# Secure transmission of Computed Tomography (CT) of the Brain using Wilcox indexive linear curve certificate- less signcryption (WILCS)

Dr. J. Shaik Dawood Ansari1

1 Western Pacific University, Ialibu, Southern Highlands 675265, Papua New Guinea

jsdansari@wpu.ac.pg;jsdansari@gmail.com

**Abstract.** In neurology, radiology, and oncology, computed tomography (CT) images are vital for research, aiding in the detection, diagnosis, and classification of diseases like cancer, tumors, and aneurysms through algorithms, deep learning, and machine learning models. However, transmitting these CT brain scan images across networks poses significant challenges, including ensuring authentication, integrity, confidentiality, and managing large image sizes. To address these issues, this paper proposes a blended approach called Wilcox Indexive Linear Curve Certificateless Signcryption (WILCS), which combines preprocessing, compression, and encryption. WILCS involves three key steps: denoising CT images using Wilcoxon filtering, compressing them with the BWHLCT method, and encrypting them via the SSCC signcryption technique. This ensures secure transmission, with receivers using reverse signcryption and decompression to retrieve the original images. Experimental evaluations demonstrate that WILCS outperforms existing methods in terms of integrity, confidentiality, compression ratio, and storage efficiency, while maintaining high security and image quality.

**Keywords:** SSCC - Schmidt-Samoa cryptographic Certificateless Signcryption, BWHLCT- Burrows Wheeler transforms using Hilbert curve based compres- sion, Secure brain CT transmission, Wilcoxon filtering, MSS Algorithm with CC Map Lattices, FOCS - Fractional-Order Chaotic System.

## 1. Introduction

Transferring medical images over open wireless networks presents significant chal- lenges, especially in ensuring data safety and security. Medical images are a critical part of digital imaging, but their sensitive nature makes secure transfer a complex issue. Unauthorized modifications during transfer can seriously impact the treatment to the patient. Our important objective is to make sure the Brain CTs are transferred safe and secure without any edition. Stego algorithms are often used worldwide to protect sen- sitive information by hiding it into the pixels of the medical image.. These algorithms enhance security during transfer and help maintain data integrity.

In [1], a new technique has been proposed using the "Fractional Chaotic Maps" to transfer secret user data over the wireless communication safely. The technique, how- ever, did not yield a higher confidentiality rate, even with its innovative approach. In

[2] A refined steganographic method based on medical Image and embedding the sen- sitive data of the patient in image. The method demonstrated enhanced confidentiality, increased embedding capacity, and improved robustness. However, the embedding pro- cess exhibited inefficiencies, which could be further optimized for better performance. In [3], a dual image compression and encryption model was developed to elevate the efficacy to secure the medical image by compression and encryption algorithm. How- ever, the model lacks to increase the confidentiality by using steganography. In, [4] proposed a quantum multiple image compression technique with an encryption algo- rithm, which raises complexity on computation using discrete cosine transformation. Nonetheless, it did not yield better compression ratios with regards to performance. In

[5] Encrypted and compressed medical images simultaneously using MSSACCML and lacks with improvement on integrity level. A new encryption method focusing on FOCS was proposed in [6], but its computational cost was more than traditional en- cryption methods. An optical-centered algorithm was presented in [7] to boost data in- corporating the medical image by offering efficiency and increased security on medical image transfer through insecure channel. Though the authentication and integrity im- proved but time consumes. A high-level compression algorithm was proposed to im- prove security with the RSA cryptography method in [8], But it was a significant chal- lenge to achieve a higher rate of integrity.

In [9] steganography method was proposed which hides patients' information within medical images securely by increasing confidentiality. But the approach did not con- sider image compressions that would help to reduce space complexity. The authors proposed an algorithm for compressing images that showed improved performance in terms of compression rate in [10], the published algorithm faced no security analysis conducted to determine the strength of the algorithm.

### 1.1. Major contributions

The major contributions of the proposed WILCS technique includes medical image se- curity enhancement before transfer by preprocessing, compression, and signcryption; employing the Wilcoxon filtering technique to minimize the MSE and enhance the PSNR, effectively performing denoising and improving image contrast; utilizing the BWHLCT to compress the image for enhancing the compression ratio also space re- duction during transmission; applying the SSCC Signcryption to encrypt the input med- ical brain CT image, to strengthen integrity and confidentiality and conducting simula- tions using various measurements to evaluate the performance enhancements of WILCS compared to existing methods.

