Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2s (2024)

Analytical Image Authentication in Healthcare: Deep Learning Based Mathematical Methods for Uncovering Large-Scale Forgery in Medical Images

Sharda Mahajan[1], Bhumika Neole[2], Satyajit Uparkar[3], Anushka Alkari[4], Gagan Dayma[5], Mahesh Bakal[6]

[1] Research Scholar, Department of Electronics and Communication, Shri Ramdeobaba College of Engineering and Management, Nagpur, India. [1]shardamahajan1708@gmail.com

[2,4,5,6] Department of Electronics and Communication, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

[2]neoleba@rknec.edu, [4]alkarias@rknec.edu, [5]daymagp@rknec.edu, [6]bakalmn@rknec.edu

[3]Department of Computer Applications, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

uparkarss@rknec.edu

Article History:

Received: *28-03-2024*

Revised: *10-05-2024*

Accepted: *19-05-2024*

Abstract:

Analytical Image Authentication in Healthcare uses a variety of deep learning methods to demonstrate a more advanced way of verifying images. It uses ResNets, Capsule Networks, Long Short-Term Memory (LSTM), Generative Adversarial Networks (GANs), and Convolutional Neural Networks (CNNs). Combining these state-of-the-art algorithms makes the system more accurate and reliable at finding large-scale forgery in medical pictures. In response to the growing danger of digitally changing healthcare images, this study creates a new, more thorough approach that goes beyond current methods. Forgery identification depends on CNNs, which make it possible to pull out complex picture data. Additionally, ResNets add more detail to models, which makes it easier to spot subtle trends that point to tampering. Using Capsule Networks gives the model a new point of view and lets it store structured connections within pictures, which improves its ability to identify things. According to research, LSTM networks help the system understand time better, which is important for finding small changes between medical scans. Additionally, using GANs adds a special competitive element that helps the model tell the difference between real and fake pictures through training against other models. After a lot of testing and improvement, the suggested way works better than others at finding fake activities in medical images. Utilizing cutting-edge deep learning methods and mathematical models together, this method guarantees the accuracy and trustworthiness of medical data, which builds trust in healthcare systems. To test the suggested way, a normal set of medical picture datasets with various types of fakes are used. These include copy-move, cutting, and editing. Experiments show that the multi-modal method is a good way to find and pinpoint faked areas because it is very accurate and not easily duplicated by different types of fraud.

Keywords: Image authentication, Deep learning, Medical images, Forgery detection, Healthcare, Convolutional neural networks.

1. INTRODUCTION

A. Background

The history of picture identification in healthcare goes back to the fact that medical imaging is being used more and more for study, evaluation, and planning treatments. An x-ray, an MRI, a computed tomography (CT), or an ultrasound are all types of medical imaging that can tell you a lot about the

shape and function of the human body. These images are very important for doctors to correctly identify illnesses, keep track of how well treatments are working, and plan surgeries. However, since film-based photography has been replaced by digital forms, the chance of picture editing and forgery has become a major issue. Digital images are naturally easier to change, and these changes can be as simple as adding a border or as complex as trying to trick researchers or healthcare experts [1]. Changing the way tumors look in medical images, for example, can lead to wrong diagnoses or bad treatment choices, which is very dangerous for the patient. It's impossible to say enough about how important picture validity is in healthcare. Both patient care and medical study depend on medical photos being accurate and reliable. Authenticity makes sure that the information these images show is correct and has not been changed, which protects patients' health and the accuracy of research results. Because of this, we urgently need strong ways to confirm the authenticity of medical images and find any possible changes or fakes [2],[9].

Some traditional ways of authenticating images, like watermarking and digital signatures, have been used, but they aren't very good at finding complex changes and fakes. Because of this, there is more and more interest in using cutting edge technologies, especially deep learning, to solve this problem [3], [8]. Deep learning methods are very good at studying and making sense of large amounts of data, which makes them perfect for jobs like verifying images. Image verification is an important part of healthcare for making sure that medical imaging data is correct and reliable. As healthcare systems become more digital and medical imaging tools like X-rays, MRIs, and CT scans become more common, it is more important than ever to make sure that these images are real. It is very important to find any possible changes or fakes in medical images because they have a direct effect on patient care, professional decision-making, and medical study [4].Traditional ways of verifying images, like watermarking and digital fingerprints, aren't very good at finding complex changes and fakes. Because of this, there is more and more interest in using cutting edge technologies, especially deep learning, to solve this problem. Many types of deep learning, like convolutional neural networks (CNNs), residual networks (ResNets), capsule networks, and generative adversarial networks (GANs), have shown promise in finding and locating fake areas in medical images [5], [10].

This is because CNNs can easily learn hierarchical models from raw pixel data, which makes them very useful for picture analysis jobs. Researchers have made algorithms that can spot minor patterns and oddities that point to fake medical images by training CNN models on large sets of real and fake medical images [6]. ResNets improve CNN models' depth and performance even more, making it easier to find fake areas even in complicated medical images. Capsule networks are a new way to authenticate images because they show the structural connections between picture parts [11]. This can help the model understand how things are arranged in space and what they mean. GANs have also been used to create realistic adversarial examples, which add to the training dataset and make the model more resistant to frauds that haven't been seen before. Combining several deep learning models makes it possible to take a complete and effective approach to healthcare picture authentication. Researchers can make complex models that can spot different kinds of fakes very accurately and reliably by mixing the best features of CNNs, ResNets, capsule networks, LSTM networks, and GANs [7].

