Vol 8, Issue 3, 2025 **Impact Factor: 8.535** DOI: https://doi.org/10.31426/ijamsr.2025.8.3.8133

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Implementing RSA-DWT Hybrid Approach for Confidential and Covert Protection of Medical Data

Kunkumalla Premchander [1]

[1] Research Scholar, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

Dr. G. Soma Sekhar [2]

[2] Supervisor, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

With the increasing digitization of healthcare records, ensuring the confidentiality and integrity of sensitive patient information has become a critical concern. This paper proposes a hybrid two-level security approach for Electronic Health Record (EHR) systems, combining RSA cryptography and Discrete Wavelet Transform (DWT) based steganography. In this approach, sensitive medical data is first encrypted using the Rivest-Shamir-Adleman (RSA) algorithm to ensure strong cryptographic protection. The encrypted data is then covertly embedded into medical images using DWT steganography, preserving visual quality and diagnostic integrity. The performance of the proposed method is evaluated using standard metrics such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Normalized Cross-Correlation (NCC). The study concludes that the RSA-DWT hybrid model provides a robust and reliable solution for secure storage and transmission of medical data, enhancing patient privacy while maintaining compliance with data protection regulations.

Keywords: *Security, Steganography, Encryption, Privacy, Watermarking.*

I. INTRODUCTION

There has been a dramatic increase in the generation and sharing of personally identifiable information (PII) inside healthcare systems in recent years, making medical data security an urgent issue. To avoid identity theft, unauthorised access, and other harmful assaults, it is crucial to safeguard sensitive medical data like patient records, diagnostic imaging, and treatment histories. The need for strong security measures has been further magnified by the proliferation of telemedicine, EHR, and the transfer of medical data via digital platforms. Encryption and steganography, two forms of sophisticated data concealment, have arisen as critical resources for

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

protecting sensitive medical information in light of these growing worries. Nevertheless, it is sometimes the case that a single layer of protection is insufficient to provide complete security. To guarantee the privacy, validity, and integrity of medical records, this study suggests a two-tiered security system that integrates steganography with encryption.

It is now common practice in many industries, including healthcare, to encrypt sensitive data. Encrypting medical data into an unreadable format that can only be deciphered with the right key is a crucial feature of cryptographic techniques, especially public-key encryption systems. The Rivest-Shamir-Adleman (RSA) algorithm is a popular encryption method that offers robust security using asymmetric key pairs. Because of the high-speed nature of medical settings, where safe communications and rapid data access are of the utmost importance, RSA is well-suited to the context of medical data because to its combination of computing efficiency and security. When dealing with sensitive medical information across multiple platforms, RSA ensures the safe transmission of encryption keys between parties. Nevertheless, it is necessary to provide an extra layer of security since even if encryption makes data unreadable by unauthorized users, it still leaves traces of the encrypted communication that might be intercepted.

Now we may talk about steganography, a method that conceals critical information by making it seem to be less important. Steganography is a great addition to encryption for protecting medical data because, unlike encryption, it hides the existence of the data rather than just its content. Steganography makes sure that no one can even tell that sensitive medical information is concealed by encrypting it and then hiding it in plain text, audio files, or photos. Discrete Wavelet Transform (DWT) is the main approach that we cover in this study for image-based steganography. In order to include data while preserving the cover image's visual integrity, DWT, a strong mathematical tool, may divide pictures into various frequency components. Among the many benefits of this approach is its resilience in the face of frequent compression and transformations seen in medical picture processing. Our two-tiered security approach combines RSA encryption with DWT-based steganography to hide medical data in a way that unauthorized users can't possibly understand or discover. This ensures both confidentiality and imperceptibility.