## 2. Proposed WILCS methodology

Advances in digital technology have simplified sharing medical information over com- munication networks. However, the security of medical data transmission remains a concern, as patients risk losing privacy over these networks. Unlike text, medical im- ages face two major risks: information loss and breaches in confidentiality. To address

these issues and minimize information loss while maintaining strong security, this pa- per introduces a new WILCS technique. The goal of WILCS is to secure medical im- ages during wireless network transmission while optimizing storage efficiency.

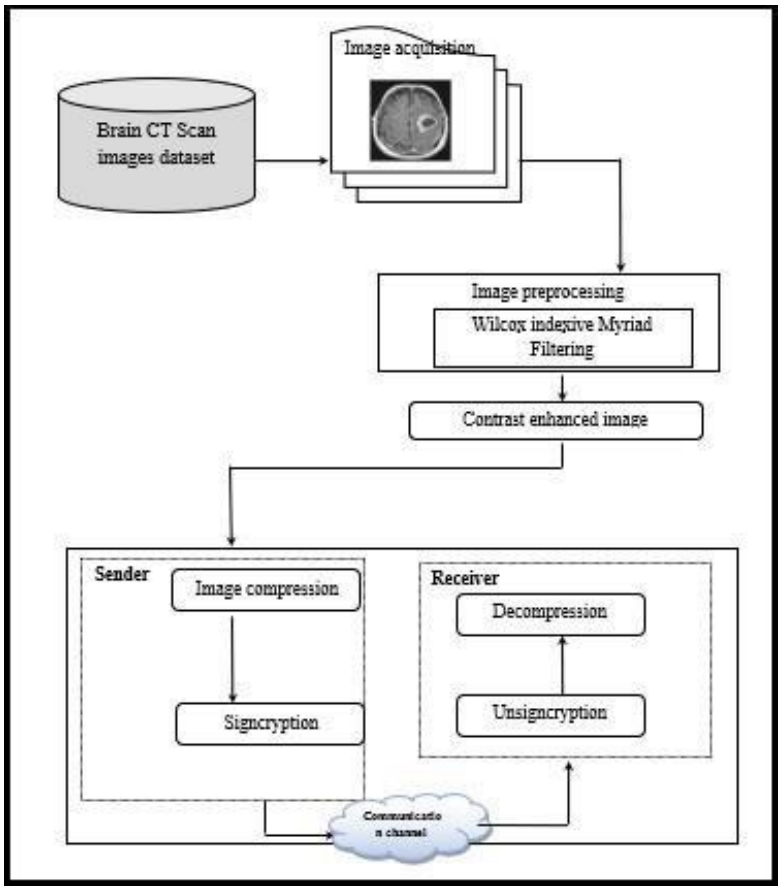



**Fig.1.** Proposed WILCS Architecture

As shown in **Fig.1.** the architectural diagram for WILCS, which uses three pro- cesses before transmission. A number of brain CT Scan images are retrieved from the dataset as BI1, BI2,…,BIn illustrated in the figure. Acquired images undergo denoising and contrast enhancement through Wilcoxon filtering. Then BWHLCT based compres- sion, and SSCC Signcryption which is

implemented on the sender side before sending. After reception, the receiver performed processes like reversal of signcryption and com- pression, to receive the original image with higher integrity and confidentiality.

## 2.1. Image preprocessing using Wilcoxon filtering Method

Image pre-processing constitutes a critical phase in imaging and analysis, expected to improve the brain CT quality, reliability, and useableness of medical images to facili- tate accurate and reliable analytical outcomes. Therefore, selecting an effective previ- ous processing method is essential to advance the quality of brain CT and ensure precise analytical outcomes. To this end, the proposed technique WILCS preprocesses the medical images using a Wilcoxon filtering method.

