Journal of Computational Science and Intelligent Technologies
eISSN: 2582-9041
DOI: 10.53409/MNAA/JCSIT/e202203030113
Type: Research Article

Modified Leading Diagonal Sorting with Probabilistic Visual Cryptography for Secure Medical Image Transmission

Vijitha S[1] and Sreelaja Unnithan N[2]

[1,2]Department of Electronics and Communication Engineering, NSS College of Engineering, Palakkad, Kerala.
[*]**Corresponding Author: Vijitha S. Email: vijithamanoj@gmail.com**
Received: 2 March 2022; Accepted: 10 August 2022

Abstract: Information is sent through public networks, and the security of that information has been a top priority. Along with many other common cryptographic approaches, Visual Cryptographic (VC) techniques have also been applied to information and data security. As VC divides the original image into share photos in sequential sequence, a hidden secret image is revealed when the shares are stacked on top of one another. The secure VC technique divides a secret file or image into sharing images to encrypt it. A progression model for large-scale systems is cloud computing. From image recovery through image processing, storage, and retrieval with the progression of data in the medical sector and healthcare systems into the cloud, security for medical image transmission has been an ongoing computational concern. However, the use of cloud computing is restricted to situations where security is guaranteed. This study proposes Modified Leading Diagonal Sorting with Probabilistic Visual Cryptography (MLDS-PVC). The MIAS dataset's breast cancer mammography images are used in this study's medical images. The proposed model might allow for the cloud-based storage and transmission of medical image data between hospitals, diagnostic facilities, and other healthcare facilities.

Keywords: Visual Cryptography; Cloud Computing; Modified Leading Diagonal Sorting; Probabilistic Visual Cryptography; MIAS dataset.

1 Introduction

Visual cryptography is a cryptographic procedure that enables visual data (images, text, etc.) to be encoded so that the decoding can be performed by users (without Computers). Moni Naor and Adi Shamir, in 1994, created the main visual cryptographic technique. It included separating the images into n shares so just somebody with all n shares can decode the image by overlaying all the shares over one another. Essentially, this should be possible by printing every share on isolated transparency and setting each transparency over one other [1-2]. Figure.1 demonstrates the concept of visual cryptography. It functions as pursues: the secret image is selected, and it is encoded into various parts (called shares) utilising VC methods. At the point when the shares were printed over transparencies and accumulated combined (manually overlaid), human eyes do the decoding. This enables a normal individual to utilize the framework without cryptography knowledge and without executing any calculations. This was the visual cryptography's benefits over various mainstream cryptography techniques. The image comprises black/white pixels. The real secret image could be retrieved by overlaying both the shares [3-5].

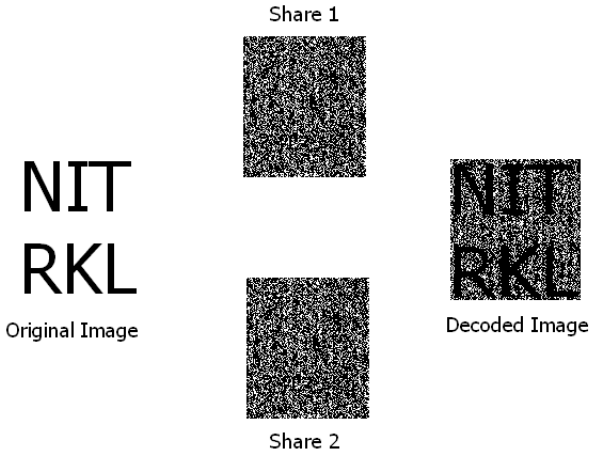


Figure 1: Working Representation of Visual Cryptography [1]

The concept was about creating image shares of a present hidden image such that the image shares seem insignificant. Retrieval of the image could be possible by overlaying the predetermined number of share images, and consequently, the decrypting method requires no specific tool or software. It can be easily done by human vision [6]. Visual cryptography is more advantageous for implementation when contrasted with regular cryptography methods; hence the decoding procedure does not require any algorithm. Further, the image-based data is more secure since the proposed receiver can uncover the real significance of the decoded image [7-10].

Cloud computing has become the most popular today, with a few points of interest over conventional figuring models. Average positive conditions include flexibility, adaptability, energy effectiveness, and cost-saving [11]. Cloud computing is a proficient computing model in which the computing architecture tools are present on the internet as services. Cloud computing has been viewed as another advancement in the growth of large-scale business IT, which could generate enormous resources from processing, storage, and applications and help users to take advantage of common, sufficient, and on-demand network access to a shared adaptive computing resource community with better productivity and reduced cost expenditure [12]. Extensive IT affiliations deliver more transparent cloud organizations to customers from independent to large companies worldwide, such as AMAZON AWS, Google cloud services, MS Azure, and Smart Cloud International Business Machines [13-15]. Our proposed model relies on private cloud computing, where the cloud computing process is executed with the private cloud implementation model. In the medical sector, medical services associations are oscillating to streamline and deal with patients and other clinical details in the cloud condition, as improvements are clear in healthcare management to minimize costs and improve clinical results. Due to the use of hardware and software with few undertakings, the extended measure of information in data storage applies to the continuous cloud computing system. Although the ability to store and retrieve data in the cloud has been improved for as long as a few years ago, the key conflicts are still posed by achieving two crucial points about data protection in medical services. The first step is to achieve high patient data protection status, and the second is to provide the patient with predictable data to ensure that the data quality is maintained.

