Complex entropy based encryption and decryption technique for securing medical images

Vinod Kumar¹,² · Vinay Pathak³ · Neelendra Badal⁴ · Purnendu Shekhar Pandey⁵ · Rajesh Mishra⁶ · Sachin Kumar Gupta⁷

Received: 25 March 2021 / Revised: 27 October 2021 / Accepted: 5 November 2021 /
Published online: 26 July 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
During medical picture transmission, the most pressing concern is security. Medical images must be encrypted since they are extremely sensitive. Watermarking, digital fingerprinting/signature, and encoding are some of the available image security techniques. Images and movies, for example, must be highly encrypted and decoded without losing any content information. Medical photos, for example, require extra protection, and protecting medical images is a critical issue when medical images and related patient information are transferred over public networks. This research work proposes a visual encryption strategy to secure medical pictures before being transmitted or stored in the cloud. This technique makes such pictures of unauthorized people unavailable and also maintains confidentiality, a prime safety requirement. The process made use of a pixel shuffling-based encryption technique and a secret key created from the image. In this research, we encrypted the medical image using modified Arnold Map Encryption and generated secret key values. Therefore, the image is encrypted, and henceforth it is decrypted as well. So this work gave us the encrypted image and decrypted image/original image as well. The modified Arnold Map Encryption tries to add more randomness, thus increasing the entropy of the image and thus makes it harder to decrypt. The modified Arnold Map Encryption is also compared to other algorithms such as Hyper Chaotic, Secure Hash Algorithm-13 (SHA-13), Ten Logistic Maps, Bakers Map, HenonMap, Cross Chaos Map, and 2D Logistic Map and shows better results in terms of encryption speed and Number of Pixel Change Rate (NPCR) value.

Keywords Security · Medical image · Encryption · Decryption · Modified Arnold map encryption · NPCR

Vinod Kumar
vinod242306@gmail.com

Sachin Kumar Gupta
sachin.gupta@smvdu.ac.in

Extended author information available on the last page of the article
1 Introduction

Internet usage for media content distribution has become a very popular way for nearly all Online-using organizations to exchange digital information. It is, hence, important to get information over open and attack the prone network to guarantee information security [10, 12]. It is critical to get information across open and attack the prone network to ensure significant information security. The patient’s medical details are important and must be safeguarded in storage and transmission between two hospitals, particularly the cloud. This is why the use of cryptography is very important in protecting these data [26]. Cryptography is used to convert information using an algorithm in encryption processes that are unreadable to anyone other than those with special expertise, which is typically referred to as a key. The process result is encrypted data. The other way around is known as decryption. From classic systems like Caesar, Trifid, or Vigenère to modern cipher systems like Diffie-Hellmann, etc. In digital computing, cryptography was built into many different digital formats, including text, video, etc., e.g. we used the chest x-rays images and encrypted them using modified Arnold’s Cat Map algorithm and then saved this data over the cloud [23]. Earlier, the hackers tried to take these images to help detect whether a patient is suffering from Covid-19. These images show the impact of medicine on the lower respiratory tract.

One will hide secret data in different communication mediums using Steganography techniques. The channel wants to hide is named a “Cover Object”. Cover Object is often in any digital form that has the flexibility to cover data like a picture, audio, video, unlike a text within, which cannot hide the existence of secret data. The key data (digital form), we would like to hide within the cover object are often text, video, audio, or an image. Cover Image at the side of the hidden information is understood as a stego image. Steganography that employs an image as a cover object is known as image steganography. The most essential consideration while constructing an Image Steganography technique is that the image’s appearance after hiding the secret message within the cover image may change dramatically, and an untrained eye will notice that the image is indisputably different from the original. An image Steganography technique is claimed to be excellent if the cover image does not show (visually) the changes made to it once concealing secret message (although there may be some statistical analysis that may be performed to find out the changes) [4, 27].

