Sun, Outsourcing chaotic selective image encryption to the cloud with steganography, Digital Signal Processing 43 (2015) 28-37.
26. Hang, Gao, Mengting Hu, Tiegang Gao, et al. Random grid and reversible watermarking-based on verifiable secret sharing for outsourcing images in cloud, International Journal of Digital Crime and Forensics, 10(1)(2018) 24-39.
27. Muhammad Arsalan，Aqsa Saeed Qureshi， Asifullah Khan and Muttukrishnan Rajarajan, Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique, Applied Soft Computing, 51 (2017) 168-179.
28. Ping, P., Zhang, X., Yang, X. et al. A novel medical image encryption based on cellular automata with ROI position embedded, Multimed Tools Appl 81 (2022) 7323–7343.

29. Liu, Z., Li, J., Ai, Y. et al. A robust encryption watermarking algorithm for medical images based on ridgelet-DCT and THM double chaos. J Cloud Comp 11(022), 60
30. Xiaojun Qi, Xing Xin: A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, Journal of Visual Communication and Image Representation, 30 (2015) 312-327.
31. Nasrin M. Makbol, Bee Ee Khoo: A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition, Digital Signal Processing, 33 (2014) 134-147.
32. Zhang Wenyin, Frank Y. Shih: Semi-fragile spatial watermarking based on local binary pattern operators, Optics Communications, 284(16-17) (2011) 3904-3912.
33. Ni, Z., Shi, Y.Q., Ansari, N., Su, W.: Reversible data hiding, IEEE Transactions on Circuits Systems for Video Technology, 16 (3) (2006) 354-362 .
34. Dimitris Souravlias, Konstantinos E. Parsopoulos, Gerasimos C. Meletiou, Designing bijective s-boxes using algorithm portfolios with limited time budgets, Applied Soft Computing 59 (2017) 475-486.
35. C Pak, L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Processing, 138 (2017) 129-137.
36. A Pandey , BS Saini , B Singh , An Integrated Approach Using Chaotic Map & Sample Value Difference Method for Electrocardiogram Steganography and OFDM Based Secured Patient Information Transmission. Journal of Medical Systems , 41 (12) (2017) 187.
37. C. Zhu, A novel image encryption scheme based on improved hyper-chaotic sequences. Opt Communications. 285(1) (2012) 29-37.
38. [36] https://www.sirm.org/category/senza-categoria/covid-19/
39. https://radiopaedia.org/ Accessed April 9, 2020.
40. https://www.kaggle.com/tawsifurrahman/covid19-radiography-database/ Accessed April 9, 2020.