2 Related Works

Archana B.D and Nitin J.J proposed a visual secret-sharing scheme for grayscale images using a visual cryptography technique. The first model was created only for bi-level, monochrome, or binary images and then upgraded for colour and grayscale images. The model was developed and analyzed based on colour decomposition methods. Using the visual cryptography (t, n) scheme, Sukumar R and Murali M created a secret image recovery method. In order to dynamically add new transparencies without regenerating and redistributing the initial transparencies, the scheme allows adjustments. Specifically, an expanded VC method was proposed based on base matrices and a probabilistic model. J Baek et al. proposed a stable

cloud computing framework for big data management in smart grids. A cloud computing-based model for smart grid management of big data offers scalability, flexibility, and security features. A secure solution was used for the proposed model based on identity-based encryption and proxy re-encryption systems, which provided the Smart-Frame with secure communication services.

Z Xia et al. used a Multi-keyword Ranked Search Scheme over Encrypted Cloud Data securely and dynamically. A special tree-based index structure and a "Greedy Depth-first Search" algorithm were used to provide a successful multi-keyword ranked search. To encrypt the index and query vectors, the stable kNN algorithm was used, thus ensuring accurate measurement of the relevance score between the encrypted index and query vectors. Crypto-based algorithms for secure image transmission were used by Ali Al-Haj et al. Strong cryptographic functions with symmetric keys and hash codes created internally were used. With the whirlpool hash function, the advanced encryption standard Galois counter mode was utilized to present secrecy and authenticity. The digital signature elliptic curve algorithm was utilized to provide authenticity and legitimacy.

3 Proposed Methodology

3.1. Modified Leading Diagonal Sorting with Probabilistic Visual Cryptography (MLDS - PVC)

The proposed research concentrates on the medical communication process with safety and privacy considerations between users or healthcare centres. Since medical records of patients are now stolen and misused in several respects, to solve those problems, the proposed research is executed. Safe login access is given between the users for accessing the cloud storage; the user has to log in with an authentication key to access the data in an approved way. The block diagram of the proposed model is shown in fig. 2.

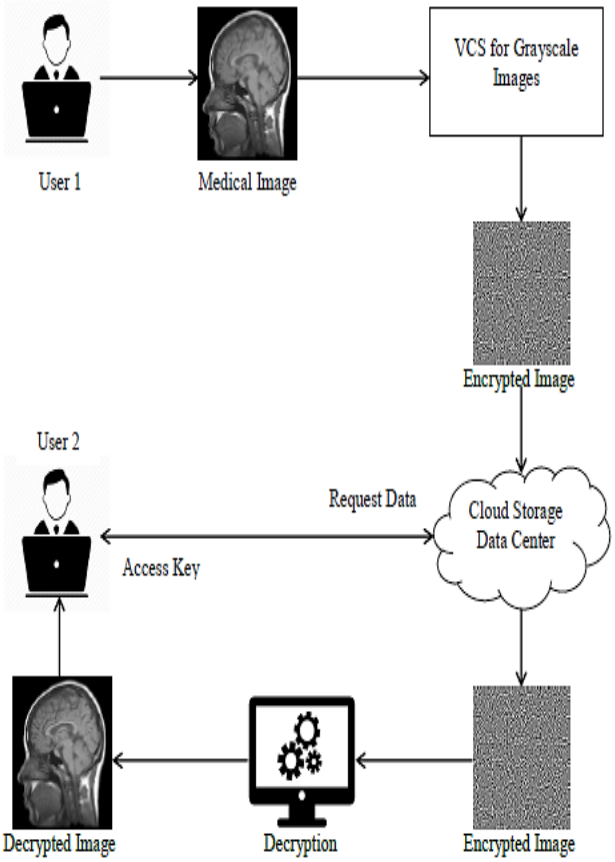


Figure 2: Block Diagram of the Proposed Method

For the data security method, visual cryptography was utilized to cover the original image with the cover image. After the user is authorized to use the details, the data must be decrypted to display the original

image. In addition, the visual cryptography method is used for encryption and decryption for safety and privacy purposes.

3.2. Modified Leading Diagonal Sorting

The proposed MLDS algorithm is implemented for the impulse noise removal in the input images before encryption, and it removes the noise at a noise density range from 10% to 90% noise density. It is correlated with the various impulse noise removal algorithms. It provides better performance results compared to the several standard algorithms. MLDS removes the noisy pixels with the diagonal element's median value in the case of all the elements in the diagonals are noisy. It eliminates the salt and pepper noise in both ways; first, it identifies the noise and then eliminates it. The present noise removal sorting technique was executed and correlated with the LDS and some standard methods for a higher noise density level from 10% to 90% [16].

The present sorting algorithm decreases the noise in a provided image. Fig. 3 represents the flow chart for the proposed model. The proposed model's steps and two cases (1) and (2) were utilized to identify and expel the noises were presented as follows

Case 1: If the whole selected part in the sliding window was impacted by the noise pixels and a mean value of the diagonal elements changed it.

Case 2: If any one or two parts were impacted by the noisy pixels '0' and '255', the relative pixel was changed by the selected element's median value.

Step 1: From the input image, choose $3 * 3$ sliding windows.