The transform Domain and the Spatial Domain are the two key domains in which Steganography is frequently done. The cover objects are translated to an entirely other frequency domain in the transform domain to induce the transformed coefficients. To conceal sensitive information, the modified coefficients are manipulated. The inverse transformation is applied to coefficients to induce Stego signals. Simultaneously, there is manipulation in the storage and concealment of secret data of a pixel’s intensity value in the spatial domain. Spatial domain techniques, which are more vulnerable to attacks due to changes in actual sample values, differ from transform domain techniques [9].

1.1 Features of Stegnography

Imperceptibility: Ought to be such that no intruder will sense the existence of the secret message. (Invisible to a naked eye).
Capacity: Must to offer the maximum amount capacity as it can.
Security: It is the measure of un-detectability.
Robustness: Keep the embedded information intact in the cover object.

Millions and billions of bytes of data are exchanged every day across the internet. Some of this data is confidential and is required to be transferred securely. The healthcare industry also relies on gigantic amounts of data, which is mainly in three forms, namely, tabular (ex. Medical records), images (X-Ray Images), and signals (Electroencephalogram, i.e. EEC data) [3, 14].

With the extensive use of technologies in the healthcare department, the old ways of handling this data have to be changed. This data is private for the individual and can be misused if it gets into the wrong hands, so it needs to be transferred safely and securely to the recipient, that is where cryptography comes into play. Numerous studies [29] have shown that the complexity of solving an “Elliptic-Curve-Discrete-Logarithmic Problem” grows exponentially in terms of the size of the key used. Therefore, Elliptic Curve Cryptography (ECC) is being used over other techniques like RSA in many industries, and even blockchain technology uses ECC to encrypt its data [30].

The “Diffie Hellman key exchange” is a cryptographic mechanism used to securely exchange crypto keys over the public network in such a way that even if someone tries to overhear communication, the keys will not be revealed. These exchanged keys will be later used for our encrypted communication, as shown in Figs. 1 and 2 [20].

RSA is one of the prior public-key cryptosystems, and it depends on the math of measured exponentiations and computational trouble of the RSA issue. It can work with different keys lengths: 1024, 2048, 3072, 4096, 8129, 16,384, or even greater than these; generally, key lengths of more than 3072-bits are considered secure. As RSA is deterministic (i.e., has no arbitrary segment), assailants can effectively cause a plain-text assault against it by encoding likely plain-texts with the public key and test if they are equivalent to the ciphertext or not. This probably will not be an issue, yet it is a shortcoming to be considered while picking an encryption scheme. Hybrid encryption plans like RSA-KEM conquers this defect and permits encoding bigger texts [8]. The most adopted standard scheme for signature verification for the RSA signatures is “PKCS#1”.

![Diffie Hellman key exchange](https://cryptobook.nakov.com/asymmetric-key-ciphers/ecc-encryption-decryption)

**Fig. 1** Encryption process in hybrid schemes (Source: https://cryptobook.nakov.com/asymmetric-key-ciphers/ecc-encryption-decryption)
Algorithms like ECC and RSA are good for encrypting and decrypting the majority of text data, but when it comes to images, the data size skyrockets, and a third party is necessary to validate the keys. As a result, simply implementing the RSA or ECC techniques took a long time [18]. As a result, Arnold’s Cat Map algorithm [6, 19] is one of the better options. The algorithm’s approach entails rotating the image repeatedly until it takes on a recognised yet unknown shape. As a result, we adopt Arnold’s Cat Map algorithm to enhance entropy; the higher the entropy, the more difficult it will be to decrypt the data.

The given model will encrypt the image using the modified Arnold 2D CATMap algorithm. Since every image will have different entropy values, there will be no connection between two different images. The attacker can identify any similarity to decrypt the images, and iterations can also be increased again, making it difficult for the attacker to decrypt the images. Overall, this approach makes the given model more secure compared to other techniques in the state of the arts and is faster also.

