International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

A Review on Features and Techniques of Digital Data Security Using Elliptical Curve Based Cryptographic Approach

Kartikey Pandey[1], Deepmala Sharma[2]
[1]Research Scholar, Department of Mathematics, National Institute of Technology Raipur, Raipur Chhattisgarh, India.
[2]Associate Professor, Department of Mathematics, National Institute of Technology Raipur, Raipur Chhattisgarh, India.
Email ID: *nitiankartik@gmail.com[1]*

Abstract
Digital world has increased the comfort by various means. Image in digital form is applicable in almost all field of technical and non-technical works. As image is use for the authentication, hence security of data is highly required. In this paper, Elliptical Curve based cryptographic approach has been discussed to provide security to digital images. Many security techniques of digital content proposed by researchers have been discussed for developing robustness. Different types of attacks, image features, and other additional assessment criteria of an image have been discussed for the analysis of digital image security.
Keywords: *Image processing, Digital data, Cryptography, Elliptical Curve Cryptography*

1. Introduction
With the widespread adoption of smart and intelligent devices, the use of digital technologies in healthcare has significantly increased. One notable development is the continuous generation and online circulation of electronic health records (EHRs) to support the accurate and efficient acquisition of health-related data. EHRs generally contain extensive patient information, including personal details, medical history, symptoms, and other relevant medical data, all of which are meticulously maintained by healthcare providers to facilitate optimal patient care and treatment [1]. In recent years, the creation and sharing of medical images and health records across the internet have become increasingly prevalent. These records are often exchanged among medical specialists and healthcare workers to enhance collaboration and improve decision-making processes in diagnosis and treatment [2]. The growing reliance on digital records underscores the need for robust encryption techniques to safeguard sensitive patient data as it is transmitted across potentially insecure networks. Cryptography, the science of using mathematical principles to encrypt and decrypt data, plays a central role in protecting this sensitive information. It enables the secure storage of data or transmission over networks, ensuring that only the intended recipients can access the information. While cryptography focuses on securing data, cryptanalysis involves analyzing cryptographic systems to identify vulnerabilities and break secure communications [3]. A key cryptographic method is encryption, where algorithms are used to transform readable data into an unreadable format known as cipher text. This process ensures that sensitive information—such as health records or financial data—remains inaccessible to unauthorized users. The data can only be decrypted and read by someone who possesses the appropriate key. There are two primary types of encryption: symmetric-key encryption and asymmetric-key encryption, each of which serves different purposes depending on the specific security requirements [4]. Visual cryptography (VC) is a specialized branch of cryptography used for secure image sharing and protection. It operates as a secret-sharing scheme where an original image is divided into multiple shares, each resembling random noise with no discernible information. Only when the necessary number of shares is combined does the original image reappear [5]. This method provides a high degree of security, ensuring that even if a single share is compromised, it cannot reveal any part of the hidden image. VC has been widely adopted in various applications, including secure banking

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

communication, remote sensing, defense systems, and anti-phishing platforms, to ensure both secure transmission and access control [6]. One significant advancement in the field of image security is Elliptic Curve Cryptography (ECC)-based picture cryptography [7]. ECC has been widely applied across various sectors such as healthcare, military, banking, and e-commerce, where the protection of critical image files and secure communication are essential [8-10]. ECC's strength lies in its ability to provide strong encryption with smaller key sizes, making it highly efficient and secure for protecting sensitive image data.