Step 2: Verify the left diagonal part of a presented sliding window, which was degraded by the noise or non-noisy element.

$$\text{if } p_{ij=0 \text{ and } p_{ij}=255} \text{ then case (1)condition satisfies}$$

$$\text{If not all processing pixel } p_{ij} \text{ is 0 and 255}$$

$$\text{then case (2)condition satisfies}$$

Step 3: Verify the right diagonal part of a presented sliding window, which was degraded by the noise or non-noisy element.

$$\text{if } p_{ij=0 \text{ and } p_{ij}=255} \text{ then case (1)condition satisfies}$$

$$\text{If not all processing pixel } p_{ij} \text{ is 0 and 255}$$

3.3. Illustration of MLDS in Input Image

Step 1: To verify if the left diagonal pixel in the chosen 3×3 window was impacted by noisy element 0 or 255

$$\begin{bmatrix} 12 & 142 & \langle 0\rangle \\ 0 & \langle 255\rangle & 26 \\ \langle 0\rangle & 255 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 12 & 142 & \langle 85\rangle \\ 0 & (85) & 26 \\ \langle 85\rangle & 12 & 0 \end{bmatrix} \quad (1)$$

From the above equation, processing pixels were 0, 255, and 0. So, each left diagonal element was impacted by noisy pixels '0' and '255'. So, change the left diagonal noisy pixels utilizing the case.1 Equ:

$$\frac{[0+255+0]}{3} = 85 \quad (2)$$

Step 2: To verify if the right diagonal part was degraded by noisy element 0 or 255.

$$\begin{bmatrix} \langle 12\rangle & 142 & 85 \\ 0 & \langle 85\rangle & 26 \\ 85 & 12 & \langle 0\rangle \end{bmatrix} \rightarrow \begin{bmatrix} \langle 12\rangle & 142 & 85 \\ 0 & \langle 85\rangle & 26 \\ 85 & 12 & \langle 12\rangle \end{bmatrix} \quad (3)$$

Left diagonal elements were 12, 85 and 0 and are shown in the above sliding window. In this window, '0' was intended as the noisy pixel. So, change the noisy pixel '0' by case.2 Equ:

$$\text{Case } 2 = \text{ median(right diagonal elements)} \quad (4)$$

The median value for the right diagonal element was obtained, and the noisy pixel '0' was changed by 12.

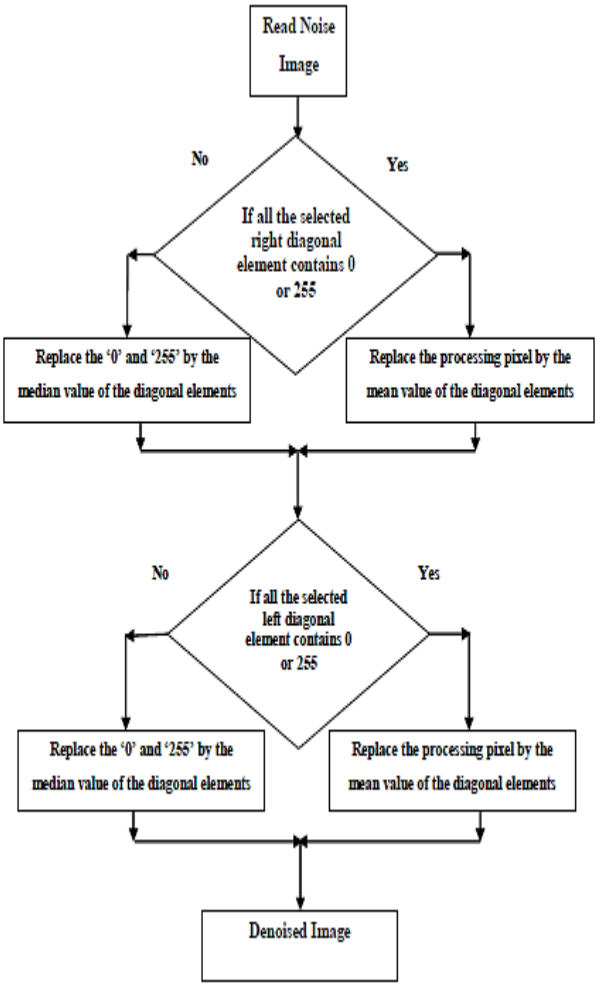


Figure 3: Flowchart of the proposed MLDS algorithm [16]

3.4. Probabilistic Visual Cryptography (PVC)

The PVC was based upon deterministic visual cryptography, and its actual reason was to create size-invariable shares, i.e., shares that possess a similar size as the hidden images. Ito et al. changed deterministic visual cryptography into a probabilistic equivalent. The matrixes D0 and D1 were equivalent to those created for deterministic visual cryptography. However, Ito et al. utilized it in a probabilistic manner. This algorithm was condensed in Algorithm1. Whether the two sets of matrices D_0 and D_1 were created by swapping sections of two basis matrices E_0 and E_1, at that point, one can securely pick $D_0 = E_0$ and $D_1 = E_1$ in Algorithm [17].

Algorithm (k, n)-threshold PVC:

Requirement:

Binary secret image: $x[n] \in \{0, 1\}$

Two sets of matrixes D_0 and D_1

Ensure:

n binary share images: $t_1[n], \ldots, t_n[n]$

1: Select randomly two matrix $D_0 \in D_0$ and $D_1 \in D_1$.