The growing volume of sensitive medical data sent across public networks, such as the internet, is a key driver behind this strategy. As an example, EHR systems facilitate the exchange of patient information across many parties, including healthcare providers, insurers, and others. Data transmission security can be enhanced by encryption, but steganography takes it a step further by encasing the data in a cover medium, making it much more resistant to interception and illegal access. Cover and hidden data in steganographic methods are often comprised of medical pictures, including X-rays, MRIs, and CT scans. Since these pictures are already in digital form, they provide a perfect medium for inserting confidential data. By using DWT-based steganography, encrypted medical data may be efficiently embedded into these photos without significantly compromising their visual quality. This guarantees that medical professionals utilizing these images in clinical practice will not encounter any degradation in data integrity.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

The possibility of data alteration or manipulation is another major obstacle to healthcare data security. Unauthorized individuals or entities may try to change medical records in order to conduct fraud or damage them while they are in transit or storage. Addressing this problem, the suggested two-level security technique verifies the integrity of the data included in the cover picture in addition to guaranteeing that the data is encrypted. To add another level of security, we may include a digital signature or hash of the initial data into the steganographic process. Because of this, it is feasible to determine if the concealed medical data has been changed in any manner during transmission or storage.

Improving data integrity and authentication are two further benefits of this dual-layer security method. The term "authentication" guarantees that the data originated from a genuine source, whereas "integrity" guarantees that the data has not been altered while being sent. These two aspects are of paramount importance in healthcare settings. A patient's health may be jeopardized, for instance, if tampering with their medical record resulted in erroneous diagnoses and treatments. The suggested approach takes use of both encryption and steganography to safeguard medical records from prying eyes while also making them impossible to alter in any way. By combining DWT steganography with RSA encryption, data is concealed and secured, making assaults like man-in-the-middle and replay attacks less likely to succeed.

Another crucial aspect of the two-level security system's practical implementation in healthcare settings is its efficiency. When access to medical records is critical in real time, such during operations or emergencies, RSA encryption guarantees that the data can be encrypted and decrypted relatively fast. Medical professionals may continue to utilize these photographs without any visible reduction in quality since DWT for steganography assures that the visual quality of medical images stays excellent while embedding the encrypted data. In addition, the strategy is compatible with current healthcare systems, providing a workable option that doesn't need major overhauls to processes or infrastructure.

RSA and DWT

An investigation on the potential of a hybrid cryptographic approach to enhance data security was undertaken in response to these worries. This method ensured the safe storage and transmission of critical health information in the cloud by combining the strengths of Discrete Wavelet Transform (DWT) and Rivest-Shamir-Adleman (RSA) encryption.

The tried-and-true asymmetric encryption method RSA was used to safeguard data while it was being sent. With RSA's use of public and private keys, encrypted patient records could only be accessed by authorized healthcare personnel who had the corresponding private key. This technique made sure that no one could decipher the data even if it was intercepted while in transit.

The research included both RSA and DWT, a signal processing method for data compression and embedding. Medical pictures including X-rays, MRIs, and CT scans were subjected to DWT, which concealed encrypted data inside the image's wavelet coefficients. That made it hard for would-be hackers, even if they cracked the cloud storage code, to tell whether the photos included any

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

important information. DWT helped decrease data size, which improved storage efficiency in the cloud, and it also introduced an extra degree of protection.

A complete answer was provided by the hybrid cryptographic strategy that included RSA and DWT; this approach guaranteed the security and integrity of patient data. It made guaranteed that patients' personal information would be protected in the ever-changing digital healthcare system, regardless of whether the records were text-based or image-based.

II. REVIEW OF LITERATURE

Jayakumar, Sujayaraj & Meher, Kunal et al., (2024) Healthcare delivery has been transformed by the fast growth of digital health technologies, which have simplified procedures and increased accessibility for both patients and medical practitioners. Nevertheless, digitizing health information poses a significant threat to individuals' privacy and data security. Data breaches in electronic health records pose several concerns, and this article provides a thorough summary of them. In a larger perspective, the possible privacy dangers associated with healthcare systems are shown by these hacks. Patient data is stored and distributed across several platforms due to the expansion of electronic health records (EHRs), cloud computing, and telemedicine. Here we'll take a look at a few of the most typical dangers that individuals confront as a result of a breach of their private health information. Everything from insiders to hackers to hospital IT systems is included in this. We also go over the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA), two of the laws and ethical standards that aim to safeguard patients' private information. Securely storing, exchanging, and accessing health data remains a challenge, despite continuous advances in the field. Several approaches for securing patient data are explored in this paper, including encryption and multi-factor authentication. Having a thorough data security strategy is crucial for healthcare organizations to gain patients' confidence and stay in compliance with policies. As digital health technologies evolve, it is crucial to maintain data privacy standards current to safeguard patient privacy and ensure the seamless operation of healthcare systems.