We consider a collection of brain CT scan images, denoted as $BI_1, BI_2, \dots, BI_n$ from a dataset of Brain CT Scans. Each image is made up of pixels, represented as

$P1, P2, P3, \dots . P_m$ . T These pixels are structured as $3 * 3$ inside a kernel window to be filtered. The structured 3 * 3 Wilcoxon filtering is shown in **Fig. 2.** Below.

| | | |
|---|---|---|
| $\boldsymbol{P_1}$ | $\boldsymbol{P_2}$ | $\boldsymbol{P_3}$ |
| $\boldsymbol{P_4}$ | $\boldsymbol{P_C}$ | $P_6$ |
| $\boldsymbol{P_7}$ | $P_8$ | $P_9$ |

Center pixel ⟶

**Fig.2.** Structured $3 * 3$ WILCOXON filtering

As shown in **Fig.2.** pixels in a filtering window are represented in rows and

col- umns. After forming the pixels, we consider the middle pixel of the window to remove noise. The Wilcoxon filtering method is used to process the window, which computes the probability that the pixel in the center is similar to its adjacent pixels. The filtering

process is detailed below: $F = arg\ min\ (q * \sum^{n} |\boldsymbol{P_C} - \boldsymbol{P_i}|)$ (1) In (1), $F$ is the

output, argument of minimum function is arg $min$ t, $P_C$ the middle pixel, $P_i$ shows the 'n' neighbor pixels and $q$ signifies a weight. This function in the equation is to regulate the medical images degree of blurring effect. In the equation, the weight function is to

control the images amount of blur. A pixel exhibiting minimal variation compared to its surrounding pixels is considered normal. Noisy pixels, which show the highest dif- ference with respect to their neighbor points, are recognized and eliminated from the window used for filtering. It improves the quality of images of the input brain CT scans.

## 2.2. Image compression using BWHLCT

After completion of the preprocessing, the WILCS compress the image to reduce the input image size for transfer purposes. Image compression reduces the file size of dig- ital images while preserving essential visual details, facilitating more efficient storage and faster transmission. BHWLCT uses lossless compression to achieve that. In loss- less compression, the output of a compressed image retains all the original information, allowing the exact reconstruction of the original image without any loss of data.

$BI_{ij}$ $_{org}$ = $B_{ij_comp}$ (2) Where $BI_{ij}$ $_{org}$ is preprocessed brain CT image and $BI_{ij}$ $_{comp}$ is compressed brain CT image. A brain CT image is shown in a 2D pixels, are saved as columns and rows mentioned by $n * m$ matrix.

$$BI_{ij} = \begin{bmatrix} P11 & P12 & \dots & P1n \\ P21 & P22 & \dots & P2n \\ \vdots & \vdots & \dots & \vdots \\ Pm1 & Pm2 & \dots & Pmn \end{bmatrix} \quad (3)$$

Where $P11$ is the pixel in the first row first column of brain CT. $Pmn$ is the brain CT '$m$' row and '$n$' column. A brain CT has values from 0 and 255. The suggested trans- formation is employed to transform a group of brain CT pixels to an ordered effectual format. In the process, Hilbert linear curve examines all pixel in the matrix '$BI_{ij}$ '. A square-shaped path with one open side, the Hilbert curve featuring four main directions. In some lossless image compression methods, the next level of the Hilbert curve is used.

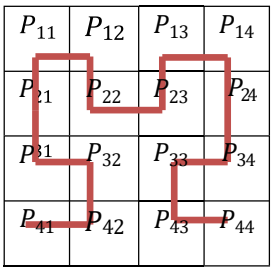


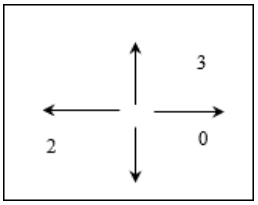

**Fig.3**. Matrix of Hilbert curve

As shown in **Fig.3**. Hilbert curve second order applied to brain CT pixels. The

brain CT pixels are gathered in a rectangular group. The filling curve[9] forms a straight path through the brain CT scan pixels. It begins at one end of the curve and moves along the path to the other end. Using the Hilbert space curve method, the current direction is converted into a single unit value. The Hilbert curve is a pattern of directions, with each direction represented by a specific symbol. {→ (right), ↑ (top), ← (left), ↓ (bottom)}. The process helps to map the symbol to the integer {0, 1, 2, 3}. $Bij_comp = T\{Bij_pre\}$

(4) Where $Bij_comp$ is a compressed brain CT, $T$ is transformation, $Bij_pre$ is a

preprocessed brain CT pixel. The preprocessed input image on which




transformation function '$T$' is applied.