2: for every pixel n, do

3: if $x[n] = 0$ hence

4: d ← choose randomly one column of D0

5: else
6: d ← choose randomly one column of D1
7: end if
8: t_i [n] ← d_i, where i = 1,...,n.
9: end for

Utilizing the basis matrices,

$$E_0 = \begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}, E_1 = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \quad (5)$$

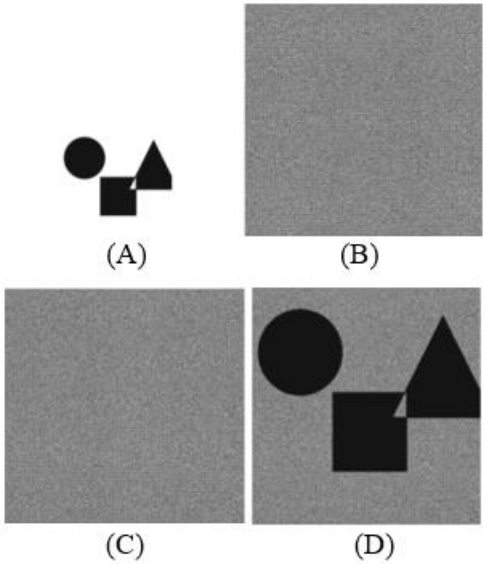


Figure 4: A) Secret Image, B) Share-1, C) Share-2, D) Target Image

The average contrasts seen on objective images were identical in contrast with the deterministic output. Yet, for deterministic visual cryptography, the black/white pixels were equally dispersed in the area according to hidden white pixels. Conversely, several black clusters are present for PVC. This was because of the probabilistic utilization of the basis matrix. The representation of secret, share and target images is shown in fig.4.

Yang technically determined the (k, n) threshold PVC method and developed a different solution. The meaning of this model can be defined as the fundamental of the PVC was two sets of vectors, D_0 and D_1. The components of every set were n-dimensional vectors. Assume that set D_0 includes v_0 vectors and set D_1 contains v_1 vectors, where v_0 may not be equivalent to v_1. For instance, if v = 3, the condition will be,

$$D_0 = \left\{\begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}\right\}, D_1 = \left\{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}\right\} \quad (6)$$

While sharing a hidden pixel t ∈ {0, 1}, a vector was randomly selected from D_t, and this vector's rows were swapped randomly. At that point, the i^{th} element was allotted to share i. For every vector d = $[d_1,..., d_v]^T \in D_i$, we can compute the stacking result R(d) = c_1 N ..., Nd_v. In this way, we have two sets R_0 and R_1 got from D_0 and D_1, individually, where

$R_i = \{R(d), \forall d \in D_i\}$, i = 0, 1. (7)

Every set R_i includes stacking results for each vector in set D_i.

If the accompanying two requirements are fulfilled, this method is called an (n, n) threshold PVC.

Contrast condition: Let p_w be the ratio of white pixels in the set R_w. At that point, the two sets D_0 and D_1 should satisfy $p_0 \geq p_{TL}$ and $p_1 \leq p_{TL} - \alpha$, for some threshold $p_{TL} > 0$ and contrast $\alpha > 0$.

Security condition: For q < k and any subset $\{i_1,...,i_q \subset \{1, 2,..., n\}$, the probabilities p_0 and p_1 must be equal. In particular, for every vector $d \in D_i$, if just the components are kept, whose index are in $\{i_1,...,i_q\}$,

we get two new sets $\hat{D}_0$ and $\hat{D}_1$, and two related sets $\hat{R}_0$ and $\hat{R}_1$. The p_0 and p_1 got from $\hat{R}_0$, and $\hat{R}_1$ must be the same.

4 Performance Analysis

4.1. Dataset Description

This work used the Mammographic Image Analysis Society (MIAS) Mini MIAS Database from London's Royal Marsden Hospital. The database of the MIAS was utilized to collect the images. The MIAS database contains 322 images belonging to the seven groups, as shown in the table.1. The 322 images are divided into 207 normal images, 115 images are unpredictable, and the form and risks are independent of the abnormal images 64 and 51. The resolution of each image is 1024x1024 pixels [18].

Table 1: MIAS Dataset

KIND	BENIGN	MALIGNANT	TOTAL
Normal tissue	-	-	207
Speculated masses	11	8	19
Architectural distortion	9	10	19
III-defined masses	7	7	14
Asymmetry lesion	6	9	15
Micro-calcification	12	13	25
Circumscribed masses	19	4	23
Total	64	51	322

In this section, the results of the visual cryptography technique for secure cloud-based medical image transmission are presented. The proposed model's step-by-step process is implemented and represented with relevant images.

4.2. Experimental Results of Noise Removal before Encryption and after Decryption in Input Image

The performance metrics are tested with the breast cancer mammography images with 256×256 before encryption and after decryption. The noise density ranges from 10 Hz to 90 Hz and is added to the standard images and evaluates the proposed method. The PSNR, MSE, SSIM & IEF analysis of the performance metrics of noise cancellation of the proposed MLDS technique before encryption is tabulated below in Table 2.