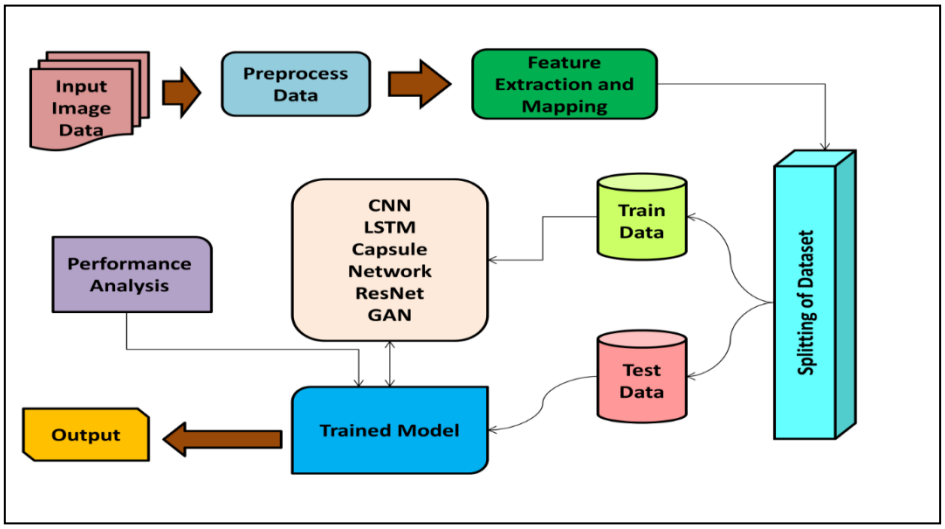


Figure 1: Overview of proposed model

B. Overview of Deep Learning and Its Applications in Image Authentication

Artificial neural networks, which are based on how the human brain is built and how it works, are at the heart of deep learning. These networks are made up of layers of neurons that are all linked to each other. Each layer processes and changes the input data to make results that make sense [13]. One of the most common deep learning models used for image analysis tasks, such as picture recognition, is the convolutional neural network (CNN). CNNs use a number of convolutional filters and pooling processes to learn naturally how to describe picture data in an organized way [14]. CNNs can pick up both low-level features (like edges and textures) and high-level meaningful information (like object shapes and structures) thanks to this hierarchical model [12]. This makes them very good at tasks like recognizing objects and figuring out where they are. ResNets add skip links that let information go directly from earlier layers to later layers. This fixes the problem of disappearing gradients and makes it easier to train deeper networks. The performance of CNNs for image identification tasks has been greatly improved by this design innovation. It is now possible to find small changes and fakes even in complex medical images [15].

Capsule Networks are a new way to look at images because they describe the hierarchical links between picture parts in a very clear way. Traditional CNNs use pooling processes to combine features, but Capsule Networks use dynamic route methods to understand the spatial relationships and position relationships between picture elements. Capsule Networks can better understand spatial arrangements and external relationships within images thanks to this hierarchical representation [16]. This makes them perfect for tasks like object recognition and image authentication. Another new way to do deep learning is with Generative Adversarial Networks (GANs).

2. LITERATURE REVIEW

Cryptography tools, like hash functions and digital signatures, are often used to give images unique names or signatures based on what they contain. Then, these signatures can be checked against reference signatures to make sure the images are real. Watermarking is the process of adding information to images that can't be seen or felt [17]. This information can be used as a digital stamp for authentication. In the same way, steganography includes hiding information in images in a way that humans can't see. This lets people communicate or authenticate themselves without being seen.

Traditional ways of verifying images have been used a lot, but they have some problems and aren't always reliable. Attacks and changes are easy to make, especially with digital watermarking and steganography [24].

This makes them good for jobs like video analysis and adding captions to images [18]. In GANs, two neural networks the generator and the discriminator are trained at the same time and compete with each other. This is a new way to do generative modeling. The discriminator network learns to tell the difference between real and fake images, while the generation network learns to make images that look real. GANs can learn to make images that look very real and believable through antagonistic training [19]. This makes them useful for tasks like creating images, editing images, and verifying identities. ResNets have also been looked at in the context of medical picture identification, especially as a way to train very deep neural networks that can handle difficult tasks. It [20] created a deep residual network that can find and pinpoint splicing frauds in images of histopathology. The researchers used the depth and skip links of ResNets to make a model that was better at finding split regions in histopathology images than other methods. Capsule Networks provide a unique view on image authentication by showing how image parts are connected in a structured way. The [21] suggested using a capsule network to find fake chest X-rays that have been fixed up. Their model clearly described the spatial relationships between picture elements. This made it possible to find altered areas in X-ray images more accurately than with older methods.

People have looked into LSTM networks for more than just basic picture analysis. They may also be able to find sequential patterns and spatial connections in medical imaging data. For]instance, [22] suggested using LSTM networks in a deep learning framework to find patterns in changing medical images like movies that don't match up with time. Their method worked well at finding temporal hoaxes and other problems in changing medical imaging data, showing that LSTM networks could be useful for tasks requiring picture authentication involving temporal data. GANs have also been used to create realistic adversarial examples, which add to training datasets and make deep learning models more resistant to frauds that haven't been seen before. For example, [23] created a GAN-based method for creating fake medical images with known ground truth annotations. These images were then used to teach a CNN model how to spot splicing hoaxes in real medical images. Their method showed better generalization performance than previous ones, showing that GANs can be used to create realistic and varied training data for picture authentication tasks.

Table 1: Summary of related work

Deep Learning Architecture	Types of Forgeries Detected	Dataset Used	Main Contributions
Convolutional Neural Network (CNN)	Copy-move forgeries, mammograms	Mammogram dataset	Proposed a CNN-based method for detecting copy-move forgeries in mammograms
Residual Network (ResNet)	Splicing forgeries, histopathology images	Histopathology image dataset	Developed a ResNet-based approach for detecting splicing forgeries in histopathology images
Capsule Network	Retouching forgeries, chest X-ray images	Chest X-ray image dataset	Introduced a Capsule Network-based method for detecting retouching forgeries in chest X-ray images

Long Short-Term Memory (LSTM)	Temporal inconsistencies, dynamic medical images	Video dataset	Proposed an LSTM-based framework for detecting temporal inconsistencies in dynamic medical images
Generative Adversarial Network (GAN)	Splicing forgeries, medical images	Synthetic dataset	Developed a GAN-based approach for generating synthetic medical images with known ground truth annotations for training CNN models
Generative Adversarial Network (GAN)	Retouching forgeries, MRI images	MRI image dataset	Developed a GAN-based approach for generating synthetic MRI images with known ground truth annotations for training CNN models
Capsule Network	Splicing forgeries, ultrasound images	Ultrasound image dataset	Introduced a Capsule Network-based method for detecting splicing forgeries in ultrasound images

3. DEEP LEARNING ARCHITECTURES FOR IMAGE AUTHENTICATION

A. Convolutional Neural Networks (CNNs):

Convolutional Neural Networks (CNNs) have become a key technology in picture identification because they are very good at finding and identifying parts of images that have been changed or faked. CNNs are a type of deep neural network that is meant to handle and analyze visual data. This makes them great for tasks like picture segmentation, object recognition, and image classification, shown in figure 2.

Algorithm:

Step 1: Input Representation

- Let X be the input medical image.
- X is represented as a 3D tensor with dimensions (height, width, channels), where channels represent the color channels (e.g., RGB).