The rest of the research paper is organized as follows. In Section 2, a literature review and background discussion have been done, while in Section 3, the proposed algorithm is explained. Section 4 shows the results of our model also in comparison with existing other models. In Section 5, the conclusion and future work is discussed.

2 Literature review and background discussion

In the transmission of medical images, security is the most important thing. Since medical pictures are so fragile, they must be secured. The current image security techniques include watermarking, digital fingerprint or signature, encryption. However, there are several disadvantages to all these approaches [1, 17]. The newly proposed approaches would be swift to ensure that no data is discarded. Traditional Internet security procedures are insufficient to ensure that medical photos are not tampered with during data transfer. As a result, we will employ a different encryption approach to ensure that no medical images are harmed.
A simple image (input image) is used to generate a secret key on a device. The secret key, which is obtained from Eq. 1, has been used to rearrange the image pixels based on our proposed algorithm randomly.

\[
S.K. = \left( m \times n + |(Q \times 103)| + \left( \frac{1}{n} \left( \sum_{i=1}^{n} x_i \right) \right) \right) \mod n
\]  

(1)

Where \( m, n \) = size of the source starting image.

\( Q \) = entropy of the source starting image.

S. K. is the secret key which is used to encrypt and decrypt the image.

In Fig. 3, OI is the input image, and EI is the encrypted image, EA: represents the encryption algorithm, and DA: represents the decryption algorithm. In the process of encryption, as discussed above, the RGB colours of the original image were randomly arranged [2, 7].

The image is ciphering for the analysis mainly focused on the image’s RGB pixel values, the secret key extracted from the image. After looking at the original image’s bit values and

![Fig. 3 Encryption and decryption phase](image-url)
pixels of the original image there was no change and expansion respectively after the encoding and decoding phase.

To get the ciphered images, pixel values changed from pixel positions, and its RGB values were swapped. This means that the overall change in all pixel values was zero. Therefore, the total image size during the whole cycle has not changed [11, 13].

Another method to secure the medical images has been suggested by Moni Naor and Adi Shamir [22]. In this method, a new technique is used to encrypt images into shares that can be decrypted only if the corresponding number of shares are stacked together, known as Visual Cryptography. It uses AES as well as visual cryptography [15, 22]. The advantage of the cloud is that we can store data and access any data at any instant of time as needed. It can be used to transfer and recover this data, as shown in Fig. 4.

The important parameter of visual cryptography (k, n):

- m - m value is indirectly proportional to the resolution of the pixel.
- α - Alpha value is proportional to the resolution of the image. Also, it tells about the dissimilarity of the image.

---

**Fig. 4** Showing encryption and decryption phases
• **k** - Minimum number of sharing of the images to build an original image. The value of ‘k’ is directly proportional to the clarity of the reorganized image.

• **n** - An integer value that tells us about the image is divided into how many “number of shares”.

This method contains the following four phases:

• In the first phase: The advanced encryption standard technique is used for encryption. In this phase, encryption uses four kinds of transformations and a substitution table. Then the result will fetch to the next phase.

• Expansion: This phase helped them to divide images into shares using the n out of n VSC techniques. In this phase, they used both VSC and AES by extracting pixels, several shares, making a growth matrix, and adding it with AES, and then those shares go into the next phase.

• Collecting data: They used to collect and store data during this phase which can be stored into AWS S3 Bucket.

• Construction/decryption phase: They take all the collected shares and rejoin them to get the real image and use the AES decryption method.

The authors used different techniques and analyzing methods to check the characteristics of this proposed method and got some amazing results. They conclude that the technique is powerful, and its opposition power is high against many direct attacks. The presented technique easily finds the difference between keys, even if there is only a slight difference between two keys. The quality of the reorganized image is high, and it also tells us about the visual quality by using Eq. 2:

\[
\text{Peak Signal} \over \text{noise(decibels)} = \infty
\]  

(2)

The real and restructured images have the same structure. They confirmed that extracting any information about the real image is difficult after evaluating the histogram. The integrated effect of VSC and AES makes this approach much more powerful and reliable.