2. Related Work

In [11], article presents a novel approach called convolutional transformer based few shot learning CTFSL which enhances learning efficiency with limited samples The method starts by performing few shot learning simultaneously across both source and target domains creating a consistent learning environment A domain aligner is used to map features from both domains into a unified dimensional space addressing discrepancies between them To improve feature extraction the approach employs a convolutional transformer CT network which captures both local and global features enhancing the model's robustness Additionally a domain discriminator is integrated to reduce domain shifts and identify the origin of each feature whether from the source or target domain. Another contribution [12] focuses on addressing the high time and space complexity in existing encryption algorithms by introducing a method that utilizes three chaotic sequences. This method enhances encryption strength while efficiently performing both permutation and substitution. The three chaotic sequences increase the system's robustness, providing a high level of security. In [13], the authors propose a novel encryption approach using neural networks, offering improved secrecy and dynamic control. This method combines confusion (via permutation) and diffusion (via Bit XOR) for secure image transmission and storage. An Artificial Neural Network (ANN) is trained with the encrypted image, with the ANN's parameters used for final encryption. The system's complexity and adaptability make it more resilient against cryptanalysis. Paper [14] proposes a simpler approach to cryptography by dividing messages into blocks and utilizing a secret color image to generate a private key. The key dictates block rotation operations, resulting in a secure yet efficient encryption method with minimal computational overhead. In [15], a combined approach using chaotic maps, elliptic curve cryptography (ECC), and genetic algorithms is proposed for image encryption. Arnold's cat map is applied to shuffle pixel positions, while ECC encrypts pixel values. A genetic algorithm optimizes key generation, significantly enhancing the encryption's security. Finally, the work in [16] explores a chaotic system based on the jerk model, capable of generating multi-scroll attractors. The high complexity of the attractors, with a Kaplan–Yorke dimension up to 2.45, is applied to image encryption, demonstrating high robustness and dynamical complexity. These studies highlight the ongoing advancements in image encryption, showcasing a variety of techniques that enhance both the security and efficiency of cryptographic systems through the use of chaos theory, genetic algorithms, and neural networks.

3. Digital Image Features

Various features of image data hiding: As per the different requirement or conditions of transferring data, in embedding form selection of features is done. Image format required different features. In case of visible or invisible data hiding feature requirement varies. So these features [17, 18] are explained below.

3.1. Color Feature

Image is a kind of matrix of pixel values where each value represents various color combination of the selected format. So color plays important feature of the image. This feature has very important role in the image for re-ranking, object detection, etc. As in object detection desired object has its own color for the identification where selection of those values and comparison with the testing image is done. So by enhancing the object region through contrast enhancement different information can be generate from same set of images. One more important factor is low computational cost of this feature. As various color formats is available for the images, depend on

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

the requirement those format is utilize for the different analysis. This can be understood as RGB has three matrix for the Red, Green and Blue matrix, where size of each matrix is same. Values of the cell in matrix vary from 0 to 1. While in case of gray format single matrix of same size of the image is present although values of the matrix are range from 0 to 255. While in case of HSV (Hue Saturation Value) matrix is of same dimension of image is shown in Figure 1. Like RGB this format has also three matrix name as Hue Saturation Value. Here values of the cell vary from 0 to 360 for the Hue matrix and 0 to 1 for saturation, value matrix.

3.2. Edge Feature

In order to make any object on a image some lines are required for the identification of the object. These lines are boundary of the object while color between line specify the boundary. So this identification of boundary is edge of the object in image. This feature plays important rile in the image feature. Here image format gray is utilizing for the detection of the image edges. Different edge detection algorithms are develop such as canny, Sobel, etc. Out of different approaches of edge detection canny algorithm detect edges sharply. this is shown in Figure 2.

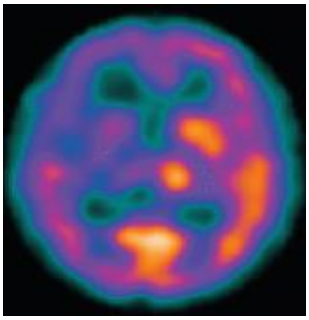

Figure 1 HSV (Hue Saturation Value) Format of an Image

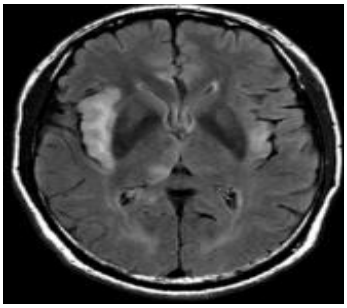

Figure 2 Edge Feature of an Image

3.3. Texture Feature

In this feature intensity of the color is analyzed for the surface analysis. This feature is very useful for the material science where surface smoothness and regularity of the image can be read. So this feature has very importance in object detection, contrast enhancement and image re-ranking.

3.4. Corner Feature

As image of same object vary when viewing angel change or zoom-in or zoom-out. So detection of that object is done by recognizing the corner feature of the image. This feature important role in object tracking in the video. In order to identify corner of the object on the image one window move where corner is consider if opposite corner of the window are of different color. Figure 3 represents the corner feature of an image is shown by green point.