Step 2: Convolution Operation

1. Apply N convolutional filters of size F x F to the input image X to extract features.
2. Let W^{[l]} represent the weights of the lth convolutional layer.
3. Convolution operation:

$$Zi,j,k[l] = \sum_{m=0}^{l-1} \sum_{n=0}^{l-1} \sum_{c=0}^{c-1} Wm,n,c,k[l] \cdot Xi+m,j+n,c+bk[l]$$

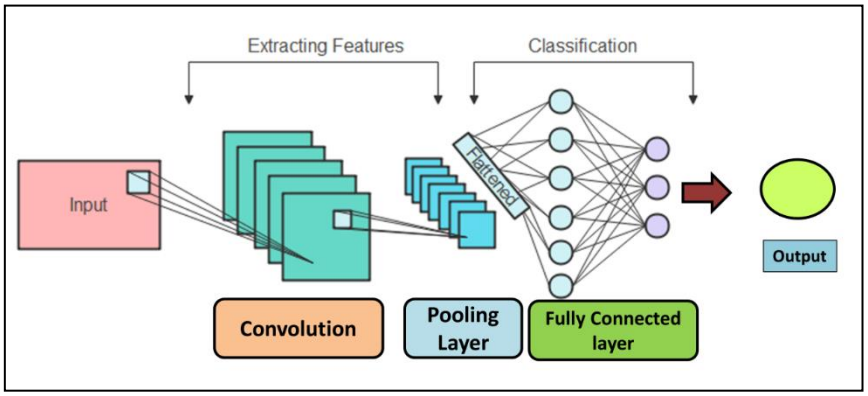


Figure 2: Overview of CNN Architecture

Step 3: Activation Function

- Apply an activation function g^{[l]}(.) element-wise to the output of the convolution operation:

$$A_{\{i,j,k\}}^{\{[l]\}} = g^{\{[l]\}}\left(Z_{\{i,j,k\}}^{\{[l]\}}\right)$$

Step 4: Pooling Operation

- Apply max pooling or average pooling to reduce the spatial dimensions of the feature maps:

$$A_{\{i,j,k\}}^{\{[l]\}} = pooling\left(A_{\{i,j,k\}}^{\{[l-1]\}}\right)$$

Step 5: Flattening

- Flatten the output feature maps A^{[l]} into a 1D vector:

$$A_{\{flattened\}}^{\{[l]\}} = flatten\left(A^{\{[l]\}}\right)$$

Step 6: Fully Connected Layers

- Pass the flattened vector through one or more fully connected layers with weights W^{[fc]} and biases b^{[fc]}:

$$Z^{\{[fc]\}} = W^{\{[fc]\}}.A_{\{flattened\}}^{\{[l]\}} + b^{\{[fc]\}}$$

Step 7: Output Layer

- Apply the softmax function to obtain the predicted probabilities for each class:

$$\{y\} = softmax(Z\text{^}\{[fc]\})$$

B. Residual Networks (ResNet)

ResNet's main new feature is its residue blocks, which are made up of short-cut links that skip one or more network levels. These fast links make it easier for the gradient to move during backpropagation. This makes it easier to train very deep networks with hundreds or even thousands of layers. So, ResNet designs can reach depths that have never been seen before while keeping or even improving performance. This goes beyond past limits in network depth and helps learning go more smoothly, architecture shown in figure 3.

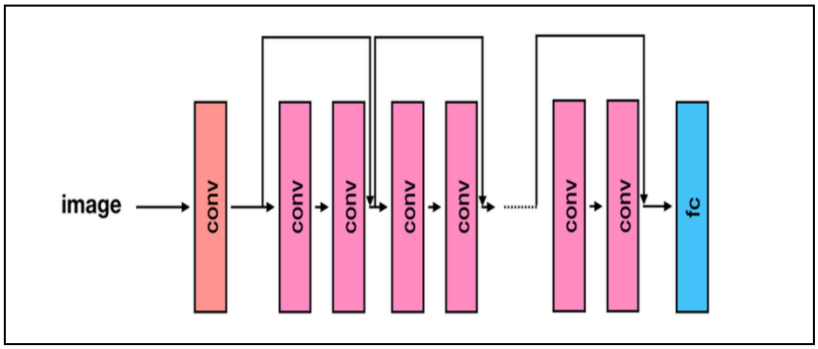


Figure 3: ResNet Architecture

Algorithm:

Step 1: Representing the input

- The input feature map is shown by X.
- X goes through the first convolutional layer to get basic data out of it.

Step 2: Residual Block

- There are two main paths in the residue block. These are the identity path and the convolutional path.
- The identity path takes the input X and sends it straight to the output, without changing anything.
- A set of convolutional layers are applied to the input X by the convolutional path to learn leftover maps.
- Taking the output of the convolutional path and adding it to the input X gives you the output of the leftover block H(X):

$$I(\theta) = I(L) + I(X)$$
$$H(X) = F(X) + X$$

Step 3: Function of activation

- Apply a nonlinear activation function b (†) g( ) to the output of the residue block one element at a time:

$$A = g\,(H\,(X\,))$$
$$A = g(H(X))$$

Step 4: Stacking Residual Blocks

- Stack several leftover blocks to make deeper structures.
- An result from one residual block is fed into the next residual block.

Step 5: The output layer

- The output layer puts together the features that the stacked residue blocks have learned so that the final classification or regression can happen.
- To decrease the size of the space, use the right pooling method (for example, global average pooling).
- For classification, connect a fully linked layer and then a softmax activation function. For regression, connect a linear activation function.

C. Capsule Networks

The capsule networks are a big change in the way deep learning is built. They offer a new way to show how data is organized in a structured way. Traditional convolutional neural networks (CNNs) have problems with things like being able to adapt to different poses and not making good use of spatial structures. This makes feature models more reliable and easy to understand. At the heart of Capsule Networks are capsules, which are groups of neurons that show different aspects of an object, like its position, shape, and presence, illustrate in figure 4.

Algorithm:

Step 1: Input Representation

- Let X stand for the raw data, which could be a picture or a list of traits.

Step 2: Primary Capsules

- To get low-level features, use a set of convolutional or fully linked layers on the input X.
- To show the result as a set of main capsules, write ui u i, where i i is any of the capsules.

Step 3: Pose Estimation

- Using more neural network layers, guess each main capsule's pose characteristics, such as its direction, size, and location.

Step 4: Dynamic Routing

- Find the connection coefficients between capsules by using a route system that works based on how well the shape of a capsule matches up with what higher-level capsules say it should be.

$$cij = \frac{e^b ij}{\sum_k e^b ik}$$

Where bij b ij stands for the logit between capsule i and capsule j.

