ISSN 2278-3091

Volume 9, No.4, July – August 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse61942020.pdf

https://doi.org/10.30534/ijatcse/2020/61942020

Privacy Preserving Image Encryption Approach for Cloud Storage

Mohamed Jafar Sadik[1], **Noor Azah Binti Samsudin**[2]

[1,2] Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Malaysia

[1]mohamad.jvp@gmail.com

[2] azah@uthm.edu.my

ABSTRACT

Hundreds of thousands of medical images are generated every single year for patients all around the world. The healthcare institutions confront the enormous challene to manage, archive, and retrieve the massive volume of medical images. Cloud is seen as a reliable solution to handle the medical imaging data; however, the need for a medical imaging management system which can preserve privacy and reliable is a must. Therefore, in this paper, a new encryption approach for medical images in cloud storage is proposed to handle privacy preserving image retrieval from the cloud. The proposed encryption approach has utilized the elliptic curve cryptography (ECC) encryption algorithm to encrypt data and store it in the cloud. The proposed approach has compared against other image encryption approaches. Results show that the proposed image encryption approach enhances the speed of the encryption process significantly and manage some powerful security features. The average processing time has decreased from 25 seconds to only 0.1 seconds.

Key words : Image Compression, Image Encryption, Elliptic Curve Cryptograph, Histogram.

1. INTRODUCTION

Nowadays, picture archiving and communication systems become very critical where the majority of hospital systems data are stored electronically, including a massive volume of patient’s information. The data include various types and forms like patient demographics, clinical measurements, test results, medical images and free text reports. The medical images can be categorized into two main types’ 2D modalities and volumetric images. Two-dimensional modalities images include plain X-rays and cell pathologies, where volumetric images include computed tomography images (CT), Positron emission tomography (PET), Ultra sound (US) and magnetic resonance images (MRI) [1]. On the other hand, multimodality devices have proposed by other approaches: PET-CT [2] and PET-MR [3] scanners, these approaches have the ability of implementing two different modalities for the same scanning session. Figure 1 demonstrates a subgroup of various kinds of medical images.

On the other hand, image encryption is essential for cloud-based image retrieval, which can be implemented in medical fields. Images stored in the cloud need to be encrypted using a reliable and secure approach which also can facilitate the searching recess and maintain user privacy [4]. In recent years, with the increasing number of medical images in hospital information management systems, different health image-based applications are developed including health information retrieval [5], recommendation and clustering [6]. These applications require a highly efficient access method to support content-based multimedia retrieval at a large scale as one of the most critical media types, medical images and their management, query, and analysis plays a critical role in the modern hospital information management systems [7].

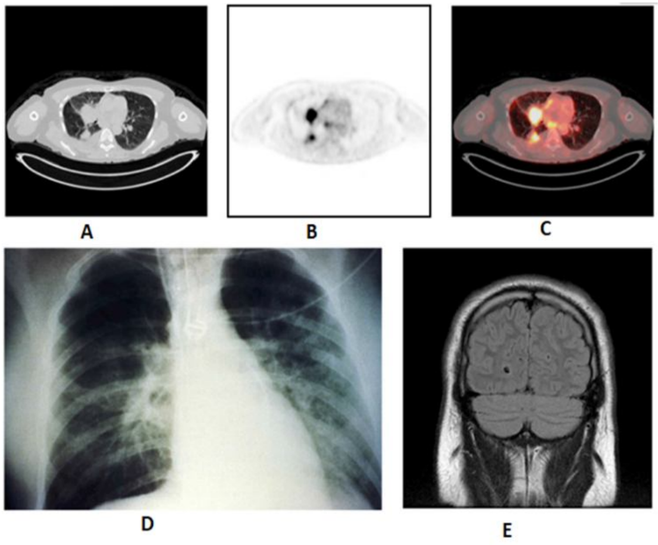

Figure 1: A subset of the medical images available in many hospitals. (A) axial CT slice, (B) axial PET slice, (C) axial fused PET-CT slice, (D) coronal MR slice, and (E) chest X-ray [8].

Various studies have been proposed to utilize potential clinical benefits of Content-Based Information Retrieval (CBIR) in medical applications. For instance, ASSERT CBIR system has used to handle high-resolution CT (HRCT) lung images. It mainly achieves enhanced accuracy of the diagnosis made by physicians [9]. Other research used the Content-Based Image Retrieval (CBIR) method to capture nodule images from the region of interest (ROI) image database in lung CT images [10]. Another study for liver CT concluded that CBIR could provide support for decisions making in real time [11]. CBIR Showed benefits when used as part of a teaching method for radiology [12].