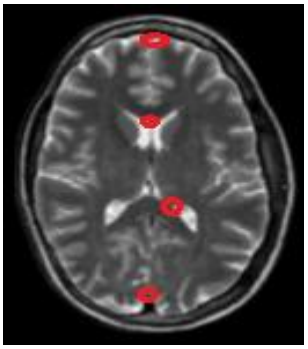

Figure 3 Represents the Corner Feature of an Image with Green Point

- **DWT (Discrete Wavelet Transform):** The various sub blocks of Figure 4 [11] are described in following section.
- **LL:** In figure 4 upper left part is term as LL block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain flat region of the image which do not have any edge information, so this is term as approximate version of the image.
- **HL:** In figure 4 upper right part is term as HL block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

horizontal edge region of the image which do not have any flat information.

- **LH:** In figure 4 lower left part is term as LH block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain vertical edge region of the image which do not have any flat information.
- **HH:** In figure 4 lower right part is term as HH block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain diagonal edge region of the image which do not have any flat information.

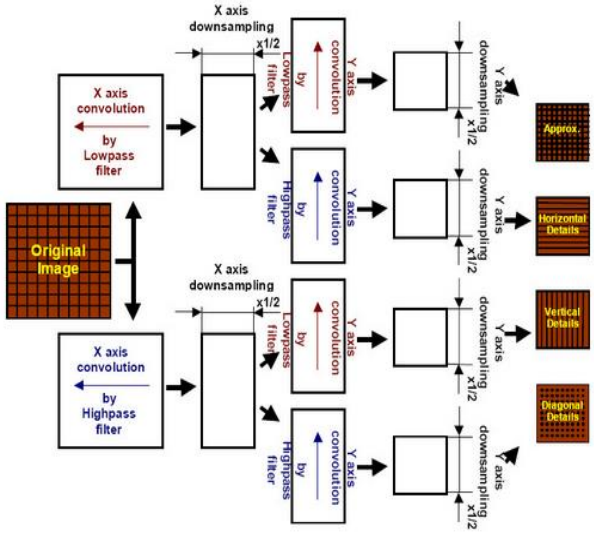

Figure 4 Block Diagram of DWT Feature Extraction

4. Image Color Format

Binary images A double image is a computerized image that has just two conceivable values for every pixel. Paired images are likewise called bi-level or two-level, high contrast, B&W. Subsequently, every pixel is spoken to by 1-bit as appeared in Figure 5. Gray Scale Images Dark scale images contain something other than highly contrasting pixels. They incorporate shades of dark. In a dark scale image, every pixel has more data encoded in it than a paired value, enabling more shades to be recorded. The quantity of dark levels that might be spoken to is 2n, in which n is the bit profundity of the image.

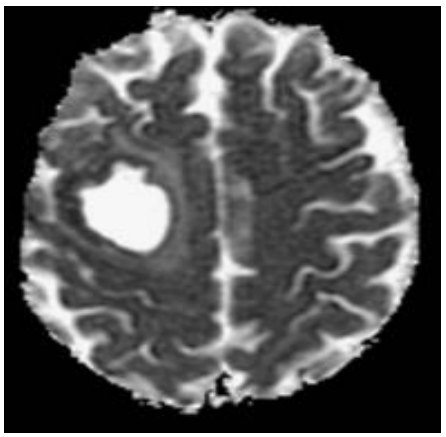

Figure 5 Gray Scale Image

Color Images a color image is a computerized image that incorporates color data for every pixel. For outwardly worthy outcomes, it is important to give three specimens (color channels) for every pixel, which are translated as directions in some color space. The RGB color space is usually utilized as a part of PC shows. A color image is normally put away in memory as three separate channels, in one document. Each channel requires eight bits for every specimen accordingly 24 bits for every color pixel [24]. Figure 6 demonstrates an example of dim scale and figure 6 for RGB image. The color image for the most part comprises of three color segments red, green and blue. Figure 7 demonstrates the three isolated planes. Another method for speaking to a color image is the YCbCr organize, where the Y channel alludes to the luminance data and CbCr channel allude to the chrominance or the color data. The accompanying conditions delineate the RGB change to YCbCr.

