International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Analysis of Protecting Lung Cancer Images Using Visual Cryptography

V. Sreeprada[1], Dr. K. Vedavathi [2]

Submitted: 25/08/2023 **Revised:** 13/10/2023 **Accepted:** 24/10/2023

Abstract: Linking the intelligent sensors and smart devices in the hospital ecosystem, medical data must be kept securely. To safeguard the privacy of patients, an intelligent working system requires improved security measures. Recently, sure imagine encryption methods based on compression sensing (CS) have been developed for securing images with visual security. In these schemes, both compression and encryption of the images are performed simultaneously, before being fixed into a holder image. The encrypted images are partial by the current systems' presentation limits along with quality and efficiency of the reconstructed images. This paper develops an Improved Visually Secure Image Encryption (IVSIC) scheme which aims to handover real-time lung-cancer images securely, without degrading their quality. The greatest level of security of our proposed system is established by contrasts and imitations. In contrast to some newly developed schemes, it is also more effective and produces cipher and reconstructed images of higher quality.

Keywords: *Lung cancer image, encryption, decryption, security, visual cryptography*

1. Introduction

One of the most lethal kinds of cancer is lung cancer which affects thousands of people. Since it cannot be discovered in the initial periods, the patient's chances of survival are extremely low. Since treatment for lung cancer depends on the period as well as type of the disease, a method should be recommended for forecasting the malignant class such that it specifics how long it will take, how serious it is, and how likely it is that the chosen treatment will cure the cancer . A clinical trained professionals determines when to conduct a lung CT, which involves looking at the body's lung parenchyma and clinical images. Segmentation algorithm for the input CT scan image is reported keeping this point in mind [1]. For accomplishing the objectives of confusion and diffusion, numerous cryptographic strategies have been proposed previously. Due to their deterministic behavior but high sensitivity to initial conditions, chaotic maps have also been utilized in cryptography to accomplish both these objectives.

An algorithm for safeguarding crucial areas in medical images was developed in an earlier work. The first step in using the constant of difference is to locate key areas, also known as lesion; The texture complexity is then examined and extra parts are treated as blocks. The pixel adaptive diffusion concept and three circles of high-speed scrambling are utilized to randomly move neighboring pixels. Furthermore, carrying out pixel versatile dispersion, the system utilizes modulo number juggling activity. Deep and machine learning techniques were applied to inspect the lung CT images.

A work including a cryptographic function and fundamental key features of blockchain skill was developed to investigate a medical image. The research for diagnosis includes a variety of neural network features including the combining of contourlet transform from a lung histopathology analysis image. Though automatic lung cancer detection system is effective on CT scan images, designing such robust system is a challenging problem.

The following is how the paper is laid out. Some related works and contributions are provided in Section 2. Section 3 presents the proposed the IVSIC scheme. The proposed system is simulated and its effectiveness is evaluated in Section 4. The conclusion and future work of the paper are presented in Section 5.

2. Literature Review

A 3D cosine number transform (3D-CNT), which defines the basis vectors using a field that is finite rotation operator transformation, has been proposed through Lima et al. [1]. They have presented a 3D clinical image encryption conspire in light of the 3D-SCNT, which utilizes the revolution points as mystery boundaries.

Tiankai et al. [2] talked about the security verification supplies for medical images. A security verification technique based on visual cryptography and fractal was developed as well.

Medical image spatial structure and gray-level statistical information are fully mined using discrete fractal Brownian

1 Department of Computer Science, GITAM Deemed to be University, INDIA
2 Department of Computer Science, GITAM Deemed to be University, INDIA
Visakhapatnam, Andhra Pradesh, India1,2
** Corresponding Author Email: sreepradav487@gmail.com*

random field method. The authentication features are formed by utilizing energy structure stability and data of fractal structure space is analyzed using spatial data mining methods. The authentication method's robustness is improved by visual cryptography (VC).

Ali Alzahrani. [3] Highlighted a DLEDNet method for encryption and decryption of medical images. In particular, the primary learning network for moving the image from its target domain into the original domain in DLEDNet is the Cycle-GAN network. The target domain is thought of as one of the "Hidden Factors" that will direct the learning method through the encryption procedure.

The scrambled image is reestablished to the plain image using recreation organization to accomplish an image decryption process.