**Fig.4.** Hilbert Curve Notion

As shown in **Fig.4**. a Hilbert integer direction and integer value. From Fig. 3 and 4, the final transformed results are attained as, $Bij_comp$ = {012110301033230} (5) Where $Bij_comp$ is a compressed pixels of input brain CT. In this manner, efficacy compression is attained, results in a good compression ratio.

## 2.3. SSCC Signcryption

After brain CT compression, the SSCC signcryption is done to elevate the security of transfer over the network channel. Certificateless Signcryption is a cryptographic tech- nique that integrates digital signature and encryption into a single process. The WILCS method merges Schmidt-Samoa cryptography into the Certificateless Signcryption framework to increase security. The certificateless signcryption framework has multi- ple steps, such as setup, generation of partial private key, generation of full private key, generation of public key, signcryption, and unsigncryption. The setup phase has the security parameter '$Q$' and returns global system parameters ($R$) which has a Session Key ($SK$), image space ($D$), cipher image space ($C$). It is mentioned as, $R \rightarrow \langle SK, D, C \rangle$

(6) Then the partial private key ($kpp$) is attained as given below, $kpp \rightarrow \langle$ID, $R, PV\rangle$

(7) The user identity (ID) takes an arbitrary value '0' and '1'. If the user identity is '1', then it returns to a partial private key. If the user identity is '0', then it returns unauthorized entity, as of (4). Given the common parameters $R$, and the corresponding public value PV. Then the full private key is generated by using Schmidt-Samoa cryptography by considering two large prime numbers '$u$'and '$v$' $kfp$ =

$k_{pb}{}^{-1}\ mod\ lcm\ (u-1, v-1)$ (8) Where $k_{fp}$ denotes a full private key, $k_{pb}$ de-

notes a public key, $k_{pb} = u^2v$ (9) The public and full private key are used to perform the encryption and signature generation process together, after the key generation is finished. The encryption is performed with receiver's public key $\beta_E =$

$CBI^{k}{}^{pb}\ mod\ k_{pb}$ (10) Where $k_{fp}$ denotes a full private key, $k_{pb}$ denotes a public

key, The corresponding signature '$Sig$' is generated as follows, $Sig =$

$CBI^{k}pp\ mod\ k_{pb}$ (11) Where $k_{fp}$ denotes a full private key, $k_{pb}$ denotes a public key, $CBI$ denotes a compressed brain CT Scan image. In this way, the cipher text and signature are generated.

## 2.4. SSCC Unsigncryption

The unsigncryption is done at the side of the receiver to revert the Initial brain CT. Unsigncryption has two key phases: digital signature verification and decryption. In first phase, digital signature verification is done to make sure the authenticity and in- tegrity of the transfer. At the receiver side, the new signature is generated '$Sig_r$' using Schmidt-Samoa cryptography. Finally, the generated signature is $Sig_r$' is verified with the signature '$Sig$'. The receiver decrypts the ciphertext only if the two signatures are valid and match. Otherwise, decryption is not possible. $CBI = EBI^{k}fp\ mod\ (k_{pb})$

(12) Where $CBI$ denotes a compressed brain image, $EBI$ indicates a cipher image, $k_{fp}$

represents receivers full private key, $k_{pb}$denotes a public key. After decrypting the brain CT scan, decompression is performed using the inverse method of BWHLCT. Finally, the decompressed brain CT image is obtained.

## 3. Experimental Evaluation

A comparison of the WILCS method with recently published works of [1] & [2], all implemented in MATLAB, through experimental evaluation. The evaluations were done on medically licensed Brain CT scan images which can be downloaded from: - https://www.kaggle.com/datasets/trainingdatapro/computed-tomography-ct-of-the- brain. All these brain CT were acquired as part of normal clinical care. All Brain CT scans were pre-screened for analysis. Dataset contains 512 Brain CT [JPEG Images], classified into two classes i.e., Tumor, non-Tumor.

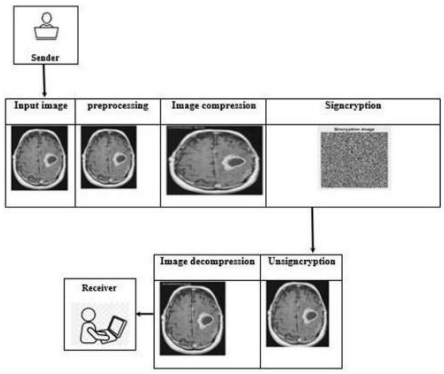



**Fig.5.** Qualitative results for WILCS

## 3.1. Qualitative analysis

WILCS involves several steps, starting with an original brain CT scan as input. First, Wilcoxon filtering enhances the CT's contrast. Next, BWHLCT compresses the brain CT. SSCC Signcryption then encrypts the CT into a cipher version. Upon receiving it, the extraction process uses the same key, in the process of unsigncryption to decipher the actual brain CT. In the end, the receiver gets the decompressed, original brain CT.