Zeenath, & Durga Devi, K et al., (2024) the creation of strong security measures is crucial in today's digital healthcare scene because protecting the privacy and authenticity of medical pictures has become a top priority. In light of these issues, the current study proposes a novel picture encryption system developed with the express purpose of strengthening the security of medical images. The suggested method strengthens the security of medical picture data by including a unique key management system with an advanced combination of symmetric and asymmetric encryption algorithms, which prevents illegal access and harmful manipulation. For an extra degree of security, the suggested DNA-based encryption technique uses the special characteristics of DNA encoding to safely encrypt picture data. The system accomplishes a high degree of data confusion and dispersion by exploiting DNA sequences in the encryption and decryption operations, considerably boosting security. Experimental tests show that the suggested encryption system is effective in protecting data while keeping computation efficient, hence validating its effectiveness. Additionally, we check that the scheme works with current medical imaging equipment, so you know it will fit right in with modern healthcare systems. By suggesting an effective encryption strategy that finds a happy

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

medium between rigorous security needs and realistic implementation concerns, our study helps move medical picture security forward. Two major advancements that greatly improve the safety of medical photographs are a new key management system and an encryption technique based on DNA. By suggesting an effective encryption strategy that finds a happy medium between rigorous security needs and realistic implementation concerns, our study helps move medical picture security forward. The proposed program enables healthcare professionals to maintain patient privacy and confidence in the digital era by protecting the confidentiality and integrity of medical pictures. This method is well-suited for sensitive medical imaging applications, since experimental findings demonstrate that it guarantees strong encryption without affecting picture quality.

Motomura, Ryota & Imaizumi, Shoko et al., (2022) this research introduces a novel method for reversible data-hiding in encrypted images that can achieve high compression efficiency without sacrificing hiding capacity. Not only can the proposed method decode marked encrypted photographs, but it also allows for the elaboration of marked encrypted images with a payload—all without the necessity for data extraction. As part of an architecture that encrypts and then compresses, a perceptual encryption approach is used to generate compressible encrypted images. For data concealment, we additionally use a very accurate predictor, an enlarged prediction error, and a shifting of the histogram. This method achieves a high concealment rate while compressing tagged encrypted photographs without loss since it follows to image coding standards. The results show that the approach produces good marked-image quality, efficient lossless compression, and hiding capacity.

Mansour, Romany & Parah, Shabir (2021) When it comes to healthcare service delivery, the integration of cloud computing and the Internet of Things is proving to be an indispensable tool. Ensuring the security, confidentiality, and availability of electronic health records poses a significant challenge to the widespread use of telemedicine. It is of the utmost significance to share EHI with a remote doctor via the cloud in order to prevent misdiagnoses that may be caused by even minor variations. There has been a lot of research on this topic, but it is still critical to create algorithms to strengthen the security of e-healthcare systems. An innovative Reversible Data Hiding (RDH) method for EHI security is suggested in this paper, which makes use of Lagrange's interpolation polynomial, secret sharing, and bit replacement. Using the subsampled cover medical image, four shares are generated. We use picture interpolation to enlarge the subsamples in order to hide EHI. Using Lagrange's interpolation polynomial, the secret information is processed before being included in the various cover photo sharing. The data is inserted into the sub-sampled interpolated shares at the points where the algorithm has already made a decision. The distributive nature of embedded data allows it to enhance the security of the proposed framework without compromising its reversibility. We show that 75% of the shares are sufficient to retrieve the whole embedded data set as well as the original cover image. The proposed method outperforms the other approaches in terms of both payload and undetectability. It can reversibly embed 163,840 bits, or 0.75 bits per pixel, and has an average PSNR of around 52.38 dB. Standard deviation, relative entropy difference, cross-correlation, and relative entropy average for the first subsample are 7.3242, 0.0382, 65.0539, and 0.9838, respectively. It outperforms the state-of-the-art by 3 dB with a 1,30,000-bit payload. The decreased

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

processing complexity of the proposed method makes it useful for e-healthcare applications as well. This approach is great for EHI security in distributed systems like the cloud because of its low computational cost and other great features.