### 3 Proposed algorithm

The algorithm clearly states that the images are taken as input and then builds an image object by interpreting each matrix element (line 2). Then the size of the image is calculated (line 3). After the size is calculated, the entropy is calculated (line 4). It should be noted that it is harder for the attacker to find the original image from the encrypted image more the entropy. Calculate the mean of the plain text (line 5). After finding the mean of the plain image, the secret key (SK) is computed (line 6). The red, green, blue component is extracted from the image as shown (in line 8–10). Image is transformed and reshaped (in lines 11–14). Add the array r, g, b in the same dimension of ‘b’ or ‘r’ or ‘g’ of the original picture. At last, the information will be changed over into a picture format to get the scrambled picture (line 16).
3.1 Explanation of algorithm

Firstly, we will import the input image into the program then we will compute the size, entropy, and mean of the image to calculate the secret key for encrypting/decrypting the image. The secret key will be obtained by using Eq. 1.

After calculating the secret key of the image, we will extract the green, red, and blue (R,G,B) components of the image, and then we will compute the permutation for each pixel of the original image. To shuffle the pixels of the input image, we will be using a chaotic map. We will perform multiple iterations of this transformation over the input image, giving us the encrypted image. To decrypt the encrypted image, we will perform the inverse of this transformation iteratively until we get the original image.
3.2 Explanation of code

The algorithm used in this research is “Modified Arnold’s Cat Map”. Following are the steps of how algorithms work:

1. The first step is reading the colour pixel value (RGB values) of the image matrix.
2. After the first step, we need to calculate and store the X, Y position of the image pixel that has to be encrypted in a 2D array.
3. In the third step, we perform the random rotation which may call the number of iterations of the RGB pixels of the image so that it becomes non-recognizable.

This map is a chaotic map often used for pixel manipulation. It applies a transform on the image that essentially shuffles the pixels by stretching and folding the image. When an optimal number of iterations of the transformation is implemented over the source image, the output of the image becomes incomprehensible and hence encrypted. The reading of the image, calculating the secret key, and its implemented code is shown in Figs. 5, 6, 7, and 8, respectively. For this implementation, the transform applied on the image is done using Eq. 3:

$$R([x, y]) = [(x + y) \mod n, (x + 2y) \mod n] \quad (3)$$

where n is the dimensions of the image.

Decryption is known as inverted encryption. The decryption phase is performed by shuffling the pixels using ACM, creating key values using the chaotic map, and eventually reversing the encrypted pixel values to obtain the real image. Since we have been using a chaotic map, i.e.
ACM, and we have got a skewed image in the encryption phase using a key-value, as shown in Fig. 9, and at the same time, we have got the source starting image in the decryption processing shown in Fig. 10 as the same key between host and client that was used during the encryption process. Figure 11 shows the image after decryption to get the original image.

### 3.3 Software’s used

Following are the libraries and platforms that have been used in this research:

1. Google Colaboratory
2. Python
3. Multiple Python Libraries
   
   3.1 NumPy
   3.2 os
   3.3 cv2
4 Result discussion and analysis

Our algorithm is highly secured as the transformation function we used to shuffle the pixel to get the encrypted image is unique and cannot be guessed by any unauthorized party to re-shuffle pixel values to get the original content. Also, our encryption and decryption are based on the number of iterations equivalent to the secret key value, and each image will have a unique secret key as every image has different values of entropy, mean, and size. Hence, it makes our algorithm more secure as iteration value will not be shared with any unauthorized party, as depicted in Fig. 12.