Alaa M. Abbas.[4] presented a Hash-BBS (HBBS) generator, a hashing version of BBS to take advantage of a hash function to support security for the creation of many key-streams. The statistical properties of the key bit-strings that resulted from each of the tested operations have been analyzed and verified using the NIST test suite. The bit strings that were produced had good randomness properties over the key length. A uniformly distributed binary sequence was produced as a result.

Li, Jian. [5] gave the work for the diagnosis and detection of internal diseases, such as breast cancer or lung cancer which aids the physicians in the treatment of medical conditions. It is difficult to guarantee image information security in public spaces due to the fact that medical images can be conveyed via a server or telecommunications network. In information security contemplations, advanced mark as well as individual plain images encryption keep information from being taken, altered, or looked by unapproved individuals. As a result, information security has emerged as a significant issue in the digital age. It provides right or left shift 2 n-1-pixel standards, an optimization-based organizer for combining binary equal cryptography processes, and hash transformation by multi-secret gold keys for medical imagine encryption and decoding to occur.

Ding, Yi. [6] presented medical image encryption and decryption, intelligent equal cryptography with a quantum-rooted key generator (KG) along with chaotic map. The scheme's overall processes include the generation of random cipher codes, training of an encryptor and decryptor, based on gray relational analysis (GRA), and the evaluation of the decrypted image. To produce 256 key-space, quantum-based KGs are utilized to rise the uncertain levels and chaotic complexity for moving the pixel values. The encryption is trained to become an encryptor and a decryptor using the first as well as second GRA models, respectively.

AL-Huseiny et al. [7] proposed the use of Deep Neural Networks (DNNs) to identify lung CT images with cancerous nodules. The method involves giving the input images a quick and easy pre-processing that isolates ROI, which are the parts of the lungs that dominate the image. This removes any other surrounding tissues or artifacts from the images. A DNN is then fed centered and size-normalized images for training and validation. GoogleNet DNN is adjusted using transfer learning to study this medical data. This incorporates restricting deep layers while permitting the DNN's final layers to evolve.

Reyad, Omar. [8] proposed a lung cancer detection method for analyzing CT image severity levels. By combining the nodule-extracted Linear Binary Pattern (LBP) and Local Directional Pattern (LDP), the Shape Local Binary Texture (SLBT) is utilized. The adaptive-salp-elephant herding optimization algorithm (adaptive-SEOA) for efficient model parameter exercise is applied to the features of DBN.

Jian-Xing Wu [9] LungNet based method was trained using medical IoT (MIoT) and CT scan data from wearable sensors. LungNet is a one-of-a-kind 22-layer CNN that improves the system's diagnostic accuracy by combining MIoT data and latent features learned from CT scan images.

Hsiang-Yueh Lai. [10] defined a Multiple Share Creation with Optimal Key Generation (MSC-OKG) procedure for secure medical communication. The approach primarily makes it possible for IoT devices to collect medical images. After that, the MSC process is used to generate Elliptic Curve Cryptography (ECC) along with multiple shares to further encrypt the shares. The OKG process gets carried performed through using Manta Ray Foraging Optimization (MRFO) technique. Thus, in this work an IVC scheme is presented by overcoming the presentation limitations forced by current image encryption algorithms.

- IVC supports a variety of real-time images, including medical images, Quick Response (QR) images, natural images, and it is applied for the (k, n) system along with the (n, n) system of VC.

- A new Error Decline Scheme (EDS) is followed by Reduced Error Filtering (REF) as well as Value Discretization Filtering (VDF)in order to give pixel values important sense in the IVC scheme.

- In addition, the embedding process's shares are selected in a chaotic sequence rather than at random in this work.

- The presentation analysis demonstrates that (k, n) SVC boosts PSNR and advances the of the reconstructed secret image. Pixel error is expressed as MSE.

- IVC keeps up with trustworthiness of the mystery image with no MSE without complex calculations.

3. Proposed Methodology

This part connects the IVC scheme with the EDS in order provide the pixel values significant meaning. A secret image

(SI) is processed by EDS to generate a signific secret image (SSI) with induced errors (IE). Thus, SSI is a meaningful image with clear pixel values. The EDS goal is to avoid pixel expansion issues, to lessen pixel replacement errors during SI reconstruction, to produce SSI, and to advance the share excellence. EDS uses the VDF and REF methods. The VDF strategy subtracts the grayscale SI from the coefficients of the pixels and determines the adjacent pixel error value that can be regularized to provide the pixel important meaning.