Fang, Liming et al., (2020) Cloud computing and other smart networks are changing the way healthcare is provided. However, there are persistent challenges, such as ensuring the secure transmission of sensitive medical data and storing sensitive data in infrastructure that is neither trusted nor regulated. The rapidly expanding use of watermarking technology offers opportunities for smart healthcare. For the purpose of managing data access and sharing, this article details our intentions for a new system. To facilitate the selective transfer of electronic medical records across healthcare facilities, doctors submit their applications to the hospital's medical data center, which processes and stores them on semi-trusted servers. We ensure that privacy problems are addressed while processing requests to view patients' medical records using our technique. Digital watermarks associated with individuals' identities must be included by both patients and doctors when they submit data. As a result, accountability is guaranteed in the case of data theft or alteration.

Prabha, K. & Jagadeeswari, M (2020) In order to make data extraction possible, this paper presents a novel technique for reversible data hiding within compressed images. The technique uses Vector Quantization (VQ) and Side Match Vector Quantization (SMVQ) to hide big secret bits, and subsequently the cover picture is restored. Accurate cover image recovery and optimum embedding capacity are achieved in this study using the Enhanced Imperialist Competitive Algorithm (EICA). The threshold value illustrates the embedding rate of each area in a cover image in relation to the hidden message size; it is determined by the fitness function contrast sensitivity in EICA. Data hiding keeps the output size of the code stream constant by merging two hidden bits into a single index value. Prior to quantization, the Discrete Cosine Transform (DCT) and the Burrows Wheeler Transform (BWT) are used to achieve a high compression ratio and accurate cover image recovery. Energy compression is much improved by DCT, in contrast to BWT, which rearranges symbols depending on their context. Thus, the proposed method delivers a novel approach to embedding concealed information into the cover picture while simultaneously reducing the size of the embedded image. Ultimately, the code streams will keep their original sizes. A high compression rate and embedding capacity are achieved by the proposed approach, according to the experimental results.

III. PROPOSED METHODOLOGY

Using a publicly accessible medical dataset for both covert and overt data is a part of this work's methodology. For speedier encryption and decryption and stronger safe key exchange, the Rivest-Shamir-Adleman (RSA) Algorithm was utilized to encode and decode the secret data, while the Discrete Wave Transform (DWT) was used to conceal the hidden message.

Encryption and Decryption

The medical photos and data were encrypted and decrypted using Rivest-Shamir-Adleman (RSA) to make their communications more secure. Generation of keys, encryption, and decryption were the three steps in the RSA process.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

- **Key Generation**

To begin creating a key, a public key and a private key were initially constructed using the prime numbers. An algorithm for creating RSA keys is shown here:

1. Enter the two produced prime numbers, p and q.
2. Determine whether $n = k \prod q$ (assuming k is not equal to c, as in that case $n = p^2$). In order to get p, one must take the square root of r.
3. The count φ(n) is equal to $(k - 1)(c - 1)$.
4. Pick an integer e such that it is coprime to φ(n) and the range of e is less than or equal to $\varphi(n)$.
5. Construct a secret key d in such a way that $d \prod e = 1(uod\ \varphi(n))$.

In the end, the public key is (e, n) and the private key is d, according to the RSA key generation procedure.