Arnold Map Encryption has been modified, and there, we tried to introduce more randomness as given in Eq. 4, by introducing randomness, we make sure that it becomes harder for an attacker to decrypt. The logic behind adding randomness is that it increases the entropy of the data and makes it harder for the attacker to decrypt.

\[
S.K. = \left[ (m \times n) + \left| \left( Q \times \text{random}(50, 103) \right) \right| + \left| \left( \bar{x} = \frac{1}{n} \left( \sum_{i=1}^{n} x_i \right) \right) \right| \right] \mod n + \text{random}(27, 99) \tag{4}
\]

---

```python
[ ] def ModifiedArnoldCatTransform_dec(img, num):
    rows, cols, ch = img.shape
    n = rows
    img_modified_arnold = np.zeros([rows, cols, ch])
    for x in range(0, rows):
        for y in range(0, cols):
            img_modified_arnold[(x+y)%n][(x+2*y)%cols] = img[x][y]
    return img_modified_arnold
```

Fig. 10 Function used to transform the original source image

```
3.4 random
3.5 Math
3.6 tqdm
3.7 PIL
```

**Fig. 10** Function used to transform the original source image

**Fig. 11** Calling the decryption function to decrypt the encrypted image

---

Multimedia Tools and Applications (2022) 81:37441–37459

---
Intensity histograms If we compare Figs. 13 and 14, particularly the pixel intensity, then from the both Figures it is clear that it is harder for the attacker to find the encrypted image. Also, it will be difficult for attacker to find out the keys which is used to encrypt the data.

4.1 Adjacent pixel autocorrelation

Since images exhibit high information redundancy, it is desirable to have an encryption algorithm that breaks this redundancy. Thus as a metric of encryption performance, we find the correlation ($\sigma$) is applied between the adjacent pixels in the various direction such as horizontal, vertical or in a diagonal way. We have considered the horizontal direction.

As shown in Figs. 15 and 16, it clearly shows that pixel correlation in modified Arnold Cat Encryption is too random compared to the source starting image and that’s what makes it harder to guess compared to the source starting image.

![Intensity Histogram - Original Image](image)

**Fig. 13** Intensity histogram-original image
4.2 Results comparison with other algorithms

Here, the modified Arnold Map Encryption is compared to other algorithms such as Hyper Chaotic and SHA-13 in terms of encryption speed as it is indeed an important criterion to select an algorithm for real-world application. If an algorithm is harder to break but takes more time to process, that algorithm is indeed not a good solution. Thus, Fig. 17 and Table 1 clearly show that it is secure and also the speed of encryption is faster compared to other algorithms such as Hyper Chaotic and SHA-13.

As shown in Fig. 18 and Table 2, the NPCR estimates the quantity of pixels change rate in an encoded picture when 1 bit is changed in the source plain picture. Thus, as shown in Fig. 18 NPCR value comparison of modified Arnold cat with ten logistic maps, bakers map, henon map, cross chaos map, and 2D logistic map. It can be seen that the modified Arnold cat outperforms all the other algorithms.
From Table 1, it is clear that the encryption speed is much higher in the modified Arnold CATMap algorithm than in other algorithms. Faster encryption speed makes our suggested algorithm more useful as compared to previously used algorithms.

For differential attack, an attacker changes a specific pixel in the plain image and traces the differences in the analogous encrypted image to find a meaningful relationship. This is also
known as a chosen-plaintext attack. A robust encrypted image must be sensitive to minor changes, and even changing one bit in the plain image should result in a wide range of changes in the cipher image. The given Eq. 5 calculates this parameter, and for an ideal encryption algorithm, it is considered 1.

**NPCR** = \(\frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} f(i, j) \times 100\)

\(f(i, j) = 0\) if \(c1(i, j) = c2(i, j)\)

\(f(i, j) = 1\) if \(c1(i, j) \neq c2(i, j)\) \hspace{1cm} (5)

Where \(c1\) and \(c2\) are obtained by encrypting two \(m \times n\) plain images and one random bit dissimilarity, from Table 2, if we compare the NPCR values, we find that NPCR values

| S.No. | Algorithms Name                | Encryption Speed |
|-------|--------------------------------|------------------|
| 1     | Hyper Chaotic                  | 0.42             |
| 2     | CAT Map                        | 0.5              |
| 3     | Modified Arnold CAT Map        | 0.6              |
| 4     | SHA-13                         | 0.39             |
are highest at 0.994 in Modified Arnold 2D CATMap while NPCR values are very less in other algorithms. Higher NPCR values make our algorithm more secure because it will make it difficult to find the decryption key.