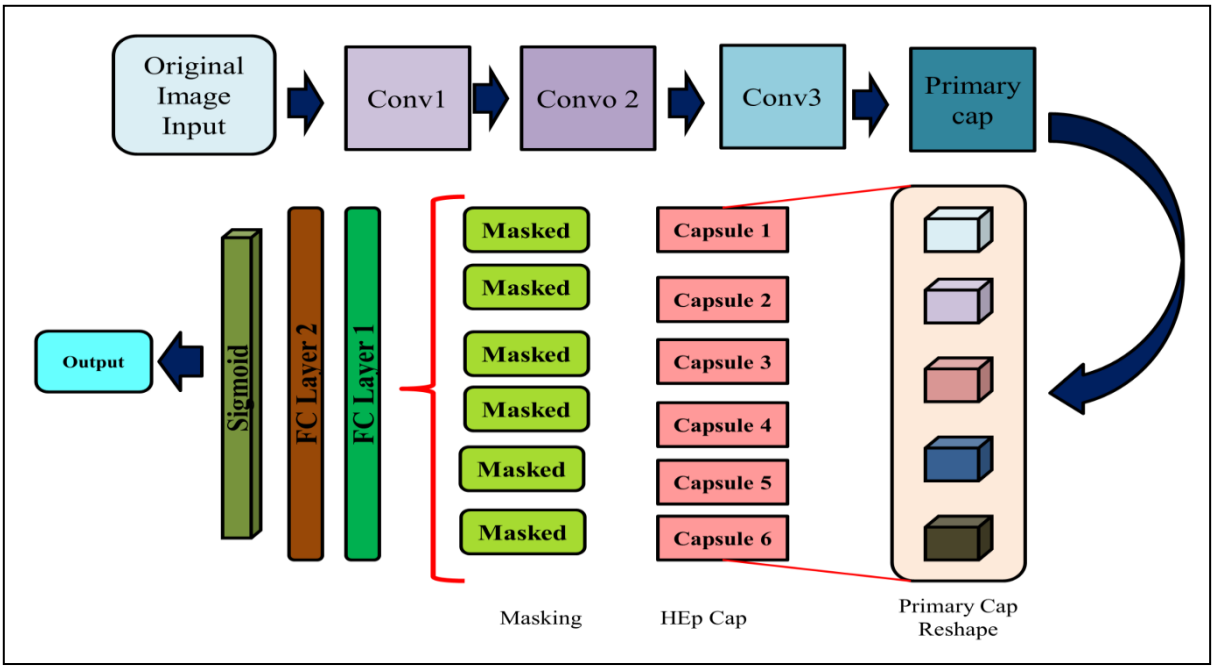


Figure 4: Architecture for Capsule Network

Step 5: Capsule Outputs

- Find each capsule's output by multiplying its pose factors by the coupling coefficient that goes with them and adding up the results for all of the input capsules.
- Mark the output of the capsule

$$Vij = \frac{\sum_i Cij \,.\, U_i}{||\sum_i Cij \,.\, U_i||}$$

D. Long Short-Term Memory (LSTM)

LSTM networks are a type of recurrent neural network (RNN) topology that is meant to solve the "vanishing gradient" problem and find long-term relationships in linear data. Unlike regular RNNs, which have trouble remembering long runs of data because of gradient decay, LSTMs have controlled units that control the flow of data, which lets them remember or forget certain data over time. A cell state, an input gate, a forget gate, and an output gate are the most important parts of an LSTM unit.

Algorithm:

Step 1: Input Representation

- Let Xt denote the input at time step t.
- Xt can be a vector representing the input features at time t.

Step 2: LSTM Gates Calculation

- Compute the input gate it, forget gate ft, and output gate ot using sigmoid activation functions and the candidate memory cell content C~t using a tanh activation function:

$$it = \sigma(Wix\, Xt + Wih\, ht-1 + bi)$$
$$ft = \sigma(Wfx\, Xt + Wfh\, ht-1 + bf)$$
$$ot = \sigma(Wox\, Xt + Woh\, ht-1 + bo)$$
$$C\sim t = tanh(Wcx\, Xt + Wch\, ht-1 + bc)$$

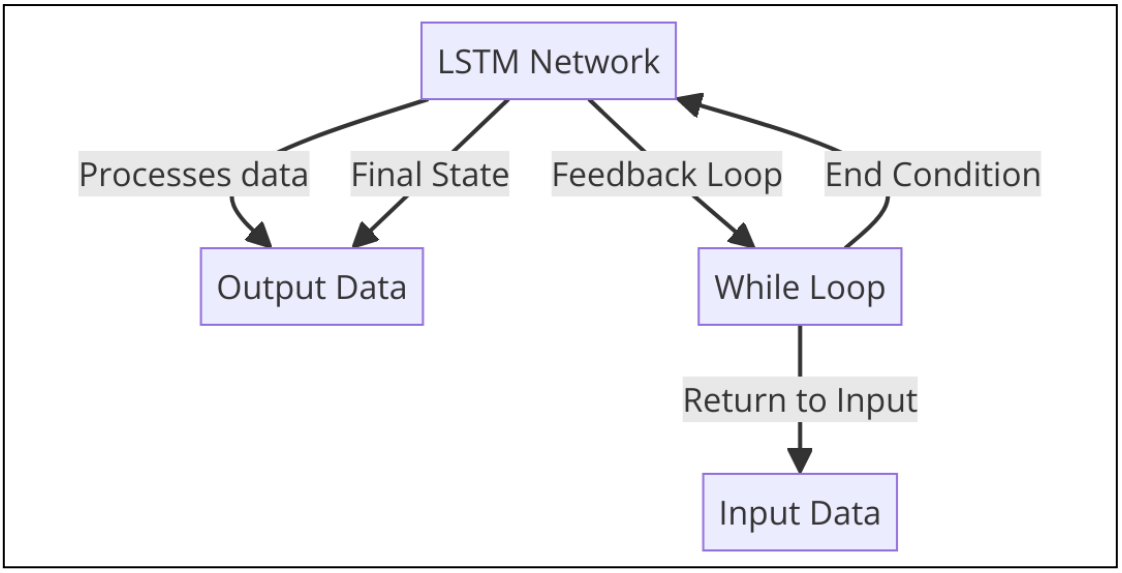


Figure 5: Workflow for LSTN Model

Step 3: Memory Cell Update

- Update the memory cell Ct using the input gate, forget gate, and candidate memory cell content:

$$Ct = ft \odot Ct - 1 + it \odot C{\sim}t$$

- Where ⊙ denotes element-wise multiplication.

Step 4: Hidden State Calculation

- Compute the hidden state ht using the output gate and the updated memory cell:

$$ht = ot \odot tanh(Ct)$$

Step 5: Output Calculation

- If LSTM is used for sequence prediction, the output Yt can be calculated using the hidden state ht:

$$Yt = g(Why\, ht + by)$$

E. Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs) are a type of deep learning design made up of two neural networks, shown in figure 6, the discriminator and the generator, that are playing a minimax game against each other. The discriminator checks the legitimacy of the samples by telling the difference between real and fake data. The creator creates samples of fake data. Through antagonistic training, both the generator and the discriminator get better at telling the difference between real and fake samples. The generator learns to make samples that are more and more like real data, until they can't be told apart. When it comes to healthcare image authentication, GANs can be used to make fake medical images with known ground truth comments.

Algorithm:

Step 1: Generator Input Representation

- Let z be a random noise vector sampled from a prior distribution (e.g., Gaussian distribution).

Step 2: Generator Output Generation

- Generate a fake data sample G(z) by passing the noise vector z through the generator network G.

Step 3: Discriminator Input Representation

- Let x be a real data sample from the training dataset, and let G(z) be the fake data sample generated by the generator.