During the revealing phase, IE can be reversed to reconstruct the original SI. Then IE result is saved, with 0< 〖IE〗_(u,v)<th, th is the maximum threshold error for all pixel. The VDF strategy is represented in Equation (2). IE is cut down using the REF strategy. Based on the calculated IE, the REF method adaptively changes the pixel values. The Median Error Value (mev) is compared to each pixel value. In the event that 〖IE〗_(u,v) is more prominent than mev, the error should be decreased further. To locate the pixel value that is closest to being meaningful, the reduced error 〖RE〗_(u,v) is utilized. SSI is obtained by changing the pixel values by the EDS method. The following steps provide explanation of the EDS algorithm.

Step 1. At first a grayscale cellular in the lungs image and size M segments are breakdown. N columns lattice portrayal is measured as SI along with $0 \le SI(u,v) \le 255$. Steps 2 to 4 should be repeated for each and every pixel starting at (1, 1) coordinates.

Step 2. Utilize the VDF method to determine the $IE_{u,v}$ error value. Equations (1)& (2) are used to calculate IE.

$$DC_{u,v} = floor\left(\frac{SI_{(u,v)}}{100}\right) + floor\left(\frac{SI_{(u,v)}}{10}\right) mod\ 10 + SI_{(u,v)} mod\ 10 \quad (1)$$

$$IE_{(u,v)} = DC_{(u,v)} mod\ th\ \ 0 \le IE_{(u,v)} < th \quad (2)$$

Step 3. Using the DEF strategy, lower the error value to $RE_{u,v}$.The closest meaningful pixel values can be found using $RE_{u,v}$.

Step 4. Utilizing equation (3), subtract the reduced error value $RE_{u,v}$ from $SI_{(u,v)}$ to determine the new pixel values.

$$SSI_{(u,v)} = SI_{(u,v)} - RE_{(u,v)} \quad (3)$$

$$RE_{(u,v)} = \begin{cases} IE_{(u,v)} - th, & IE_{(u,v)} > mev \\ IE_{(u,v)}, & otherwise \end{cases}$$

Step 5. As a result, the pixel changes between SI and SSI range from 0 to mev, resulting in an improved image for securing the communication. After error reduction, the SSI maximum pixel range is found to be 252, and its value is max_r.

Step 6. In order for the resulting SSI to be significant, the pixel values must have the fewest errors possible. Equation (4) is used to calculate the RE percentage.

$$RE\% = \frac{max\{RE_{(u,v)}\}}{max\{SI_{(u,v)}\}} \times 100\ where\ 1 \le u \le M\ and\ 1 \le v \le N \quad (4)$$

3.1. Improved Visual Cryptography (IVC)

The IVC supports the (k,n) and (n,n) schemes, in which n denotes the count of generated shares and k denotes the least required shares needed to rebuild the secret. In this case, k is set to (n -1). Figure 1 depicts the proposed IVC's architecture[11].

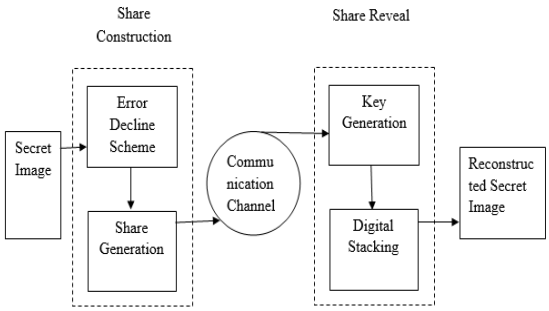

Fig. 1. Proposed IVC Architecture

The share construction and share revealing phases are described in detail below.

Consider the input $SI_{(u,v)}$ to be $0 \le SI_{(u,v)} \le 255$.