Thus, Table 3 clearly explains the importance of Modified Arnold Cat algorithm over conventional approaches such as Attribute-based Cryptography Technique, Identity Based Encryption (IBE), Diffie-Hellman Key exchange, Homomorphic Encryption and Challenge-based Trust Mechanism. It not only supersedes the conventional approaches but suffices the latest approaches such as 10 logistic maps, bakers map, henon map, cross chaos map, and 2D logistic map, hyperchaotic and SHA-13 as shown in Tables 1 and 2, respectively.

Table 2  Comparison of modified Arnold cat with other algorithms in terms of NPCR values

| S.No. | Algorithms Name               | NPCR Values |
|-------|-------------------------------|-------------|
| 1     | 10 Logistic Map               | 0.935       |
| 2     | Arnold 2D CAT Map             | 0.98        |
| 3     | Modified Arnold 2D CAT Map    | 0.994       |
| 4     | Baker Map                     | 0.932       |
| 5     | Henon Map                     | 0.94        |
| 6     | Cross Chaos Map               | 0.94        |
| 7     | 2D Logistic Map               | 0.942       |

Table 3  Comparison of modified Arnold cat with conventional approaches

| S.No. | Techniques                          | Demerits                                                                 | Merits                                                                 |
|-------|-------------------------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------|
| 1     | Attribute based Cryptography Technique [28] | While decoding or so called decryption phase, the code text is unscrambled completely which uncovers the whole message. | During unscrambling measure, the code text is decoded specifically divides just, for which secret keys are available. |
| 2     | Identity- based encryption (IBE) [24, 25] | Assuming Public Key Generation (PKG) is undermined, the information is at a more risk of exposure. | In Modified Arnold Cat algorithm, whole information has been put as per function and the secret keys. Information are produced separately for each function applied to plain content. |
| 3     | Diffie-Hellman Key exchange [5]     | Verification phase is not done.                                          | The confirmation phase is done among all entities such as server, client etc. by utilizing nonce signal. |
| 4     | Homomorphic encryption [21]         | The decoding of code text will either uncover the whole message or won’t be unscrambled by any means. | The decoding of code text will create just that segment of plain-text which the client has requested. |
| 5     | Challenge based trust mechanism [16] | Technique can be fizzled, if the vindictive hub has some data about close by traffic. | Regardless of whether the malicious host has some data in regard to continuous traffic, they cannot uncover the whole plain-instant message as it is scrambled by various functions. |
5 Conclusion and Future Work

A modified Arnold Cat algorithm is an encryption approach that is good enough to safeguard digital documents, particularly pixel security whereas other algorithms are more focused on protecting files or text. The image can be readily safeguarded using the Modified Arnold Cat algorithms without compromising the image’s importance or details. Hence, the proposed scheme may be used to protect the crucial medical image data. In the future, an interface or software can be created to save the medical image in a huge database, ensuring that the encrypted image is securely stored before transmission. We can say that this approach is suitable for operations like the encryption of medical images and the secure transfer of internet content.

Authors’ contributions Vinod Kumar, Vinay Pathak, Neelendra Badal, Sachin Kumar Gupta are the main authors of the current paper. They contributed to the development of the ideas, design of the study, theory, result analysis, and paper writing. Purnendu Shekhar Pandey, Rajesh Mishra contributed to the result analysis and paper revision. All authors read and approved the final manuscript.

Data availability Not applicable.

Declarations

Conflict of interests/competing interests The authors declare that they have no competing interests in terms of financial or non-financial.