- **Encryption**

The exponential function in modular n is used by the RSA encryption technique, as seen in the Equation. It is possible to determine the cipher text C from a numeric plaintext P by doing the following:

$C = P^e\ mod\ n$

- **Decryption**

Like RSA encryption, the RSA decryption technique may be thought of as an inverse. Employing the private key in the same way as the encryption method, the RSA decryption algorithm is also a modular exponential function n. Discovering the plaintext is as easy as using the private key (n, d):

$P = C^d\ mod\ n$

Embedding and Extraction

Because it decomposes the picture into sub-bands using the Discrete Wave Transform (DWT), the DWT was used to incorporate the secret message because it projects low- and high-frequency features. This makes it possible to find and change the high-frequency coefficients that stand in for the picture's edges and other characteristics. The four wavelet sub-bands LL (approximation coefficients), LH (vertical details), HL (horizontal details), and HH (diagonal details) are generated by applying DWT on the edge-detect cover-image. The cover picture has the message embedded into it via the embedding process. Details of the embedding process as laid forth in Algorithm 1.

Algorithm 1: DWT Embedding Phase Procedure

Step 1: Read the cover-image (C) and cipher secret information (I)

Step 2: Decompose the cover-image (C) into four sub- frames (C_{LL}, C_{LH}, C_{HL}, C_{HH}) respectively using the DWT filter.

Step 3: Perform embedding of cipher secret information (I)

Step 4: Calculate inverse DWT (IDWT)

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

In order to extract data, one must do the inverse of what is done during embedding. The secret information is recovered from the updated DWT coefficients, which are adjusted according to the placements of the encoded information. The extraction process began with DWT decomposing the stego-image (S) into four separate frames. Separate, non-overlapping chunks make up the sub-frames. *S* is used to extract the blocks that are the best matches. Extracted from the detail coefficients blocks are the blocks that represent the differences. A description of the extraction process according to Algorithm 2.

A machine running Windows 11, 64-bit OS, Intel Core i5 CPU with speeds ranging from 2.40GHz to 2.50GHz, 16GB of RAM, and MATLAB R2023a version were used to build the two-layered security solution for medical data.

Algorithm 2: DWT Extraction Phase Procedure

Step 1: Decompose the stego-image(S) into four sub-frames (S_{LL}, S_{LH}, S_{HL}, S_{HH}) respectively using DWT filter

Step 2: Extract the best matched block from sub- frame S_{LL}

Step 3: Perform extraction of cipher secret information (I)

Step 4: Perform IDWT to generate the original C

Step 5: Return I and C

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The samples used in our investigation were from a publicly available internet database (Kaggle.com). The availability of multiple medical imaging modalities was a driving factor in the dataset's selection, making it a significant resource for healthcare research and analysis. As shown in the Table for Cover Image (CI), the experiment made use of two benchmark pictures and six randomly picked gray scale medical photos of 1024 by 1024 dimensions. The following images were used as cover images: CI1—a JPEG of a healthy chest; CI2—a healthy kidney; CI3—a healthy brain infected with a glioma tumor; CI4—a PNG of a healthy chest and joint X-ray with a COVID infection; CI5—a healthy joint X-ray without an infection; CI6—a healthy joint X-ray with an osteoarthritis infection; and the PNG versions of Lena and Peppers benchmark images were all utilized as cover images.

Table 1 shows that the Secret Image (SI) was a jpg file with grayscale medical data. Medical reports may be found in SI4, SI5, and SI6, whereas SI7 shows a lung free of infection and SI1, SI2, and SI3 are prescription photos.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Table 1: Performance Metrics (MSE, PSNR, NCC) for Different Combinations of Cover and Secret Images

Cover Image (CI)	Secret Image (SI)	MSE	PSNR	NCC
CI1	SI1	0.105	43.120	0.902
CI1	SI7	0.142	41.980	0.872
CI2	SI2	0.245	35.500	0.755
CI3	SI6	0.378	33.600	0.770
CI4	SI4	0.160	36.900	0.781

Three commonly used metrics for picture quality and similarity—Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Normalized Cross-Correlation (NCC)—were used to evaluate various combinations of cover images (CI) and secret images (SI) in Table 1. The visual quality and integrity of image embedding or steganography methods may be evaluated using these measures.

With the lowest mean squared error (0.105) and greatest peak signal-to-noise ratio (43.120 dB), the CI1-SI1 combination has the best overall performance, suggesting that there is little distortion between the processed and original pictures. Additionally, the NCC value of 0.902 indicates a high level of embedding accuracy with minimum information loss, indicating a good resemblance between the embedded and original secret picture.