Mean Square Error (MSE): MSE is the most common parameter for measuring image quality. It is a full reference metric, and the values closer to zero are the better. MSE was expressed in equation (8). Lesser the MSE better the outcome.

$$MSE = \frac{1}{xy}\sum_{i=0}^{x-1}\sum_{i=0}^{y-1}(I_{ij} - D_{ij})^2 \quad (8)$$

Peak Signal-to-Noise Ratio (PSNR): PSNR was contrary to MSE; the higher the PSNR better the outcome.

$$PSNR = 10 \times \log_{10}\frac{255^2}{MSE} \quad (9)$$

SSIM relates to the similitude between the recovered image and the real image. It is a quality proportion of one image when contrasted with others viewed as of better quality. It is in the structure of fraction; in this way, the closer the value of SSIM to one, the more comparative the recovered image is to the real image and, subsequently, the better outcome.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (10)$$

IEF shows the performance of the filter under various noise densities. IEF shows the relative quality enhancement of the image displayed by the filter processing.

$$IEF = \frac{\sum[g(i,j)-f(i,j)]^2}{\sum[f'(i,j)-f(i,j)]^2} \quad (11)$$

Table 2: Performance Metrics of Noise Cancellation using MLDS technique (Before Encryption)

Noise density Hz	PSNR dB	MSE dB	SSIM	IEF
10	15.312	2.47E+03	0.9512	0.978
20	12.3749	4.86E+03	0.8931	0.9515
30	10.5667	7.35E+03	0.8236	0.9189
40	9.2963	9.89E+03	0.749	0.879
50	8.3128	1.21E+04	0.665	0.8319
60	7.5445	1.46E+04	0.5676	0.7759
70	6.8701	1.70E+04	0.4629	0.7079
80	6.2803	1.94E+04	0.3445	0.6344
90	5.7577	2.17E+04	0.2068	0.5355

The performance analysis of the PSNR, MSE, SSIM and IEF parameters are evaluated for the image used before encryption with noise cancellation with the proposed model. The noise density is varied simultaneously to calculate the performance metrics of the noise cancellation with the proposed parameters. The noise density is varied step by step from 10Hz to 90Hz. Figure. 5 (a) shows the user registration process for accessing the system for safe transmission over the cloud platform. Fig.5 (b) shows the user's login process; after the registration, the user has to use unique login credentials for safer transmission. Figure.6 (a) shows the original medical image uploaded and figure.6 (b) shows the share image-1 generated using cryptography and is also represented in fig.7 (a) as share-2. Figure. 7 (b) represents the encrypted image, the stacked image of share-1 and share-2 images. That stacked image of shares 1 and 2 is represented in figure 8 (a).