References

1. Abdemouleh MK, Khalfallah A, Bouhlel MS (2017) A novel selective encryption scheme for medical images transmission based-on JPEG compression algorithm. Procedia Computer Science 112:369–376
2. Aqel MJ, QadiZA, Abdullah AA (2018) RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication. Int J Eng Technol 7(3.13):104–107
3. Avudaipan T, Balasubramanian R, Pandiyans S, Saravanans M, Lakshmanprasamsk SK, Shankar K (2018) Medical image security using dual encryption with opposition based optimization algorithm. J Med Syst 42(208):408–424. https://doi.org/10.1007/s10916-018-1053-z
4. Blesswin AJ, Visalakshi P (2013) "an improved gray scale visual secret sharing scheme for visual information security," fifth international conference on advanced computing (ICOAC). Chennai:560–564. https://doi.org/10.1109/ICOAC.2013.6922012
5. Diffie W, Hellman ME (1979) Privacy and authentication: an introduction to cryptography. Proc IEEE 67(3):397–427
6. Elshamy AM, El-Samie FEA, Faragallah OS, Elshamy EM et al (2016) Optical image cryptosystem using double random phase encoding and Arnold’s Cat map. Opt Quant Electron 48:212–230. https://doi.org/10.1007/s11082-016-0461-x
7. Ghrib T, Pandey PS (2021) Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques. Bulletin of Electrical Engineering and Informatics (BEEI) 10(4):950–961
8. Groza B (2007) An extension of the RSA trapdoor in a KEM/DEM framework. Ninth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania:182–187. https://doi.org/10.1109/SYNASC.2007.61
9. Ismail SM, Said LA, Radwan AG, Madian AH, Abu-Elyazed MF (2018) Generalized double-humped logistic map-based medical image encryption. J Adv Res 10:85–98
10. Kester Q (2013) A visual cryptographic encryption technique for securing medical images. International Journal of Emerging Technology and Advanced Engineering 3(6):496–500
11. Kester QA (2013) Image encryption based on the RGB PIXEL transposition and shuffling. Int J Comput Network Information Security 5(7):43–50. https://doi.org/10.5815/ijcenis.2013.07.05