In the medical field, the sharing platforms for Cloud-based medical image become triumphant in an increasing manner. In the end, physicians can build better and deeper referral networks using the online medical image transfer systems, which result in increasing data volumes and a more open collaboration platform. Cloud computing grasp more attention from vendors of information technology systems to provide substantial storage applications and efficient management for remote services. All healthcare corporations can use the cloud platform as an exchange platform, which provides storage center service for massive medical records. On the other hand, Security has considered as one of the critical issues of cloud computing, so adopting cloud approach can have its pros and cons in term of data security [13].

Security has been considered as the primary focal point when implementing a cloud-based medical image for knowledge sharing, and it also includes technological, physical or administrative safe parameters or tools which have implemented to handle identifiable health data protection from malicious access. Privacy and security requirements need to cover all storage media aspects, including disaster recovery and data protection. The mission of medical images security can be more challenging when it compared to other data aspects where health data are transmitted between various providers very often, where patients transfer between different places seeking additional care from another entity. On the other hand, privacy mainly focused on data protection where personal information of patients can be used carefully [13].

Based on the information demonstrated before a reliable and secure medical image system is required to encrypt the patient data and maintain its privacy. This system needs to depend on the cloud-based storage as its primary storage architecture to reduce the burden of storage management. The encryption process needs to be secure and efficient to minimize the processing overhead and support reliable searching in the cloud.

The rest of this paper has organized as follows. In section 2, a detailed description of related work for image encryption is presenting were drawbacks of existing algorithms have investigated. In section 3, the details of the proposed encryption algorithm have presented. Section 4 includes the implementation details of the ECC based encryption algorithm, and results is investigated and discussed. Section 5 concludes the findings.

2. LITERATURE REVIEW

Image privacy can be defined as the field of research that aims to defend image data from malicious attackers while still allowing legal users to manipulate image data [14]. Cryptography plays a key role mostly in secure transfer of images. Encryption is a method that used a finite set of guidelines called an algorithm to convert the original message defined as plain text into encrypted (or coded form) known as ciphertext. There are two types of encryption. This form of encryption uses a secret key, called the shared secret, to convert data into ciphertext. The person on the other end needs the shared secret (key) to unlock the data [15]. It is called symmetric cryptography because the same key is used on both ends for both encryption and decryption, e.g., -Genetic algorithm. The other is the Asymmetric Algorithm, which is also called Asymmetric cryptography. It is usually implemented by using one-way functions that are simple to compute in one direction, but very difficult to compute in reverse, e.g., the RSA algorithm [16]. Different algorithms have been proposed for achieving reliable image encryption. In the following table, different papers have been listed, and the pros and cons of each paper are discussed.

A new image encryption algorithm is proposed based on non-adjacent coupled map lattices in [17]. A new image encryption algorithm based on the spatiotemporal chaos of the mixed linear–nonlinear coupled map lattices. This chaotic spatiotemporal system has more outstanding cryptography features in dynamics than the logistic map, or the system of coupled map lattices does. It employs the strategy of bit-level pixel permutation, which enables the lower bit planes and higher-bit planes of pixel permute mutually without extra storage space. However, it has high computation overhead, and symmetric has the same keys used in the encryption and decryption process. An RGB image encryption algorithm based on total plain image characteristics and chaos is proposed in [18]) it mainly uses color image encryption algorithm based on total plain image characteristics to resist a chosen/known plain image attack, and 1D logistic map with optimized distribution, for the fast encryption process, based on Murillo-Escobar's algorithm. It mainly depends on RGB colors, which degraded with grayscale medical images and have high computation overhead.

Ye and Huang [19] propose a new structure of pre-modular, permutation, and diffusion (PPD) cipher for image encryption .it solves the low sensitivity of the plain-image when meeting invariance of pixel summation. A self-adaptive encryption scheme is implemented, and no extra transmission is needed. The keystreams used for encryption are designed dependent on the plain-image. However, it has a high computation overhead where symmetric has the same keys used in the encryption and decryption process. It also does not meet the requirement of the cloud in terms of third-party authentication.

Image encryption using 2D Logistic-adjusted-Sine map proposed in [20] A two-dimensional Logistic-adjusted-Sine map (2D-LASM). It mainly a mechanism of adding random values to plain-image that is designed to enhance the security level of cipher-image. However, 2D-LASM has complex, chaotic behavior, which requires high computation, and they use a large key-sized secret key of 232bits. Authors re-evaluate the security of a typical image-scrambling encryption algorithm (ISEA). They are using the internal correlation remaining in the cipher image. They also disclose important visual information of the corresponding plain image in a ciphertext-only attack scenario. The proposed solution has weak encryption due to the class of permutation-only encryption algorithms and using symmetric secret for encryption and decryption. A Modified Technique for Reliable Image Encryption Method using Merkle-Hellman Cryptosystem and RSA Algorithm. Finally, an enhanced Image Encryption Technique using DES algorithm with Random Image overlapping and random key Generation is proposed in [21]. In this approach, the authors used a random key along with random image overlapping for higher variation, which improved the security. However, this approach presents high computation overhead and required more time to complete the encryption process.