SI is transformed into SSI during the share construction phase, and share values are generated. Here IE is obtained by the EDS procedure utilizing equations (5 & 6).

$$IE_{(u,v)} = EDS\left(SI_{(u,v)}\right) \quad (5)$$

$$SSI_{(u,v)} = EDS\left(SI_{(u,v)}\right) \quad (6)$$

The Random Share Value (RSV) was developed from SSI and IE, haphazardly by equation (7 to 11). The SI sized random matrix known as $radkey$ was selected for the share values using the random function $rand()$.

$$radkey = rand(0,1) \quad (7)$$

$$RSV1_{(u,v)} = V_{(u,v)} where\ V_{(u,v)} \in \left\{\left(\frac{SI_{(u,v)}}{100}\right), \left(\frac{SI_{(u,v)}}{100}\right) mod\ 10, SI_{(u,v)} mod\ 10\right\} \quad (8)$$

$$RSV2_{(u,v)} = V_{(u,v)}$$

$$where\ V_{(u,v)} \in \left\{\left(\frac{SI_{(u,v)}}{100}\right), \left(\frac{SI_{(u,v)}}{100}\right) mod\ 10, SI_{(u,v)} mod\ 10\right\} - \left\{RSV1_{(u,v)}\right\} \quad (9)$$

$$RSV3_{(u,v)} = radkey_{(u,v)} \quad (10)$$

$$RSV4_{(u,v)} = IE_{(u,v)} \quad (11)$$

The LSB embedding process embeds RSVs in cover images by randomly swapping the smallest important bit with RSV_1, RSV_2, RSV_3 and RSV_4 to generate meaningful shares using an equation (12).

$$Sx_{(u,v)} = \left(Cx_{(u,v)} - mod\left(Cx_{(u,v)}, 10\right) + RSVx_{(u,v)}\right) where\ 1 \le x \le n \quad (12)$$

Where n is the quantity of offers along with determined by making a turbulent grouping as $CS(i)\ where\ i = 1\ to\ size\ of\ SI$. Then, the estimated number of chaotic share PCS pixels is computed in equation (13).

$$PCS = CS(i)\ mod\ 2 \quad (13)$$

Consequently, the division is then determined by attractive XOR action among the turbulent offer along with the SI as in equation (14)

$$share = PCS \oplus SI \quad (14)$$

Through a communication channel, participants are informed of the shares generated during the share construction stage. A key share is then created from the established shares during the revealing phase. To reveal the secret, the afresh produced share is signed with the determined shares.

In order to reconstruct the secret, there are four steps in the revealing phase. Initially, the LSB extraction process extracts the LSB from the received shares. The secret that is encoded into the Extracted Random Share Values (ERSV) is shown in equation (15).

$$ERSVx_{(u,v)} = \left(Sx_{(u,v)} mod\ 10\right)\ where\ 1 \le x \le n \quad (15)$$

Equation (16) is used to generate a new Key Share ($Shkey$) from the ERSV during the revealing phase.

$$Shkey_{(u,v)} = \begin{cases} th - \left(ERSV1_{(u,v)} + ERSV2_{(u,v)}\right), \\ \quad if\ ERSV1_{(u,v)} + ERSV2_{(u,v)} \le th \\ 2 \times th - \left(ERSV1_{(u,v)} + ERSV2_{(u,v)}\right), \\ \quad if\ ERSV1_{(u,v)} + ERSV2_{(u,v)} > th \\ 0 \quad ERSV1_{(u,v)} + ERSV2_{(u,v)} = 0 \end{cases} \quad (16)$$

By numerically loading the ERSVs along with the $Shkey$, the secret is exposed in this step using the (k, n) SVC equation (17).

$$RSSI_{(u,v)} = \begin{cases} Shkey_{(u,v)} \times 100 + IRSV2_{(u,v)} \times 10 + IRSV1_{(u,v)}, & IRSV3_{(u,v)} = 1 \\ IRSV2_{(u,v)} \times 100 + IRSV1_{(u,v)} \times 10 + IRSV1_{(u,v)}, & IRSV3_{(u,v)} = 0 \\ 0, & IRSV3_{(u,v)} > 1 \end{cases} \quad (17)$$

The IE will have Reconstructed Significant Secret Image (RSSI) from EDS. The (n, n) SVC scheme is used to reveal the secret in this step. A Transitional RSI (IRSI) is applied by prudently loading each of the n shares and Skey, utilizing equation (18). The original SI is reconstructed with the help of this IRSI using equation (19).