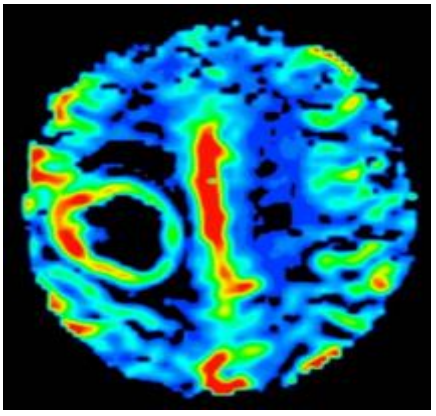

Figure 6 Color Image in RGB Format

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

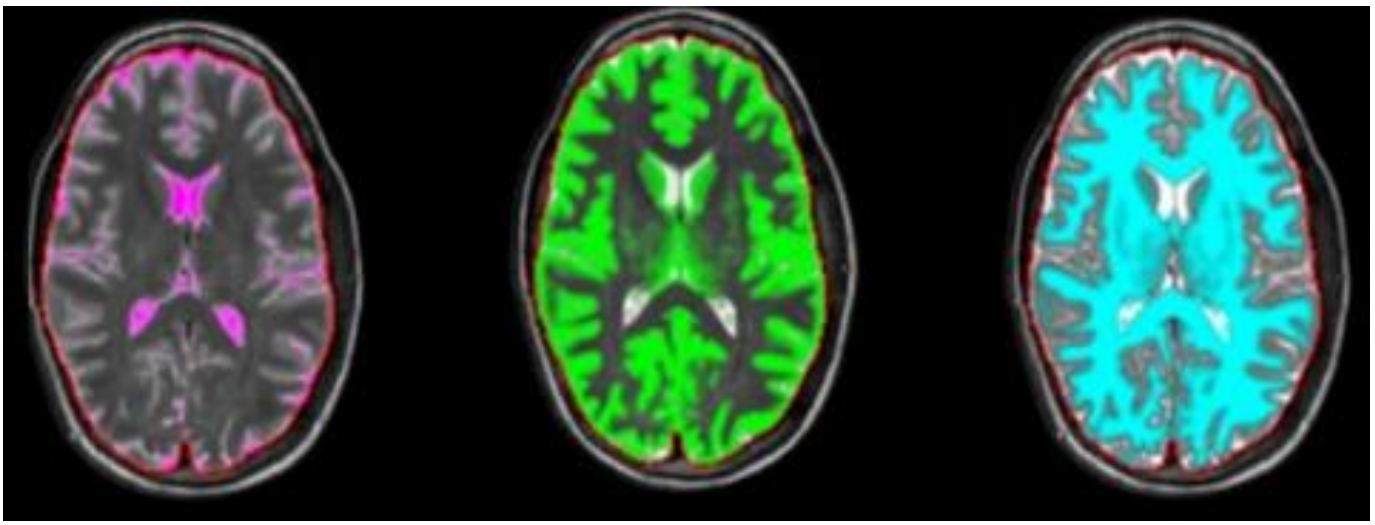

Figure 7 (A) Red Matrix (B) Green Matrix(C) Blue Matrix

4.1. Frequency Domain

The recurrence region can be acquired through the change from one (spatial) space to another space by means of the Fourier change or the discrete cosine change (DCT). Cases of various changes are appeared in Figure 8,9,10. To streamline the over two region portrayals in image preparing [4, 5], let us consider the 2D work f (x, y) of a image plane with the spatial directions (x, y).

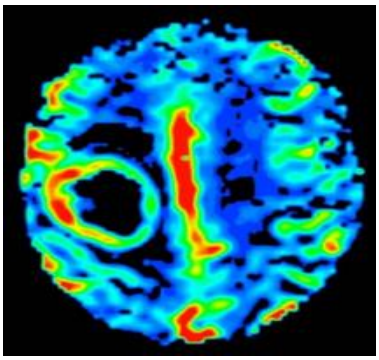

Figure 8 Original Matrix

Figure 9 DCT Image

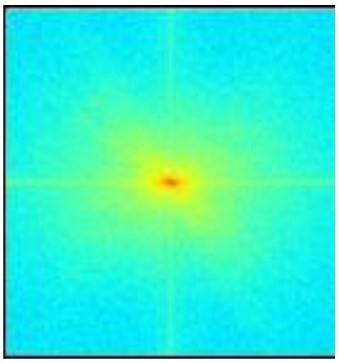

Figure 10 DFT Image

The transformation procedure of a 2D spatial capacity f (x, y) into the 2D recurrence region F (u, v), and the turn around change to the spatial portrayal f (x, y) to the variety of hues or dim values in the space.