## 3.2. Quantitative analysis

The performance analysis compares three methods: the WILCS technique, an existing secure lightweight signcryption method [1], and an improved wavelet steganography

algorithm for DICOM images [2]. Key metrics like PSNR, DCoR, DCR, and DIR are tested on brain CT images of various sizes.

### 3.2.1 PSNR

PSNR is to measure the quality of a denoised brain CT compared to the actual brain CT. PSNR is found based on the Mean Squared Error (MSE) between brain CT pixels of the two images. The formula for calculating PSNR is $\overline{PSNR}$ = 10 log 10 ( $L^2$ )

$MSE$

(13) The PSNR is calculated using the extreme possible pixel value (L) and the Mean Squared Error (MSE). $MSE = [DBI - BI]$ (14) The mean square error (MSE) is calculated based on the denoised brain CT (DBI) and the actual brain CT scan image (BI). The PSNR analysis is shown in **Table 1.** below.

**Table 1.** PSNR analysis

| **Image size (KB)** | **PSNR (dB)** | | |
|---|---|---|---|
| | **WILCS** | **Certificateless Group Signcryption** | **Enhanced wavelet steganographic** |

| Techniquealgorithm | | | |
|---|---|---|---|
| **61.77** | 35.81 | 27.13 | 30.44 |
| **405.3** | **47.56** | 32.24 | 41.32 |
| **581.63** | **54.45** | 41.53 | 50.47 |
| **470.55** | **52.96** | 41.23 | 47.93 |
| **450.28** | **50.34** | 37.14 | 43.95 |
| **668.28** | **57.87** | 44.54 | 50.72 |
| **401.64** | **60.41** | 47.14 | 53.14 |
| **421.26** | **65.53** | 51.34 | 60.67 |
| **457.08** | **66.31** | 51.14 | 58.51 |
| **383.92** | **60.27** | 47.54 | 55.52 |




**Fig.6.** PSNR Graph

As shown in **Fig.6**. the result of the PSNR variations in relation to different medical brain CT. The horizontal axis shows various sizes of the brain CT, while the vertical axis shows the corresponding PSNR values. The results show that WILCS method achieves a higher PSNR compared to other two methods. A comparative analysis of the WILCS method with other two methods shows that the performance of the PSNR using the WILCS method has risen 13% and 6% compared to the [1] & [2] respectively.

### 3.2.2 Analysis of Data Compression Ratio (DCoR)

The data compression ratio is another quantitative measure of brain CT, compression method efficiency in reducing the size of the brain CT. This measurement is applied to actual brain CT that have processed compression while storing classified data. To gov- ern the compression ratio, one divides the size of the uncompressed actual brain CT by that of its compressed brain CT. The mathematical notion for calculating the compres- sion ratio is as follows:

Com_R=[(OBI (KB) )/(CBI (KB))] (15) In this context, Com_R is the compression ratio, while OBI (KB) and CBI (KB) are the sizes of uncompressed and compressed brain CT, respectively. The data compression ratio is measured

in kilobytes (KB). The efficiency of the method is directly proportional to the magnitude of the compression ratio. The data compression ration analysis is shown in **Table 2.** below.

**Table 2.** Data Compression Ratio Analysis

| Size of Image (KB) | Data Compression Ratio | | |
|---|---|---|---|
| | **WILCS** | **Certificate less Groupd Signcryption Technique** | **Enhance wavelet steganographic algorithm** |
| **860.78** | 8.8 | 6.5 | 7.7 |
| **403.21** | 6.1 | 4.3 | 5 |
| **581.54** | 7.6 | 5.6 | 6.7 |
| **474.46** | 8 | 5.7 | 7.1 |
| **450.39** | 8.1 | 6.2 | 7.3 |
| **668.69** | 9.5 | 6.2 | 7.3 |
| **402.35** | 8.7 | 5.1 | 6.1 |
| **411.57** | 9.1 | 6.4 | 7.7 |

| | | | |
|---|---|---|---|
| **456.29** | 7.4 | 5 | 6.3 |
| **383.92** | 8.2 | 5.2 | 6.8 |