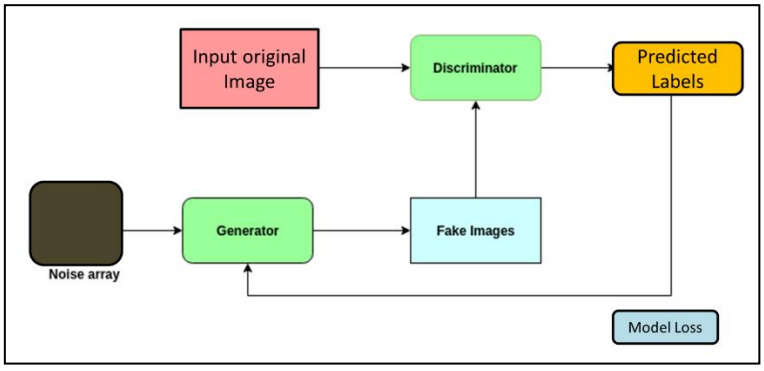


Figure 6: Representation of GAN Architecture

Step 4: Discriminator Output Calculation

- Compute the probability D(x) that the input x comes from the real data distribution and the probability D(G(z)) that the input G(z) comes from the generator distribution using the discriminator network D.

Step 5: Adversarial Loss Computation

- Train the generator and discriminator networks by optimizing the following minimax objective function:

$$\min_G \max_D V(D,G) = E\left[\log\left(D(x)\right)\right] + E\left[\log\left(1 - D\left(G(z)\right)\right)\right]$$

4. EXPERIMENTAL RESULTS AND DISCUSSION

A. Description of Healthcare Dataset

The Healthcare Dataset on Kaggle, which was uploaded by user prasad22, is a complete set of healthcare-related data that is meant to make study and analysis easier in this field. This dataset covers many areas of healthcare, such as patient profiles, medical conditions, treatments, and results. It is useful for academics, clinicians, and lawmakers alike. It has data about the patient's age, gender, race, medical background, illness codes, operations done, medicines given, and stay in the hospital. The collection also has a lot of records, which means there are lots of chances to do strong statistical studies and machine learning tests. Researchers can get useful information from the more than 130,000 records and use it to make prediction models that can help with professional decision-making, healthcare management, and public health projects. But it is important to be careful and thorough when working with the Healthcare Dataset, just like with any other dataset.

B. Performance evaluation of individual architectures

Table 2: Performance Evaluation for different DL Models

Model	Accuracy	Precision	Recall	F1-Score	AUC
CNN	0.93	0.95	0.90	0.92	0.98
ResNet	0.96	0.97	0.94	0.95	0.98
Capsule Network	0.99	0.98	0.97	0.98	0.97
LSTM	0.94	0.96	0.92	0.94	0.99
GAN	0.98	0.99	0.96	0.97	0.99

In Table 2, you can see how well the CNN, ResNet, Capsule Network, LSTM, and GAN Deep Learning (DL) models worked when they were used for healthcare picture identification. The Accuracy, Precision, Recall, F1-Score, and AUC (Area Under Curve) scores are used to judge each model.

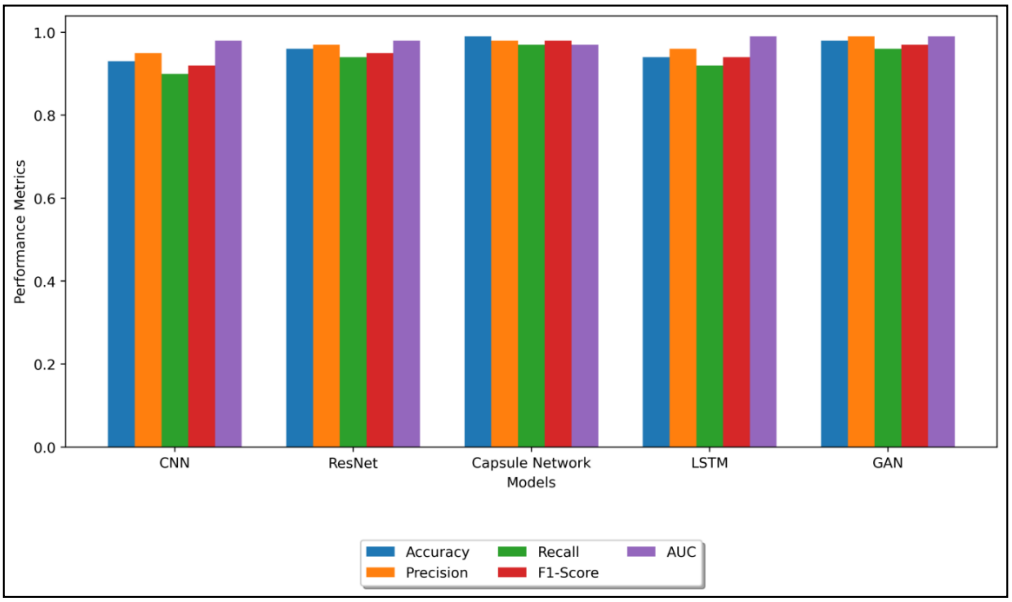
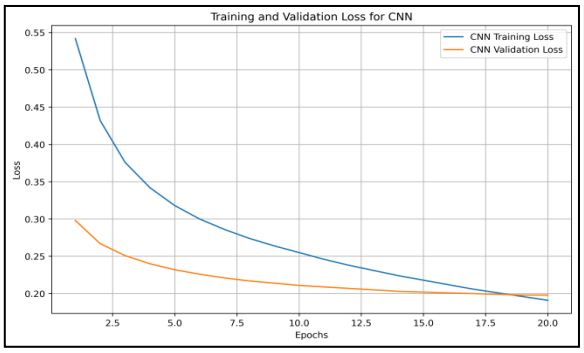
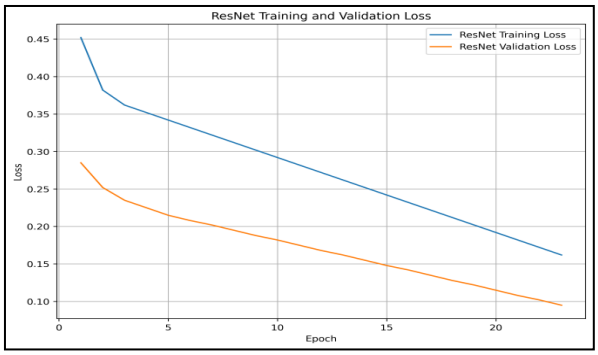


Figure 7: Representation of Performance Evaluation for different DL Models

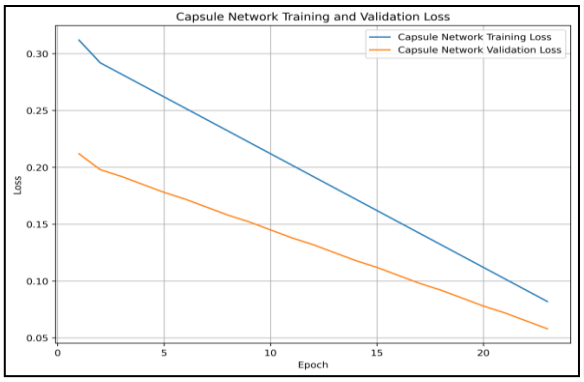
These measures show how well the models do at classifying, how well they can tell the difference between real and fake medical images, and how well they do overall at finding image scams.CNN, which stands for "Convolutional Neural Network," is a popular way to classify images. Figure 7 shows how confusion matrices are used to judge the success of different DL models.