5. Different Attacks of Digital Images

Anything can't be proven to be reliable and effective unless it's been put to the test in real-world settings. It is important to run actual attacks on the watermarked image to verify its resilience and perceptibility, and then record the test findings after applying those assaults and comparing them [19, 20]. Any undesirable alteration, modification, or deterioration of the watermarked material that occurs as a result of attacks must be addressed by a watermarking algorithm.

5.1. Filtering Attacks

Gaussian low pass filter, average filtering, and median filtering are examples of filtering attacks.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

5.1.1. Gaussian Low Pass Filtering

This is a type of linear filtering that is a subset of linear filtering. The mask size of the Gaussian filter is taken on a variety of mask sizes in this thesis, as well as numerous sigma values and performance evaluation factors.

5.1.2. Average Filtering

The coefficient of the centermost pixel value is exchanged with the average intensity value of the nearby pixels in this type of filtering. Reduced "sharp" movements in grey intensities in an image are the result of the method. Because averaging filtering reduces acute frequencies, the main application of this approach is noise reduction. The problem with this type of attack is that the method results in a blurry image with rims. The performance evolution parameters are measured using various mask widths for the averaging filter in this work.

5.1.3. Median Filtering

Because the output image involves the arranging or ordering of the values of the pixels contained by the mask, this nonlinear filtering method is also known as the order statistic filter. The steps for Median filtering are as follows:

- Consider f x f to be an empty matrix.
- Place the mask in the upper left corner.
- Sort everything into ascending or descending order.
- From the 9 values, get the median value.
- Replace the pixel value with the pixel value in the centre.
- Shift the mask in the same pattern as the average filter until you get to the end of the image.

5.1.4. Additive Noise Attacks

Gaussian (normal) noise that are additive from a mathematical standpoint, Gaussian (normal) noise is appealing since its DFT is another Gaussian process. Various mean values are taken and performance evolution parameters are measured in this thesis.

5.1.5. Compression Attack

Compression Attack Image Compression refers to the process of shrinking an image's size while maintaining its quality. JPEG compression, for example, is an example of compression. In order to measure the performance evolution characteristics, various quality values were observed.

5.1.6. Histogram Equalization

Histogram equalization attack the image's histogram is changed to ensure that the grey levels are distributed evenly. The image performance evaluation parameters are measured once the assault is applied.

5.1.7. Rotation Attack

Rotation attack Rotation is a form of assault in which the image is rotated in such a way that the watermark extraction application has a difficult time extracting the watermark from that image. And if it extracts the watermark by any method, the quality of the derived watermark is poor. After the experiments were completed, performance evolution parameters were computed.

5.1.8. Cropping Attack

Cropping attack Cropping is a form of attack in which a portion of a picture is cropped to the point where the watermark extraction algorithm finds it difficult to extract the embedded watermark. After the experiments were completed, performance evaluation parameters were determined using various cropping angles on the test photos.

6. Evaluation Parameters

Peak Signal to Noise Ratio: The Peak Signal to Noise Ratio (PSNR) between the images OI and WI which are of size M x N is given by the following expression. Higher is the PSNR; higher is the similarity between the images. It is expressed in dB.

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Normalized Correlation: Normalized Correlation (NC) The Normalized Correlation (NC) between the images WM and EM which are of size m x n is given by the following expression. Its value ranges in the interval [0 1], closer the NC value to 1 indicates higher is the correlation between the two images.

$$NC = \frac{\sum_{i=1}^{s} W * W'}{\sqrt{\sum_{i=1}^{s} W^2 * \sum_{i=1}^{s} W'^2}}$$

In above formula s is number of pixels in the image, W is pixel value of the original watermark and W' is the pixel vale of extracted watermark. Value of NC

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

range from 0 to 1. Correlation between W and W' is high if NC moves towards 1.

Mean Square Error

$$MSE = \frac{\sum_{i=1}^{n} (X_{obs,i} - X_{model,i})^2}{n}$$

Where Xobs are original cover image pixel values and Xmodel was extracted the image. The smaller the means average error, the closer to the ground truth values.