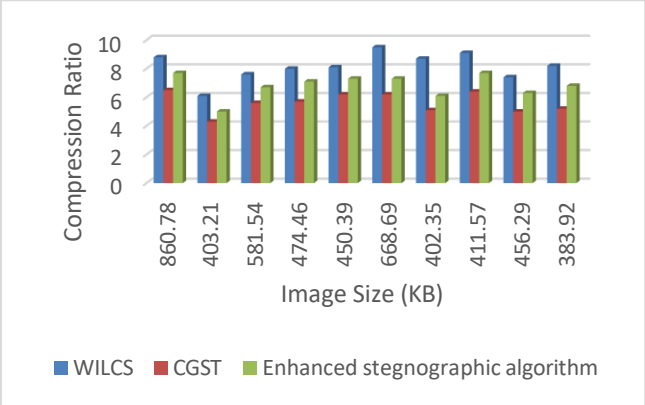



**Fig. 7.** Data Compression ratio Analysis

As shown in **Fig.7.** The comparisons of the performance of three methods using brain CT scans of various sizes. The results show that the WILCS method outperforms

the other two methods. Based on ten repetitions, WILCS improves the compression ratio by 5% over [1] and 7% over [2].

### 3.2.3 Analysis of Data confidentiality rate (DCR)

The DCR is simulated by calculating the ratio of user access authorization to brain CT to the collection of brain CT. The mathematical notion for calculating is shown below:

$$CR = \sum_{i=1}^{n} \left(\frac{BI_{AAU}}{100}\right) * \frac{}{BIi} \quad (16)$$

Where '$CR$' is data confidentiality rate, $BI_{AAU}$ is user access authorization on the collection of brain CT based on the collection of brain CT'$BIi$'. The data confidentiality rate analysis is shown in **Table 3.** below.

**Table 3.** Data Confidentiality rate Analysis

| Number of images | Data Confidentiality Rate (%) | | |
|---|---|---|---|
| | **WILCS** | **Certificate less Signcryption Technique** | **Groupd wavelet steganographic algorithm** |
| **100** | **94** | **89** | **91** |
| **200** | 93.5 | 86.3 | 90 |

| | | | |
|---|---|---|---|
| **300** | 93.33 | 84 | 86.32 |
| **400** | 92.75 | 82.74 | 85.24 |
| **500** | 92.6 | 82 | 85 |
| **600** | 91.5 | 80.65 | 83.15 |
| **700** | 90.42 | 81.72 | 82.56 |
| **800** | 91.62 | 81 | 80.85 |
| **900** | 87.77 | 77.32 | 80.53 |
| **1000** | 86 | 73.4 | 75.4 |




**Fig.8.** Data Confidentiality rate Analysis

As shown in **Fig.8.** The comparison of the data confidentiality rates of three methods using different numbers of brain CTs. The results show that WILCS achieves higher data confidentiality than [1] and [2]. On average, WILCS improves data confidentiality by 11% over [1] and 8% over [2], based on ten repetitions.

### 3.2.4 Analysis of Data integrity rate (DIR)

The DIR is another quantitative measure of brain CT, by the ratio of the collection of brain CT that are not changed by any intruding users to the collection of brain CT. The

mathematical notion to calculate the DIR is: $DIR_{i=}(\sum^{n} \frac{BIna}{BIi}) * 100$ (17)

Where $DIR$ is data integrity rate, $BI_{na}$ is number of brain CTs that not altered by in- truders, and the collection of brain CTs '$BI_i$ '. The data integrity rate analysis is shown in **Table 4.** below.