With a PSNR of 41.980 dB and an MSE of 0.142, the CI1-SI7 combination also exhibits high-quality findings. It is still within the realm of high-quality steganographic findings, however it is somewhat worse than CI1-SI1. The NCC of 0.872 provides more evidence of a strong connection between the original and derived hidden picture, further supporting this.

In contrast, the CI2-SI2 and CI3-SI6 combinations produce visibly more visual distortion, with MSE values of 0.245 and 0.378, respectively, and PSNR values of 35.500 and 33.600 dB, respectively. Reduced similarity and lesser embedding accuracy are suggested by the lower matching NCC values (0.755 for CI2-SI2 and 0.770 for CI3-SI6).

With a PSNR of 36.900 dB and an MSE of 0.160, the CI4-SI4 coupling has intermediate performance, positioned between the top and worst performing pairings. Its NCC score of 0.781 lends credence to this level of moderate quality.

According to the findings, CI1 is the best cover picture for maintaining image quality and embedding fidelity, but CI2 and CI3 combinations exhibit more distortion and less similarity. The significance of choosing the right cover-secret picture pairings to guarantee that image embedding methods are efficient and undetectable is highlighted by these results.

V. CONCLUSION

Finally, the research proved that a hybrid cryptographic approach was the best way to protect patient information in e-health cloud storage. An effective security solution was achieved by merging RSA encryption with DWT, which ensured the confidentiality and integrity of critical medical

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

information. By using RSA, we could guarantee the safe transmission of patient data, limiting decryption access to approved receivers. By doing so, we were able to avoid data breaches and illegal access while in transit. However, by including encrypted data into wavelet coefficients, DWT significantly improved the safety of medical pictures like X-rays and MRIs. This made it very hard for attackers, even if they managed to get into the cloud storage, to identify and extract useful information from medical photographs. In order to keep sensitive patient data safe in the ever-changing digital healthcare sector, RSA and DWT worked together as a multi-layered defensive mechanism against cyber attacks. When it came to the increasing difficulty of protecting patient data in healthcare IT systems hosted in the cloud, the research found that hybrid cryptographic methods were the most successful. Patients and healthcare professionals alike benefited from this method's dependable and effective solution, which helped create a more secure setting.

REFERENCES

1. J. He *et al.*, "A novel high-capacity reversible data hiding scheme for encrypted JPEG bit streams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 12, pp. 3501–3515, Dec. 2019.
2. H.-T. Wu, Y.-M. Cheung, Z. Yang, and S. Tang, "A high-capacity reversible data hiding method for homomorphic encrypted images," *J. Vis. Common. Image Represent.* vol. 62, no. 1, pp. 87–96, Jul. 2019.
3. Y. Wu *et al.*, "An improved reversible data hiding in encrypted images using parametric binary tree labelling," *IEEE Trans. Multimedia*, to be published, vol. 3, no. 1, pp. 12–24, Jan. 2019.
4. S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labelling," *IEEE Trans. Multimedia*, vol. 21, no. 1, pp. 51–64, Jan. 2019.
5. K. Chen and C.-C. Chang, "High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement," *J. Vis. Common. Image Represent.* vol. 58, no. 2, pp. 334–344, Jan. 2019.
6. Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Trans. Multimedia*, to be published, vol. 21, no. 1, pp. 51–64 .2019
7. J. Qin and F. Huang, "Reversible data hiding based on multiple two-dimensional histograms modification," *IEEE Signal Process. Lett.* vol. 26, no. 6, pp. 843–847, Jun. 2019.
8. S. Xiang and X. Luo, "Reversible data hiding in homomorphic encrypted domain by mirroring cipher text group," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 11, pp. 3099–3110, Nov. 2018.
9. P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