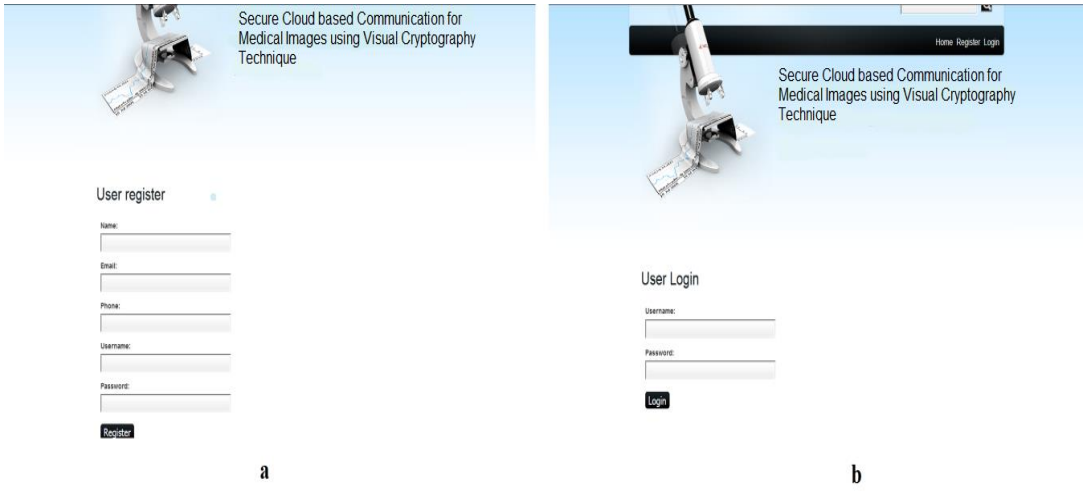


Figure 5: a) User Registration Process, b) User Login Process

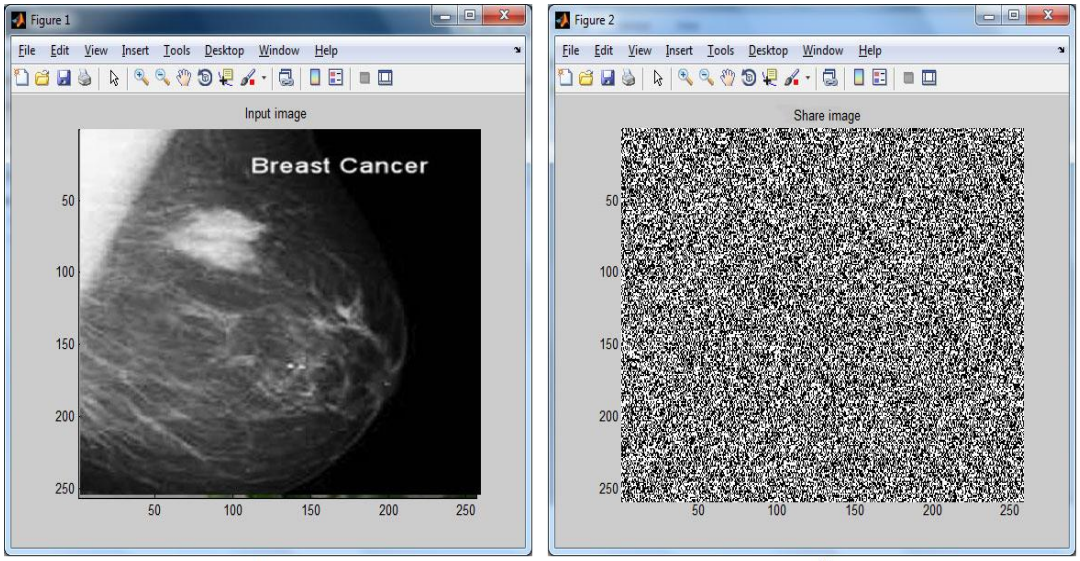


Figure 6: a) Original Medical Image, b) Share Image 1

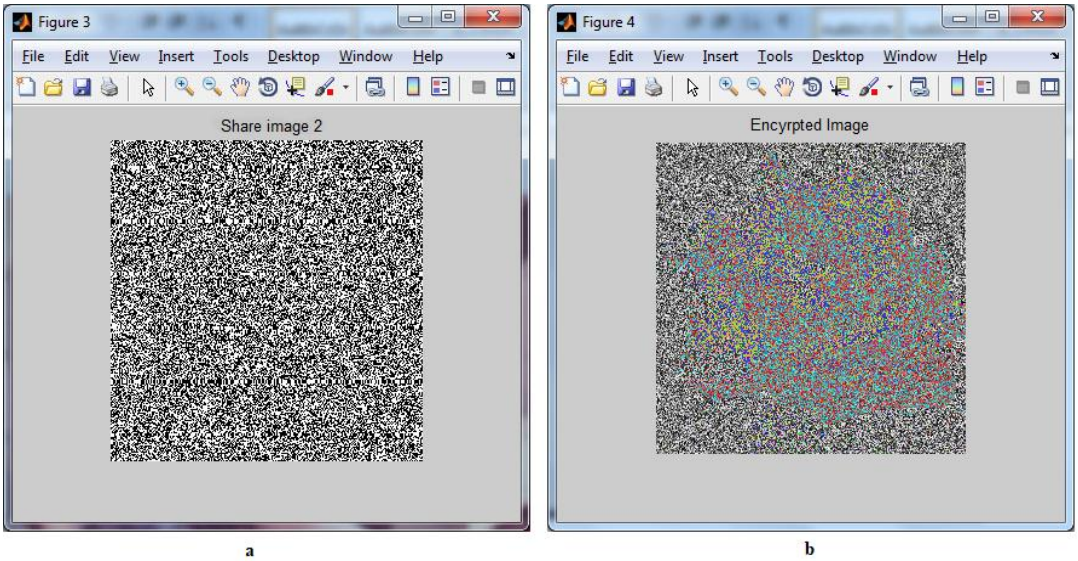
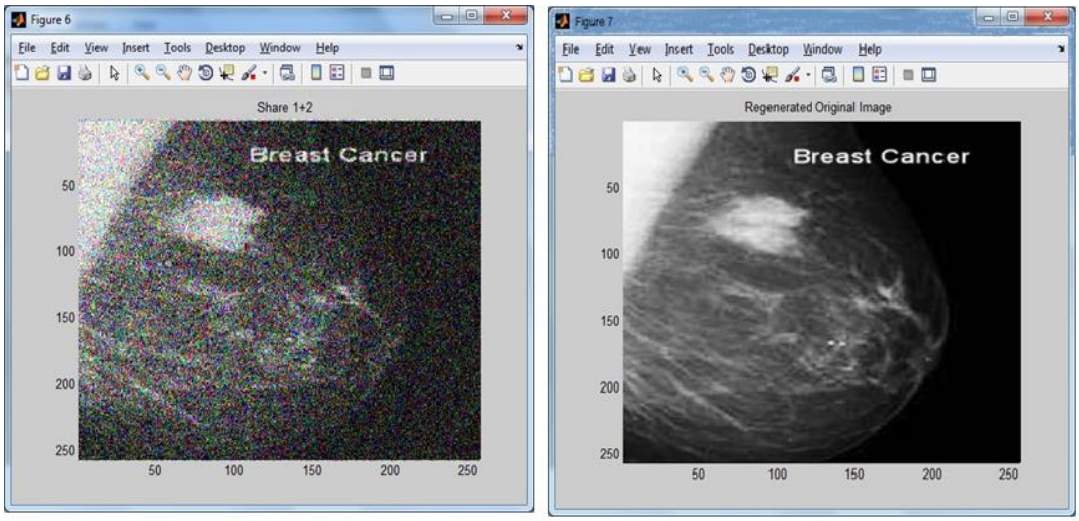