**Table 4.** Data Integrity Rate Analysis

| **Number of images** | **Data Integrity Rate (%)** | | |
|---|---|---|---|
| | **WILCS** | **Certificate less Signcryption Technique** | **Enhance Groupd wavelet steganographic algorithm** |
| **100** | 93 | 73 | 84 |
| **200** | 92.4 | 72 | 83 |
| **300** | 92.32 | 69 | 82.23 |
| **400** | 90.24 | 68.74 | 82 |
| **500** | 91 | 68.1 | 81 |
| **600** | 88.15 | 68.15 | 78.83 |
| **700** | 87.84 | 66.84 | 81 |
| **800** | 87.11 | 65.86 | 78.61 |
| **900** | 86.21 | 64 | 79.42 |
| **1000** | 85.4 | 62.6 | 76.4 |

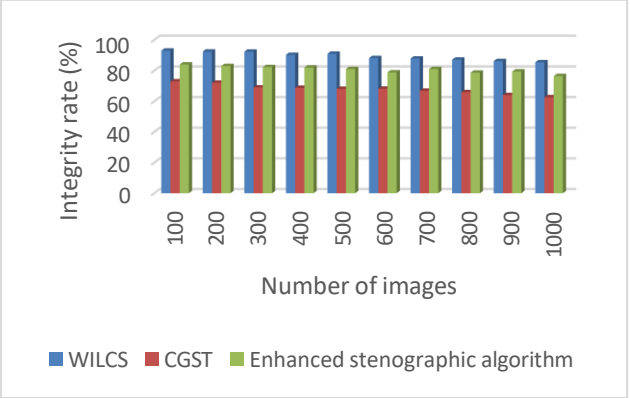



**Fig.9.** Data Integrity Rate Analysis

As shown in **Fig.9**. the comparison of the data integrity rates of three methods us- ing different numbers of brain CTs. WILCS achieves higher data integrity than the existing methods [1] and [2]. On average, WILCS improves data integrity by 10% over [1] and 12% over [2], based on ten repetitions.

## 4. Conclusion

Securing sensitive medical images during digital transmission is a huge challenge in today's fast-paced tech world. Hospitals and researchers need to share critical data like brain scans wirelessly but keeping that information safe from breaches or corruption is no small act. Our new method, the WILCS algorithm, comes in.

1. Clean up the image: First, we remove noise from medical images (like blurry spots in a CT scan) to sharpen their quality. This step boosts something called the "Peak Signal-to-Noise Ratio (PSNR)", which basically measures how crisp the image stays after processing.

2. Shrink the file size: To save space during wireless transfers, we compress the images using a clever technique inspired by the BWHLCT Imagine folding a map effi- ciently, it is like that, but for pixels!

3. Lock it down: Next, we encrypt the compressed images using a special security key (called a "stego key") and a robust encryption method named SSCC Signcryption". This double-layered protection ensures only authorized users can access the data.

4. Send it safely: The encrypted images are then transmitted over the network. When they reach the receiver, the right user can unlock and rebuild the original image using the shared stego key.

## References


1. Meshram, C., Imoize, et al. CGST: Provably secure lightweight certificateless group signcryption technique based on fractional chaotic maps. *IEEE Access, 10*, 39853– 39863. (2022).

2. Ahmad, M. A., Elloumi, M., et al. Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. *Alexandria Engineering Journal, 61*(12), (2022).

3. Yang, Y.-G., Guan, B.-W., et.al. Double image compression-encryption algorithm based on fractional order hyper chaotic system and DNA approach. *Multimedia Tools and Applications, 80*, 691–710. (2021).

4. Dai, J.-Y., Ma, Y., et.al., Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map. *Quan- tum Information Processing, 20*(1), 1–24. (2021).

5. Selvi, C. T., Amudha, J., et.al., A modified salp swarm algorithm (SSA) combined with a chaotic coupled map lattices (CML) approach for the secured encryption and compression of medical images during data transmission. *Biomedical Signal Pro- cessing and Control, 66*, 1–13. (2021).

6. Xu, J., Mou, J., et.al., The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system. *The Visual Computer, 38*, 1509–1526. (2022).

7. El-Shafai, W., Almomani, I., et.al., An optical-based encryption and authentication algorithm for color and grayscale medical images. *Multimedia Tools and Applica- tions, 82*, 23735–23770. (2023).

8. Wahab, O. F. A., Khalaf, A. et.al., Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE Access, 9*, (2021).

9. AlEisa, H. N., Data confidentiality in healthcare monitoring systems based on image steganography to improve the exchange of patient information

using the Internet of Things. *Journal of Healthcare Engineering, 2022*, 1–11. (2022).

10. Liu, X., Zhang, et.al., Medical image compression based on variational autoen- coder. *Mathematical Problems in Engineering, 2022*, 1–12. (2022).