$$IRSI_{(u,v)} = \begin{cases} Shkey_{(u,v)} \times 100 + IRSV2_{(u,v)} \times 10 + IRSV1_{(u,v)} + IRSV4_{(u,v)}, \\ \quad IRSV3_{(u,v)} = 1 \\ IRSV2_{(u,v)} \times 100 + IRSV1_{(u,v)} \times 10 + IRSV1_{(u,v)} + IRSV4_{(u,v)}, \\ \quad IRSV3_{(u,v)} = 0 \\ 0, \quad IRSV3_{(u,v)} > 1 \end{cases} \quad (18)$$

$$RSI_{(u,v)} = \begin{cases} IRSI_{(u,v)} - th, & IRSV4_{(u,v)} > mev \\ IRSI_{(u,v)}, & otherwise \end{cases} \quad (19)$$

The SI and the Reconstructed Secret Image (RSI) are equal. Using various performance metrics, the SI is compared to RSSI as well as RSI, and the results are interpreted. Section 4 provides an explanation of the experiments and outcomes.

4. Results and Discussions

The chest X-ray images utilized in this work were taken from the NIH X-ray database. The NIH's download website offered access to these images for patient care. The hospital's storage system was used to accumulate and store chest X-ray images. Additionally, some secret cover images from MATLAB were also selected. The proposed security mechanism's simulation results were carried out in the MATLAB 2019a environment on a 64-bit Windows 11 operating system with an Intel core 5 processor. The SSIM, MSE, MAE and PSNR metric are utilized to evaluate the proposed IVC[12].

PSNR is an excellence estimation among the decoded and the original image. The reconstructed image quality's equated in with a higher PSNR equation (20).

$$PSNR = 10log_{10}\left(\frac{SI_{(max)^2}}{MSE}\right) \quad (20)$$

The grayscale SI's maximum pixel value is $SI_{(max)}$ v is 255 for an unsigned 8-bit integer data type. If the output image contains noise, then the two images are considered to be equal. MSE addresses the aggregate squared error between the remade image and the first SI. According to the formula in equation (21), a lower MSE value is obtained when the error in the reconstructed image is lower.

$$MSE = \frac{\sum_{M,N}\left[SI_{(m,n)} - RI_{(m,n)}\right]^2}{M \times N} \quad (21)$$

M, N addresses the quantity of lines as well as segments in the image. The SI pixel in the m^{th} row as well as n^{th} column is given by $SI_{(m,n)}$. $RI_{(m,n)}$ addresses the Remade Image pixel at m^{th} line and n^{th} segment.

Equation (22) indicates that MAE is a pixel value average change among the reconstructed and the original image.

$$MAE = \frac{\sum_{M,N}|SI_{(m,n)} - RI_{(m,n)}|}{M \times N} \quad (22)$$

The luminance, contrast, and structure terms are used to calculate the SSIM Index, a quality assessment metric. The sum of the three aforementioned terms is used to calculate the overall index as equation (23).

$$SSIM(m,n) = \frac{(2\mu_m\mu_n + C1)(2\sigma_{mn} + C2)}{(\mu_m^2 + \mu_n^2 + C1)(\sigma_m^2 + \sigma_n^2 + C2)} \quad (23)$$

The values of the original (m) as well as reconstructed (n) images are represented by μ_m, μ_n. The original as well as reconstructed image normal deviations are exposed by σ_m, σ_n, along with the covariance of the two images is exposed by σ_{mn}. SSIM have a range of values from -1 to +1. In this case, the value +1 indicates that the decoded and original images share each pixel values.

4.1. Comparative Analysis

The IVC results are recorded and comparison is done with the existing techniques. The reconstructed image quality with MSE as well as PSNR variables is depicted in Table 1.

Table 1. comparison of PSNR and MSE

Methods	PSNR	MSE
Halftone VC [23]	28.328	95.560
Multi-secret semantic VC [24]	33.214	31.023
SVC [22]	40.06	6.402
Proposed (k,n)	33.46	1.23
Proposed (n,n)	Inf	0

Table 1 displays the MSE and PSNR values of existing scheme as well as proposed schemes. Results for the lung cancer images using the proposed along with the existing methods are given. The table displays the proposed method has good security than the existing methodologies. The method in achieves a PSNR value as 28.328 dB and provides it up to 33.214 dB. The (k, n) IVC improves the excellence of the output image up to 7 dB likened to the other state-of-art VC schemes. The (k, n) IVC decreases the pixel errors other than the current VC methods[13]. The (n, n) system grades the MSE as zero as well as PSNR value as Inf. This shows that the original real time images and the reconstructed images are same such that there is no pixel losses.