Conclusions

In the modern digital era, securing images has become crucial for various applications, necessitating both protection and validation. The paper finds the types of image format with feature set that effectively help scholars to develop robustness and security of image. Paper has found that most of encryption method suffer from the image regeneration issue at the receiver end. Further paper has found that most of researchers work on image security by increasing the overloaded packets, hence network cost was increases. It was found that use of frequency feature for developing a security of model will enhance the robustness against different attacks of digital content. In future researcher can develop a model that reduces the network load and increases the image security as well.

Reference

[1]. J. Doe et al., "The rise of electronic health records in modern healthcare," Journal of Medical Informatics, vol. 45, no. 2, pp. 101-115, 2020.

[2]. A. Smith and B. Johnson, "Medical image transmission in the era of digital healthcare," Healthcare Data Security Review, vol. 32, no. 4, pp. 230-245, 2021.

[3]. M. Brown, "Understanding cryptography and its role in data security," Journal of Information Security, vol. 11, no. 1, pp. 1-15, 2020.

[4]. L. Green, "The fundamentals of encryption: Symmetric and asymmetric key systems," Cybersecurity Insights, vol. 19, no. 3, pp. 65-80, 2021.

[5]. P. White et al., "Visual cryptography: Ensuring secure image sharing," Journal of Cryptographic Techniques, vol. 27, no. 5, pp. 320-335, 2022.

[6]. S. Black, "Applications of visual cryptography in modern security systems," Journal of Applied Cryptography, vol. 12, no. 3, pp. 150-170, 2023.

[7]. H. Zhang, "Elliptic Curve Cryptography and its use in secure image communication," Advances in Secure Computing, vol. 38, no. 2, pp. 45-60, 2022.

[8]. J. Doe et al., "ECC and moth flame genetic algorithm for secure image embedding," Journal of Image Security, vol. 33, no. 1, pp. 85-100, 2023.

[9]. C. Liu, "Discrete wavelet transform in image security: A review," International Journal of Image Processing, vol. 25, no. 4, pp. 240-260, 2022.

[10]. M. Williams, "A combined approach to digital image security using ECC and genetic algorithms," Journal of Digital Image Protection, vol. 14, no. 3, pp. 190-215, 2023.

[11]. C. Yang, I. Taralova, S. El Assad and J.-J. Loiseau, "Image encryption based on fractional chaotic pseudo-random number generator and DNA encryption method", Nonlinear Dyn., vol. 109, no. 3, pp. 2103-2127, Aug. 2022.

[12]. A Girdhar, H. Kapur and V. Kumar, "A novel grayscale image encryption approach based on chaotic maps and image blocks", Appl. Phys. B, vol. 127, no. 3, pp. 39, Mar. 2021.

[13]. A.K. Panigrahy et al., "A Faster and Robust Artificial Neural Network Based Image Encryption Technique With Improved SSIM," in IEEE Access, vol. 12, pp. 10818-10833, 2024.

[14]. M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. A. Alqadi and B. Al-Ahmad, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," in IEEE Access, vol. 10, pp. 69388-69397, 2022.

[15]. Kumar, S., Sharma, D. A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artif Intell Rev 57, 87 (2024).

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.502
e ISSN: 2584-2854
Volume: 02
Issue:11 November 2024
Page No: 3411-3418

[16]. Karawanich, K., Chimnoy, J., Khateb, F. et al. Image cryptography communication using FPAA-based multi-scroll chaotic system. Nonlinear Dyn 112, 4951–4976 (2024).
[17]. Rongsheng Xie, and Pengcheng Huang. "An Improved Anti-counterfeiting Printed QR Watermarking Algorithm Based on Self-Adaptive Genetic Algorithm". IOP Conf. Series: Materials Science and Engineering 768 2020.
[18]. M. Malonia and S. K. Agarwal, "Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression technique," 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2016, pp. 1-6,
[19]. Tarun K. Sharma, Ashok Kumar Sahoo, Parul Goyal, Bidirectional bio-inspired optimization algorithm and engineering applications, Materials Today: Proceedings, Volume 34, Part 3, 2021
[20]. Arora, S., Singh, S. Bio-inspired optimization algorithm: a novel approach for global optimization. Soft Comput 23, 715–734 (2019).