10. Y. Qiu *et al.*, "Reversible contrast mapping based reversible data hiding in encrypted images," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Hong Kong, vol. 42, no.4, pp. 1–7. Dec. 2018
11. Z. Qian, H. Zhou, X. Zhang, and W. Zhang, "Separable reversible data hiding in encrypted JPEG bit streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1055–1067, Nov. 2018.
12. D. Hou, W. Zhang, Y. Yang, and N. Yu, "Reversible data hiding under inconsistent distortion metrics," *IEEE Trans. Image Process.*, vol. 27, no. 10, pp. 5087–5099, Oct. 2018.
13. D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Process.*, vol. 148, no.2, pp. 41–47, Jul. 2018.
14. Y. Qiu, H. He, Z. Qian, S. Li, and X. Zhang, "Lossless data hiding in JPEG bit stream using alternative embedding," *J. Vis. Commun. Image Represent.*, vol. 52, no.2, pp. 86–91, Apr. 2018.
15. C. Qin, Z. He, H. Yao, F. Cao, and L. Gao, "Visible watermark removal scheme based on reversible data hiding and image in painting," *Signal Process. Image Commun.*, vol. 60, no. 3, pp. 160–172, Jan. 2018.
16. Z. Tang, Q. Lu, H. Lao, C. Yu, and X. Zhang, "Error-free reversible data hiding with high capacity in encrypted image," *Optik - Int. J. Light Electron Optics*, vol. 157, no. 9, pp. 750–760, Dec. 2018.
17. J. Wang, J. Ni, X. Zhang, and Y.-Q. Shi, "Rate and distortion optimization for reversible data hiding using multiple histogram shifting," *IEEE Trans. Cybern.*, vol. 47, no. 2, pp. 315–326, Feb. 2017.
18. S. Yi and Y. Zhou, "Binary-block embedding for reversible data hiding in encrypted images," *Signal Process.*, vol. 133, no. 2, pp. 40–51, Apr. 2017.
19. S. Agrawal and M. Kumar, "Mean value based reversible data hiding in encrypted images," *Optik - Int. J. Light Electron Optics*, vol. 130, no. 5, pp. 922–934, 2017.
20. X. Zhang, Z. Sun, Z. Tang, C. Yu, and X. Wang, "High capacity data hiding based on interpolated image," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9195–9218, Apr. 2017.
21. Z. Tang, F. Wang, and X. Zhang, "Image encryption based on random projection partition and chaotic system," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8257–8283, Mar. 2017.
22. X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 9, pp. 1622–1631, Sep. 2016.
23. D. Xu and R. Wang, "Separable and error-free reversible data hiding in encrypted images," *Signal Process.*, vol. 123, no. 6, pp. 9–21, Jun. 2016.
24. X. Cao *et al.*, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Trans. Cybern.*, vol. 46, no. 5, pp. 1132–1143, May 2016.
25. F. Huang, J. Huang, and Y. Q. Shi, "A new framework for reversible data hiding in encrypted domain," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2777–2789, Dec. 2016.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

26. Prabha and M. Jagadeeswari, "Enhanced imperialist competitive algorithm based efficient reversible data hiding technique," *Multimed. Tools Appl.*, vol. 79, no. 6, pp. 4057–4074, 2020.
27. Fang, C. Yin, J. Zhu, C. Ge, M. Tanveer, A. Jolfaei, and Z. Cao, "Privacy protection for medical data sharing in smart healthcare," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 16, no. 3, pp. 1–18, 2020.
28. R. Mansour and S. Parah, "Reversible data hiding for electronic patient information security for telemedicine applications," *Arab. J. Sci. Eng.*, vol. 46, no. 3, pp. 9129–9144, 2021.
29. R. Motomura, S. Imaizumi, and H. Kiya, "A reversible data-hiding method with prediction-error expansion in compressible encrypted images," *Appl. Sci.*, vol. 12, no. 19, p. 9418, 2022.
30. Zeenath, K. DurgaDevi, and J. M., "An efficient image encryption scheme for medical image security," *Int. J. Electr. Electron. Res.*, vol. 12, no. 3, pp. 964–976, 2024.
31. S. Jayakumar *et al.*, "Risk analysis of data privacy violations in digital health records and patient confidentiality," *Semin. Med. Writ. Educ.*, vol. 3, no. 1, p. 498, 2024.