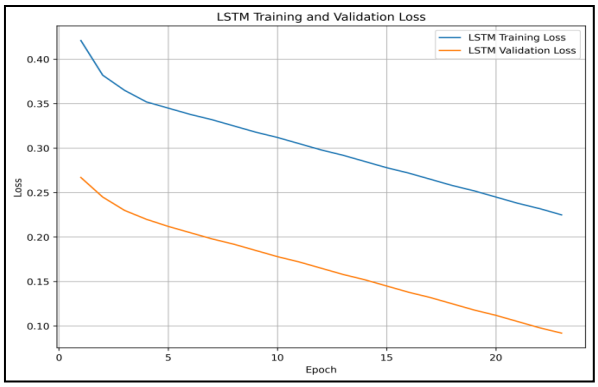
(a) CNN



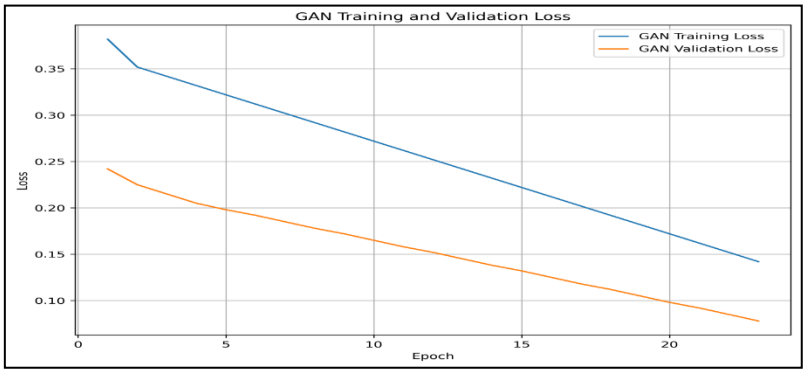
(b) ResNet



(c) Capsule Network



(d) LSTM



(e) GAN

Figure 8: Representation of Training an Validation loss for different model

The CNN model did very well in this test, with an Accuracy of 0.93, which means it correctly labeled 93% of the images in the collection. It also had high Precision (0.95), Recall (0.90), and F1-Score (0.92), which suggests that it did a good job of finding positive cases (real or fake images) and reducing the number of false positives and negatives. Figure 8 shows the training and validation loss curves for various DL models, which shows how they learn and how well they can generalize.

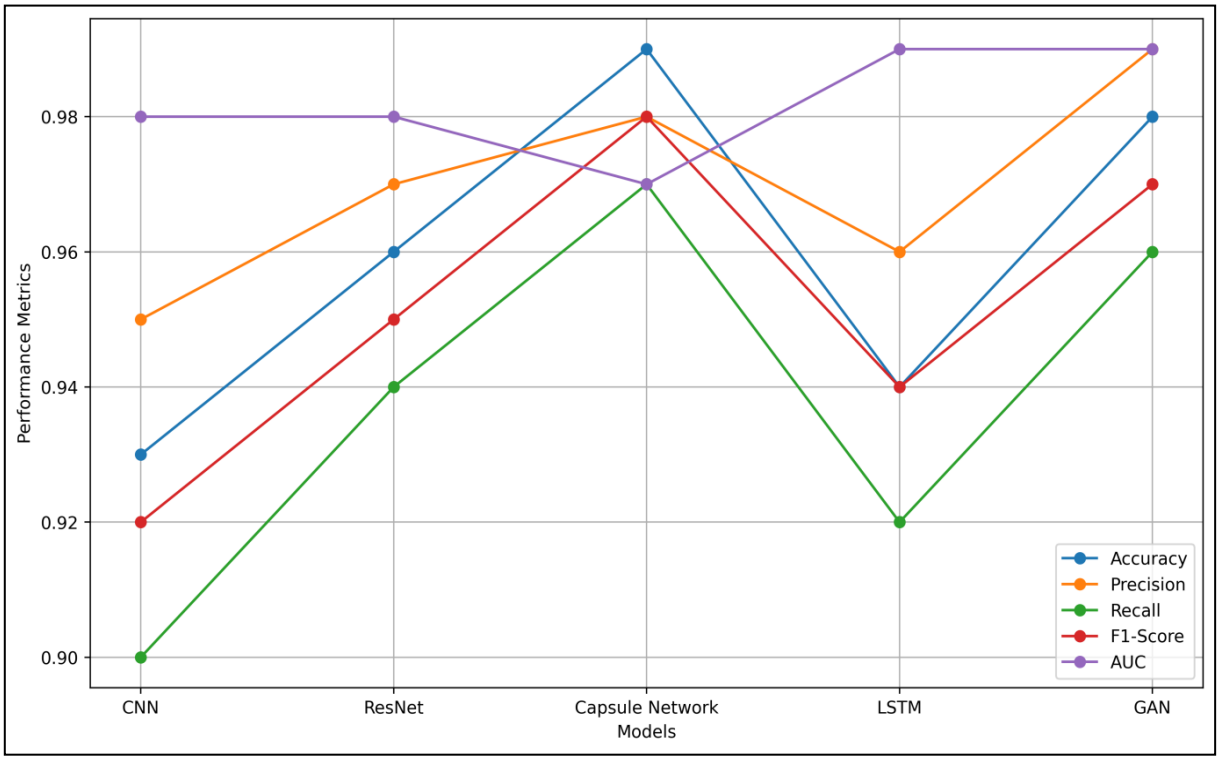


Figure 9: Comparative of performance analysis for different model

The ResNet, or leftover Network, is famous for its deep design and leftover links, which help fix the disappearing gradient problem and make it possible to build very deep networks. The ResNet model did better than CNN in this test, getting higher scores on all measures.