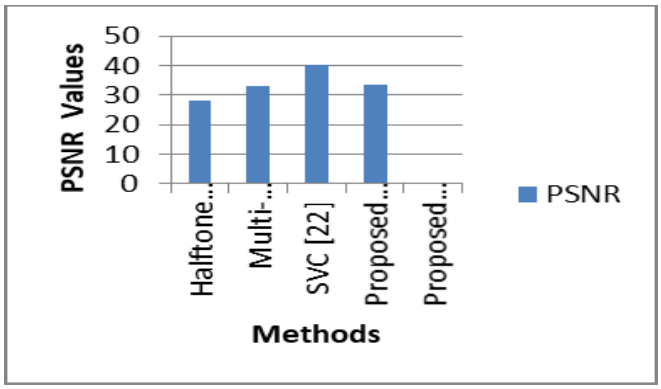

Fig. 2. Comparison of PSNR values

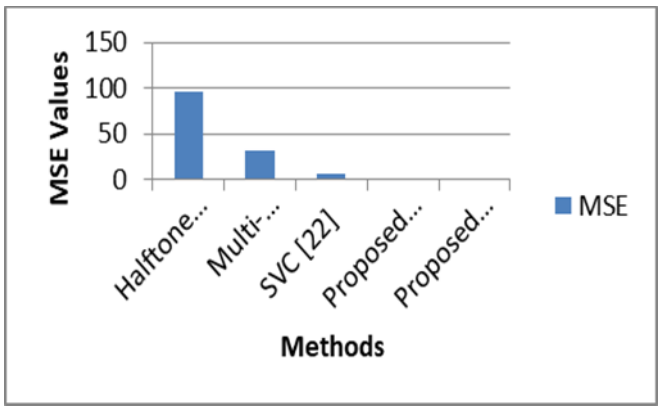

Fig. 3. Comparison of MSE values

Figure 2 and Figure 3 show the MSE and PSNR values of existing scheme as well as proposed schemes. Results for the lung cancer images using the proposed along with the existing methods are given. The table displays the proposed method has good security than the existing methodologies. The method in achieves a PSNR value as 28.328 dB and provides it up to 33.214 dB. The (k, n) IVC improves the excellence of the output image up to 7 dB likened to the other state-of-art VC schemes. The (k, n) IVC decreases the pixel errors other than the current VC methods[14]. The (n, n) system grades the MSE as zero as well as PSNR value as Inf. This shows that the original real time images and the reconstructed images are same such that there is no pixel losses.

Since shares resemble real-time natural images, it is impossible to guess whether a secret is present during share analysis. The share values are produced using chaotic sequence as well as are fixed with the protection pictures. This improves the share performance. This gives extra security for the protected transmission. Hence by these methods in CC one can transmit the secret safely when an intruder or attacker is present.

The chaotic sequence there is no chance of confusion are estimated by the share values. Because the share values are not chosen at random. Hence reconstruction of the secret during the close-fitting stage is the attacker gains access or

intruder to the shares. Consequently, the analysis of the MSE and SSIM indexes is done. The SSIM as well as MSE values are calculated among with the SI as well as the shares to ensure that the Secret is exposed by the separate shares. The SSIM as well as MSE index values for the original SI as well as shares are shown in Table 2. Here Sn is the last share.

Table 2. Analysis Of Mse And Ssim With Shares

Shares	SSIM	MSE
S1	0.00570	1751.95265
S2	−0.00011	1751.95265
S3	0.00369	1616.26162
Sn	-0.00008	1576.64356

There is a MSE of more than 1500 between SI and individual shares. The SSIM value is examined in a similar manner. The experimental result indicates that the values are unrelated and very close to zero. Hence the results prove that the proposed IVC scheme shows better security when compared to other approaches. The proposed method can thus be utilized to protect the medical images in the medical management system.

5. Conclusion

Two parameters are used to examine the effectiveness of the (k, n) as well as (n, n) IVCs in this study. First, the reconstructed image's quality is assessed. Finally, security is looked at in relation to incidents of cheating and attacks. By not expanding the images in space, humble mathematical operations are performed to decode the secret. In comparison to the existing VC schemes that are currently in use, the (k, n) SVC has produced the output image with a PSNR that is up to 24% higher and a MSE that is down to 79% per pixel. The reconstructed secret real time image produced by the (n, n) IVC is like that of original image in terms of integrity, demonstrating that the proposed IVC is effective and robust for grayscale images. An opportunity for future work focuses primarily on some other real-time cover images as well as grayscale secret.