Figure 7: a) Share Image 2, b) Encrypted Image

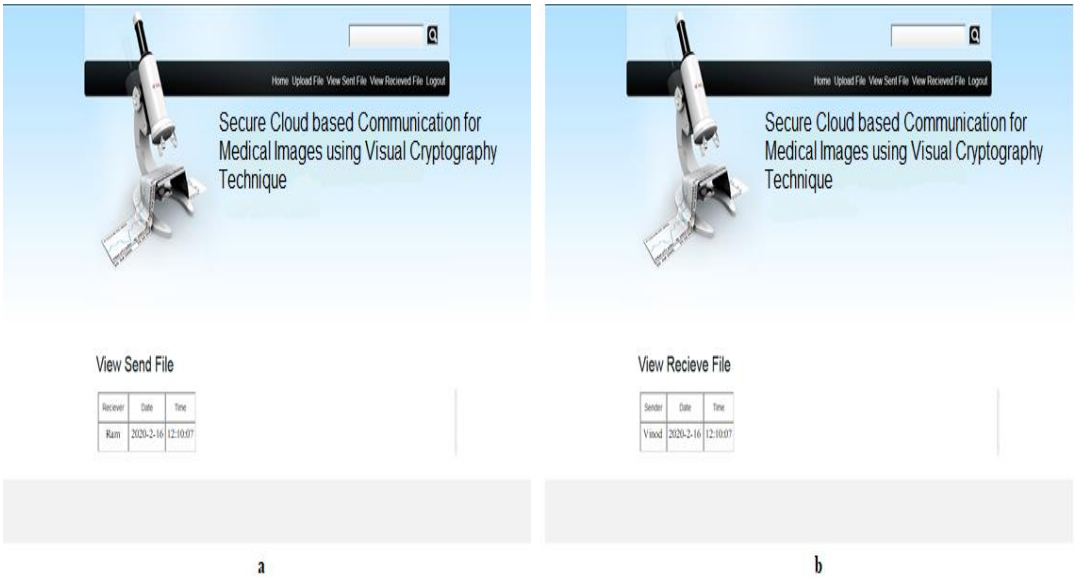
The encoded image was stored in the cloud using the Cloud Php platform after using the proposed algorithm. After the receiver uses the sender's encryption key, the encrypted image will be decrypted using the same algorithm. Figure 8(b) shows that the receiver will obtain a regenerated original image.

The sender and recipient should also verify the specifics of the files used in this safe communication medium. As shown in figure.9, the files utilized for transmission are displayed with the user name, time & date of the operation.



a) b)

Figure 8: a) Share 1+2 Image, b) Decrypted Image



a b

Figure 9: a) Transferred Files Details, b) Received Files Details

Table 3: Performance Metrics of Noise Cancellation using MLDS technique (After Decryption)

Noise density Hz	PSNR dB	MSE dB	SSIM	IEF
10	16.1320	3.47E+03	0.9632	0.9778
20	13.7149	5.86E+03	0.8931	0.9615
30	11.6267	9.35E+03	0.8736	0.9389
40	10.9363	10.89E+03	0.7249	0.8379
50	9.3428	2.21E+04	0.6365	0.8419
60	8.4455	2.46E+04	0.5776	0.7659
70	7.7801	2.70E+04	0.4729	0.7279
80	7.8303	2.94E+04	0.3345	0.6444

90	6.7777	3.17E+04	0.2168	0.5465

As shown in the above table.3, the performance metrics of noise cancellation of the proposed method after decryption are computed. Similar to the previous noise cancellation process before the encryption process is carried out here. The computation is evaluated by varying the noise density from 10Hz to 90Hz.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \% \quad (12)$$

$$\text{Sensitivity} = \frac{TP}{TP+FN} \% \quad (13)$$

$$\text{Specificity} = \frac{TN}{TN+FP} \% \quad (14)$$

$$\text{PPV} = \frac{TP}{TP+FP} \quad (15)$$

$$\text{NPV} = \frac{TN}{TN+FN} \quad (16)$$

The accuracy is referred to as the percentage of correctly identified results. The accuracy of the proposed MLDS-PVC obtained 98.99%, which is better than other techniques in this work, as represented in table.4. The sensitivity is the measure of the true positive rate. It is also known as recall in some cases. The proposed technique achieved a 90.76% sensitivity rate. The specificity is the measure of the proportion of noisy images that are correctly identified. It is also termed as True Negative Rate. The proposed MLDS-PVC attained an 86.23% specificity rate.

PPV is the percentage of images with a test positive, which have the noise. It represents how many test positives were TP; if it is higher (as close to 100 as possible), then it indicates that the results are better.

NPV It is the percentage of images with a test negative, which do not have the noise. It represents how many test negatives were TN; if it is higher (should be close to 100), then it indicates that the results are better.

Table 4: Comparison of Performance of MLDS-PVC with other Techniques

Algorithm	**Accuracy**	**Sensitivity**	**Specificity**	**PPV**	**NPV**
MLDS-PVC	98.99	90.76	86.23	88.7	96.4
NNVC	94.52	88.21	78.22	92.3	79.0
PSOVC	94.33	88.10	78.11	81.6	76.5
ABCVC	93.33	87.43	77.44	87.1	66.7
FVC	92.24	86.45	76.36	86.9	98.1
ANFISVC	92.20	85.89	75.38	84.0	77.7
GSOVC	92.01	84.91	74.17	84.0	73.5

The graphical representation of the evaluated results is shown in fig.10, which represents that the proposed Modified Leading Diagonal Sorting with Probabilistic Visual Cryptography (MLDS - PVC) technique accomplished better results in all the parameters proposed in this work compared with other existing techniques.