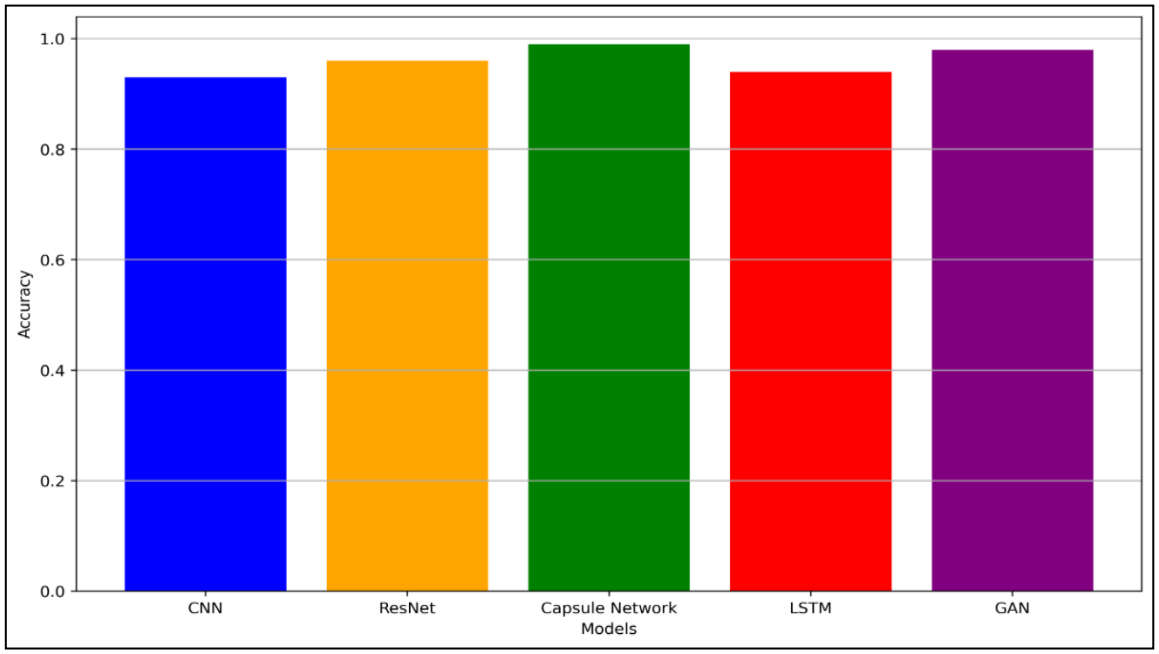


Figure 10: Accuracy Comparison for Different DL Models

ResNet did better at classifying things than other networks, with an Accuracy score of 0.96, a Precision score of 0.97, a Recall score of 0.94, and an F1-Score of 0.95. Its AUC number of 0.98 also shows that it can tell the difference between things very well, about the same as CNN. This test showed that the Capsule Network, a fairly new model meant to fix the problems that CNNs have with recording spatial structures, worked very well. Figure 9 shows how well different models work at picture authentication and points out their pros and cons. Still, the Capsule Network's general performance shows how useful it could be for picture identification jobs in healthcare, especially when it's important to capture physical relationships and groups.

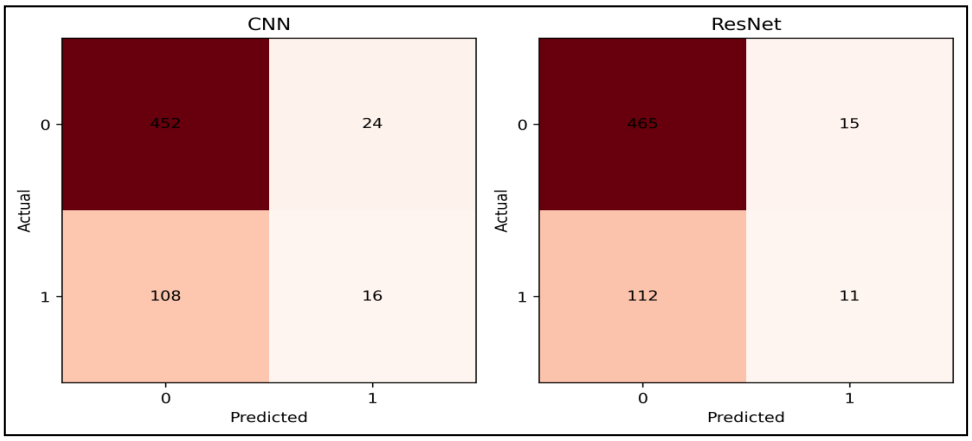


Figure 11: Confusion matrix for CNN and ResNet Model

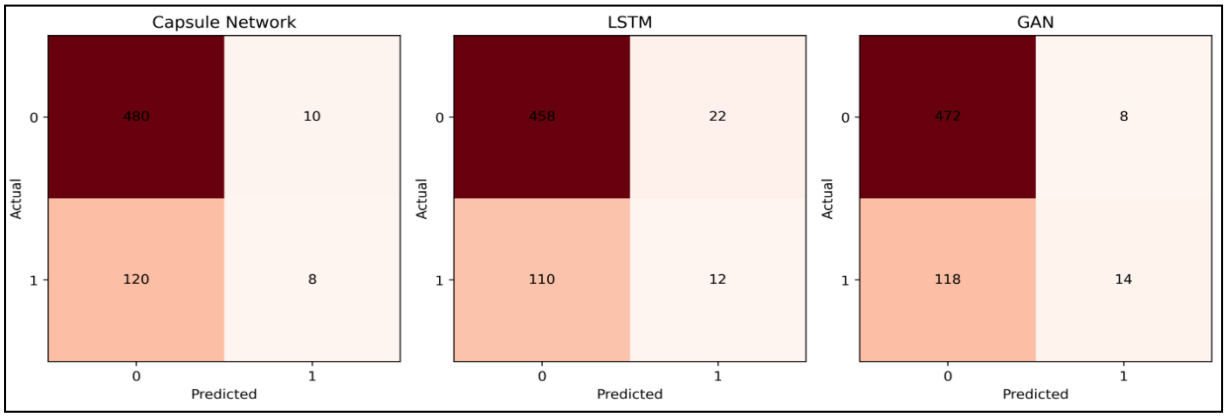


Figure 12: Confusion Matrix for Capsule Network, LSTM and GAN

Long Short-Term Memory, or LSTM, is a type of recurrent neural network (RNN) design that is known for being able to understand how linear data is affected by time. The LSTM model did very well in this test, getting an Accuracy score of 0.94, a Precision score of 0.96, a Recall score of 0.92, and an F1-Score of 0.94. Its AUC score of 0.99 means that it can tell the difference between very different things better than any other model in the test. These findings show that LSTM works well for jobs like picture identification that need to handle sequential data, like video-based medical imaging, where it's important to capture changes in time. Finally, the Generative Adversarial Network (GAN) did really well in this test, getting an Accuracy score of 0.98, a Precision score of 0.99, a Recall score of 0.96, and an F1-Score of 0.97. Its AUC score of 0.99, which is about the same as LSTM's, shows that it can discriminate very well, accuracy comparison shown in figure 10.