References

[1] 2nd ed., G. Lima, Verusca S., Francisco Madeiro, and Juliano B. Lima. "Encryption of 3D medical images based on a novel multiparameter cosine number transform." Computers in biology and medicine 121 (2020): 103772.

[2] Tiankai, Sun, Wang Xingyuan, Jiang Daihong, Lin Da, Ding Bin, and Li Dan. "A robust authentication algorithm for medical images based on fractal Brownian model and visual cryptography." Scientific Programming 2020 (2020): 1-11.

[3] Memon, Nisar Ahmed, and Ali Alzahrani. "Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection." Ieee Access 8 (2020): 75448-75462.

[4] Al-Otaibi, May A., Hesham Alhumyani, Saleh Ibrahim, and Alaa M. Abbas. "Efficient Medical Image Encryption Framework against Occlusion Attack." Intelligent Automation & Soft Computing 34, no. 3 (2022).

[5] Li, Jian, Zelin Zhang, Shengyu Li, Ryan Benton, Yulong Huang, Mohan Vamsi Kasukurthi, Dongqi Li et al. "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology." BMC Medical Informatics and Decision Making 20 (2020): 1-16.

[6] Ding, Yi, Guozheng Wu, Dajiang Chen, Ning Zhang, Linpeng Gong, Mingsheng Cao, and Zhiguang Qin. "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things." IEEE Internet of Things Journal 8, no. 3 (2020): 1504-1518.

[7] Khan, Jalaluddin, Jianping Li, Amin Ul Haq, Shadma Parveen, Ghufran Ahmad Khan, Mohammad Shahid, Happy N. Monday, Sana Ullah, and Sun Ruinan. "Medical image encryption into smart healthcare IoT system." In 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 378-382. IEEE, 2019.

[8] Reyad, Omar, and Mohamed Esmail Karar. "Secure CT-image encryption for COVID-19 infections using HBBS-based multiple key-streams." Arabian Journal for Science and Engineering 46, no. 4 (2021): 3581-3593.

[9] Chen, Pi-Yun, Jian-Xing Wu, Chien-Ming Li, Chao-Lin Kuo, Neng-Sheng Pai, and Chia-Hung Lin. "Symmetric Cryptography With Shift 2 n-1, Hash Transformation, Optimization-Based Controller for Medical Image Infosecurity: Case Study in Mammographic Image." IEEE Photonics Journal 12, no. 3 (2020): 1-15.

[10] Lin, Chia-Hung, Jian-Xing Wu, Pi-Yun Chen, Hsiang-Yueh Lai, Chien-Ming Li, Chao-Lin Kuo, and Neng-Sheng Pai. "Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images Infosecurity." IEEE Access 9 (2021): 118624-118639.

[11] Lakshmanaprabu, S. K., Sachi Nandan Mohanty, K. Shankar, N. Arunkumar, and Gustavo Ramirez. "Optimal deep learning model for classification of lung

cancer on CT images." Future Generation Computer Systems 92 (2019): 374-382.

[12] AL-Huseiny, Muayed S., and Ahmed Sattar Sajit. "Transfer learning with GoogLeNet for detection of lung cancer." Indonesian Journal of Electrical Engineering and Computer Science 22, no. 2 (2021): 1078-1086.

[13] Shanid, Malayil, and A. Anitha. "Adaptive optimisation driven deep belief networks for lung cancer detection and severity level classification." International Journal of Bio-Inspired Computation 18, no. 2 (2021): 114-121.

[14] Berwer, Rajiv Kumar, Sanjeev Indora, and Dinesh Kumar Atal. "Blockchain-Based Medical Image Processing Mechanism." In 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), pp. 38-43. IEEE, 2022.

[15] Abdul Rahman, Artificial Intelligence in Drug Discovery and Personalized Medicine , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[16] Steffy, A. D. . (2021). Dimensionality Reduction Based Diabetes Detection Using Feature Selection and Machine Learning Architectures. Research Journal of Computer Systems and Engineering, 2(2), 45:50. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/32

[17] Juneja, V., Singh, S., Jain, V., Pandey, K.K., Dhabliya, D., Gupta, A., Pandey, D. Optimization-based data science for an IoT service applicable in smart cities (2023) Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities, pp. 300-321.