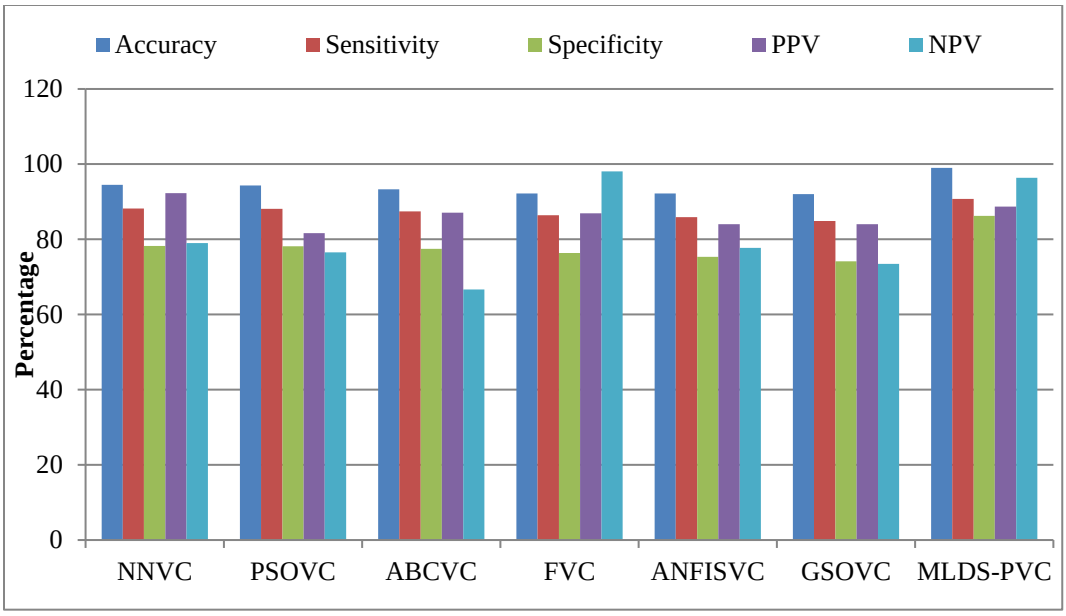


Figure 10: Graphical representation of the Results

5 Conclusion

Through the combination of visual cryptographic technique and cloud computing, the proposed model is developed using the Modified Leading Diagonal Sorting with Probabilistic Visual Cryptography (MLDS - PVC) technique for both the process of encryption and decryption. The medical image was encoded with share images and uploaded to the cloud storage, where the medical image was recovered and converted for diagnosis without any loss in the process. The entire operation was performed through a secure and protected medium with the support of accessing the database using authorized login credentials. The user can access the medical records via the authorized login anytime and anywhere. Finally, the proposed research was concluded as a successful cloud-based medical data transmission strategy. In future, the proposed model can be utilized for data transmission applications in various domains.

Acknowledgements: The authors thank their families and colleagues for their continued support.

Funding Statement: The author(s) received no specific funding for this study.

Availability of Data and Materials: The data used to support the findings of this study can be obtained from the corresponding author upon request.

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

References

[1] Dipesh Vaya, Sarika Khandelwal, and Teena Hadpawat, "Visual Cryptography: A Review," Int J Comput Appli, Volume 174 – No.5, pp.40-43, 2017.

[2] R. Sun, Z. Fu and B. Yu, "Size-Invariant Visual Cryptography With Improved Perceptual Quality for Grayscale Image," in IEEE Access, vol. 8, pp. 163394-163404, 2020.

[3] A B. Dhole and N J. Janwe, "Visual Cryptography in Gray Scale Images," Int J Eng Res Develop, Volume 8, Issue 4, pp.65-68, 2013.

[4] M. S Reddy and S. M Mohan, "Visual Cryptography Scheme for Secret Image Retrieval," Int J Comput Sci Net Secur, Vol.14 No.6, pp.41-46, 2014.

[5] S. Guo, T. Xiang, X. Li and Y. Yang, "PEID: A Perceptually Encrypted Image Database for Visual Security Evaluation," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1151-1163, 2020.

[6] F Baby, Arun R, and S S Babu, "ViCry: Visual Cryptography Schemes for Security (An overview of different types of visual cryptography schemes)," International Conference on Emerging Trends in Engineering & Management, IOSR J Comput Eng, pp.15-18, 2016.

[7] B. Han, Y. Jia, G. Huang and L. Cai, "A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 2644-2648, 2020.

[8] Ito R, Kuwakado H, and Tanaka H, "Image size invariant visual cryptography," IEICE Trans Fundam, E82-A(10), pp.2172–2177, 1999.

[9] S. Ali and C. Adnen, "Implementation of a Cryptography Algorithm for Image Transmission," 2019 IEEE 19th Mediterranean Microwave Symposium (MMS), pp. 1-6, 2019.

[10] Yang C.N, "New visual secret sharing schemes using probabilistic method," Pattern Recognit Lett, 25(4), pp.481–494, 2004.

[11] B. Pushpa, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 329-334, 2020.

[12] C Modi, D Patel, B Borisaniya, A Patel and M Rajarajan, "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," Springer, J Supercomputing, Vol.63, No.2, pp.561–592, 2013.

[13] J Baek, Q H Vu, J K. Liu, X Huang and Y Xiang, "A Secure Cloud Computing based framework for Big Data information management of smart grid," IEEE T Cloud Comput, Vol.3, No.2, pp.233-244, 2013.

[14] Z Xia, X Wang, X Sun and Q Wang, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE T Parallel Distribut Sys, Vol.27, No.2, pp.340-352, 2015.

[15] C Liu et al., "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates," IEEE T Parallel Distribut Sys, Vol. 25, No.9, pp.2234-2244, 2014.

[16] R.Rajkumar, S.Saira Banu and K.G.Padmasine, "Impulse Noise Removal Using Enhanced Efficient Leading diagonal Sorting Algorithm," Int J Advan Inform Sci Technol (IJAIST), Vol.5, No.7, pp.118-128, 2016.

[17] Ali Al-Haj, Gheith Abandah, and Noor Hussein, "Crypto-based algorithms for secured medical image transmission," IET Information Security, Vol.9, No.6, pp.365-373, 2015.

[18] https://www.kaggle.com/kmader/mias-mammography