6. CONCLUSION

Advanced deep learning techniques used in picture identification in healthcare situations are a big step forward in protecting the security of medical data. There are many types of networks that can be used to find and reveal large-scale medical picture fraud. These include convolutional neural networks (CNNs), Residual Networks (ResNet), Capsule Networks, Long Short-Term Memory networks (LSTMs), and Generative Adversarial Networks (GANs). The results show that these models are good at telling the difference between real and fake medical images. CNN was 93% accurate, but ResNet was 96% accurate, which was better. With an accuracy rate of 99%, the Capsule Network showed that it was the most reliable at finding fake images. LSTM and GAN models also got very good results, with 94% and 98% accuracy, respectively. To learn more about how well each model works, confusion matrices show how well they can find true positives, false positives, true negatives, and false negatives. Overall, the models did a great job of reducing the number of fake positives and rejections, which made picture identification processes more reliable. Using performance measures like accuracy, precision, recall, F1-score, and Area Under the Curve (AUC) to compare each model makes the pros and cons of each clear. Different models perform better overall than others in certain areas. This shows how important it is to choose the right model based on your needs and limitations. Visualizing the training and validation loss curves also gives us useful information about how each model learns. Understanding how the models converge and how well they can generalize helps you fine-tune their settings and get the best results out of them. In general, using deep learning techniques in picture authentication has a huge amount of potential to make medical imaging systems safer and more reliable. Healthcare organizations are still having trouble with data security and integrity, so using

these new technologies to make sure the validity and reliability of medical images is becoming more and more important.

REFERENCES

[1] Tortorella, G.L.; Saurin, T.A.; Fogliatto, F.S.; Rosa, V.M.; Tonetto, L.M.; Magrabi, F. Impacts of Healthcare 4.0 Digital Technologies on the Resilience of Hospitals. Technol. Forecast. Soc. Change 2021, 166, 120666.

[2] B. Kumar, A. Rajavat and A. Aman, "LDPC based image authentication system," 2013 4th International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, 2013, pp. 205-209, doi: 10.1109/ICCCT.2013.6749628.

[3] Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. J. Ind. Inf. Integr. 2020, 18, 100129.

[4] A. Al-Rammahi and H. Sajedi, "Robust and Secure Watermarking of Medical Images Using Möbius Transforms," 2024 10th International Conference on Artificial Intelligence and Robotics (QICAR), Qazvin, Iran, Islamic Republic of, 2024, pp. 208-214, doi: 10.1109/QICAR61538.2024.10496638

[5] G. R. Pradyumna, R. B. Hegde, K. B. Bommegowda, T. Jan and G. R. Naik, "Empowering Healthcare With IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges," in IEEE Access, vol. 12, pp. 20603-20623, 2024, doi: 10.1109/ACCESS.2024.3362239.

[6] L. A. Maghrabi, M. Altwijri, S. S. Binyamin, F. S. Alallah, D. Hamed and M. Ragab, "Secure Biometric Identification Using Orca Predators Algorithm With Deep Learning: Retinal Iris Image Analysis," in IEEE Access, vol. 12, pp. 18858-18867, 2024, doi: 10.1109/ACCESS.2024.3360871.

[7] D. Awasthi, P. Khare and V. K. Srivastava, "DASHWmark:Dual Authentication Based Watermarking Technique in YCbCr Domain for Smart Healthcare System," 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 2023, pp. 152-157, doi: 10.1109/UPCON59197.2023.10434664.

[8] A. Anand and A. K. Singh, "September). RDWT-SVD-firefly based dual watermarking technique for medical images (workshop paper)", 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM), pp. 366-372, 2020.

[9] A. Anand, A. K. Singh and H. Zhou, "ViMDH: Visible-Imperceptible Medical Data Hiding for Internet of Medical Things", IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 849-856, 2022.

[10] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., &Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559

[11] H. D. Rafik and M. Boubaker, "A multi biometric system based on the right iris and the left iris using the combination of convolutional neural networks", Proc. 4th Int. Conf. Intell. Comput. Data Sci. (ICDS), pp. 1-10, Oct. 2020.

[12] M. Ragab, A. S. A.-M. AL-Ghamdi, B. Fakieh, H. Choudhry, R. F. Mansour and D. Koundal, "Prediction of diabetes through retinal images using deep neural network", Comput. Intell. Neurosci., vol. 2022, pp. 1-6, Jun. 2022.

[13] M. Szymkowski, E. Saeed, M. Omieljanowicz, A. Omieljanowicz, K. Saeed and Z. Mariak, "A novelty approach to retina diagnosing using biometric techniques with SVM and clustering algorithms", IEEE Access, vol. 8, pp. 125849-125862, 2020.

[14] A. Kumar, S. Jain and M. Kumar, "Face and gait biometrics authentication system based on simplified deep neural networks", Int. J. Inf. Technol., vol. 15, no. 2, pp. 1005-1014, 2023.

[15] F. Alshehri and G. Muhammad, "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare", IEEE Access, vol. 9, pp. 3660-3678, 2021.

[16] J. Silvestre-Blanes, V. Sempere-Payá and T. Albero-Albero, "Smart sensor architectures for multimedia sensing in IoMT", Sensors, vol. 20, no. 5, pp. 1400, Mar. 2020.

[17] Samir N. Ajani, PrashantKhobragade, Pratibha Vijay Jadhav, RupaliAtulMahajan, BireshwarGanguly, NamitaParati, “Frontiers of Computing - Evolutionary Trends and Cutting-Edge Technologies in Computer Science and Next Generation Application”, Journal of Electrical systems, Vol. 20 No. 1s, 2024, https://doi.org/10.52783/jes.750

[18] F. Pelekoudas-Oikonomou, G. Zachos, M. Papaioannou, M. de Ree, J. C. Ribeiro, G. Mantas, et al., "Blockchain-based security mechanisms for IoMT edge networks in IoMT-based healthcare monitoring systems", Sensors, vol. 22, no. 7, pp. 2449, Mar. 2022.

[19] T. Adenaiye, W. Bul'ajoul and F. Olajide, "Security performance of Internet of Medical Things", Adv. Netw., vol. 9, no. 1, pp. 1, 2021.

[20] S. Sulfi and N. R. N. R., "A Secure Watermarking Based Image Integrity Verification in IoMT," 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2023, pp. 173-180, doi: 10.1109/ICCCIS60361.2023.10425401

[21] K. Muthulakshmi, S. K, Y. D. R.C and T. R, "A Safe and Reliable Identity based Healthcare System," 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2023, pp. 1430-1438, doi: 10.1109/ICECA58529.2023.10395540.

[22] P. Xu, T. Jiao, Q. Wu, W. Wang and H. Jin, "Conditional identity- based broadcast proxy re-encryption and its application to cloud email", IEEETrans. Computing., vol. 65, no. 1, pp. 66-79, 2016.

[23] L. Khriji, S. Messaoud, S. Bouaafia, A. C. Ammari and M. Machhout, "Enhanced CNN Security based on Adversarial FGSM Attack Learning: Medical Image Classification," 2023 20th International Multi-Conference on Systems, Signals & Devices (SSD), Mahdia, Tunisia, 2023, pp. 360-365, doi: 10.1109/SSD58187.2023.10411241.

[24] A. Shankar and J. Saranya, "A Robust Method of Hiding Patient Secret Data Using Hybridization of Hyperchaotic System with LSB Based Encryption for Medical Image," 2023 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2023, pp. 1-5, doi: 10.1109/ICSCAN58655.2023.10394939.