Springer
12. Kester Q, Nana L, Pascu AC (2013) A novel cryptographic encryption technique for securing digital images in the cloud using AES and RGB pixel displacement. European Modelling Symposium, Manchester 293–298. https://doi.org/10.1109/EMS.2013.51
13. Krishnan GS, Loganathan D (2011) Color image cryptography scheme based on visual cryptography. International Conference on Signal Processing, Communication, Computing and Networking Technologies, Thuckalay, India:404–407
14. Kumar V, Badal N, Mishra R (2021) Elderly fall due to drowsiness: detection and prevention using machine learning and IoT. International Journal of Modern Physics B 35(7):60–91. https://doi.org/10.1142/S0217984921501207
15. Kumar V, Badal N, Mishra R (2021) Body sensor networks architecture and security issues in healthcare application. IOP Conf Series: Materials Science and Engineering 1022:1–12. https://doi.org/10.1088/1757-899X/1022/1/012075
16. Li W, ForKwok L (2019) Challenge-based collaborative intrusion detection networks under passive message fingerprint attack: a further analysis. J Inform Security Appl 47:1–7
17. Madih S, Hussain MA (2014) Securing medical images by image encryption using the key image. International Journal of Computer Application 104(3):30–34
18. Mallouli F, Hellal A, Saeed NS, Alzahrani FA (2019) "a survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms," 6th IEEE international conference on cyber security and cloud computing (CSCloud)/5th IEEE international conference on edge computing and scalable cloud (EdgeCom). Paris, France: 173–176
19. Mansouri A, Wang X (2021) Image encryption using shuffled Arnold map and multiple values manipulations. Vis Comput 37:189–200. https://doi.org/10.1007/s00371-020-01791-y
20. Mohanty SN, Ramya KC, Rani SS, Gupta D, Shankar K, Lakshmanaprabu SK, Khanna A (2020) An efficient lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Futur Gener Comput Syst 102:1027–1037
21. Murugesan A, Saminathan B, Al-Turjman F, Kumar RL (2020) Analysis on homomorphic technique for data security in fog computing. Trans Emerging Tel Tech 31:1–16. https://doi.org/10.1002/ett.3990
22. Naor M, Shamir A (1994) Visual cryptography. Eurocrypt '94, Lect Notes Comput Sci 950:1–12
23. Prusty AK, Pattanaik A, Mishra S (2013) An image encryption & decryption approach based on pixel shuffling using Arnold cat map & Henon map. International Conference on Advanced Computing and Communication Systems, Coimbatore:1–6. https://doi.org/10.1109/ICACCS.2013.6938729
24. Rashid A, Sharma D, Lone TA, Gupta S, Gupta SK (2019) “Secure Communication in UAV Assisted HetNets: A Proposed Model,” 12th International Conference, SpaCCS, Atlanta, GA, USA, LNCS, Vol. 11611, 427–440
25. A. Rashid, D. Sharma, T. A. Lone, S. Gupta, S. K. Gupta, “Identity-Based Encryption in UAV Assisted HetNets: A Survey,” 10th IEEE International Conference on Computing, Communication and Networking Technologies, IIT Kanpur, 6(8), 2019. https://doi.org/10.1109/ICCCNT45670.2019.8944826.
26. Rohini S, Bairagi V (2010) Lossless medical image security. International Journal of Applied Engineering Research, dindigul 1(3):536–541
27. Sarmah D, Kulkami, A. Abraham, “Cryptography and Digital Image Steganography Techniques.” Optimization Models in Steganography Using Metaheuristics. Intelligent Systems Reference Library, Springer, Cham, 187, 33–48, 2020. https://doi.org/10.1007/978-3-030-42044-4_2
28. Sharma D, Gupta SK, Rashid A, Gupta S, Rashid M, Srivastava A (2020) A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. Transactions on Emerging Telecommunications Technologies, Wiley:1–32. https://doi.org/10.1002/ett.4114
29. Tahat N, Alomari AK, Al-Hazimeh OM, Al-Jamil MF (2020) An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem. J Discret Math Sci Cryptogr 23:4:935–948. https://doi.org/10.1080/09720529.2020.1734293
30. Varma, C., “A study of the ECC, RSA and the Diffie-Hellman algorithms in network security,” international conference on current trends towards converging technologies (ICCTCT), Coimbatore, 1-4, 2018, https://doi.org/10.1109/ICCTCT.2018.8551161.

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Affiliations

Vinod Kumar\textsuperscript{1,2} \cdot Vinay Pathak\textsuperscript{3} \cdot Neelendra Badal\textsuperscript{4} \cdot Purnendu Shekhar Pandey\textsuperscript{5} \cdot Rajesh Mishra\textsuperscript{6} \cdot Sachin Kumar Gupta\textsuperscript{7}

Vinay Pathak
vinaypathak85@gmail.com

Neelendra Badal
n_badal@hotmail.com

Purnendu Shekhar Pandey
shekhar.rockwell@gmail.com

Rajesh Mishra
rajeshmishra25@rediffmail.com

\textsuperscript{1} Computers Science & Engineering Department, O P Jindal University, Raigarh, Chhattisgarh 496109, India
\textsuperscript{2} Computer Science & Engineering Department, Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh 226031, India
\textsuperscript{3} Computer Science and Engineering Department, Galgotia College of Engineering and Technology, Greater Noida 201310, India
\textsuperscript{4} Computer Science & Engineering Department, Kamla Nehru Institute of Technology, Sultanpur, Uttar Pradesh 228118, India
\textsuperscript{5} Computer Science & Engineering Department, KIET, Group of Institutions, Ghaziabad, Uttar Pradesh 201206, India
\textsuperscript{6} Electronics Engineering Department, Gautam Buddha University, Greater Noida 201308, India
\textsuperscript{7} School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Kakryal, Katra, Jammu & Kashmir 182320, India