In general, the overhead of the recently proposed image encryption approach is quite high due to the used encryption algorithm. Symmetric algorithms like RSA present high overhead at the encryption process to encrypt and decrypt images. ECC encryption provide less overhead and higher encryption complexity when it is compared to symmetric encryption algorithms.

3. ECC BASED IMAGE ENCRYPTION APPROACH FOR CLOUD

In our study, images can be encrypted using a lightweight approach using ECC, and these encrypted images can be searched and retrieved from the cloud while image privacy is preserved. Proposed encryption can also be efficient to handle cloud-based image storage to maintain privacy.

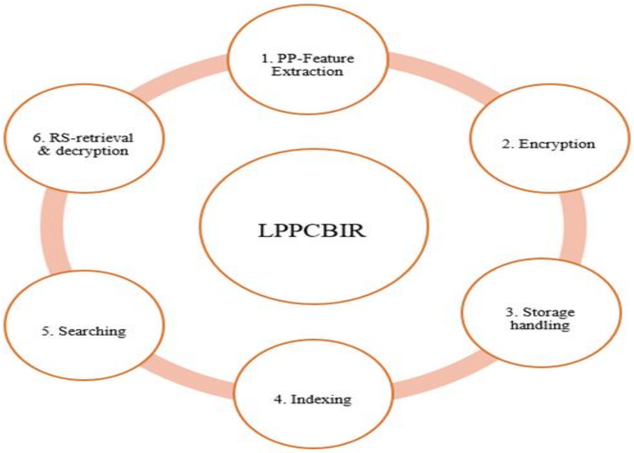

Figure 2: Proposed framework main modules.

The proposed framework mainly includes six different modules, as shown in figure 2:

1. Privacy-Preserving Image feature extraction module
2. Image encryption module
3. Image cloud storage handling module
4. Image indexing at the server-side module
5. Image searching module
6. Image result set retrieval and decryption

After extracting the features from the image, the next step is the encryption process. In this research, we proposed a lightweight and sturdy image encryption mechanism using Elliptic curve cryptography [22]. Elliptic Curve Cryptography (ECC) based algorithms give better security solutions in comparison to other algorithms such as Public Key Cryptography (PKC) algorithms due to small key sizes and efficient computations [23]. To encrypt an image, the encryption process is applied to each pixel of the encrypted image; however, with recent high-resolution images which composed of a massive number of pixels, the encryption process requires higher computation power. In our situation, encryption and decryption are performed at the client-side, where it is limited in resources.

ECC is applied at a group of pixels to minimize the computation overhead and introduce a lightweight and reliable encryption mechanism. Pixels are grouped depending on the parameters used in ECC to minimize the computation overhead. The length size used for ECC encryption is 256, which is equivalent to 3072 key size of the RSA encryption mechanism. The encryption process is performed by the following steps, as shown in figure 3.

1. Extract the pixels information of the required image
2. Group the extracted pixels
3. A key generation where the public and the private key is generated depending on the security parameters of ECC.
4. Pixels groups encryption using the generated public key

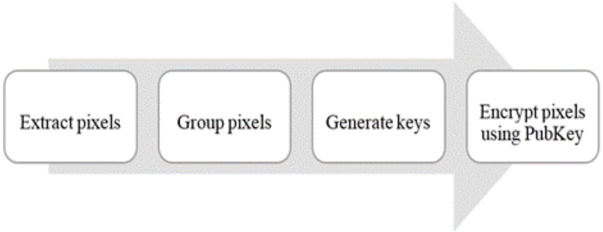

Figure 3: Image encryption process

In this phase the image is converted into a matrix of the image size for example 512 x 512 pixels image after extracting the pixels information of the required image, then group the extracted pixels, the matrix generated in the first phase is then divided based on the size of the ECC encryption key. Dividing the image pixels instead of encrypting every single pixel reduces the encryption cost significantly [24].

3.1 Key Generation Where the Public and The Private Key is Generated Depending on the Security Parameters of ECC

The beginning of this phase includes generating public and private keys for the encryption process at the Private Key Generator (PKG) [25]. PKG implements the elliptic curve equation before encryption where $Y^2 = x^3 + a_1 x + a_2\ over\ Z_p$ is the finite field group. The values of both a1, a2 belong to Z_p is selected by PKG side to meet the equation of $4a_1^{\ 3} + 27a_2^{\ 2} \neq 0$. Suppose that the Generation Point G is the elliptic curve base point with a prime order of n where n > 2160 and Y be the point at infinity such that n×G = Y. The PKG then selects a random number K_v as its private key. K_p is the public key of the client where

$$K_p = K_v \text{ x } G.$$

In this approach a 256-bit encryption key is selected which can provide ECC encryption level up to 3072 bit of RSA encryption. As shown in figure 4, the encryption key of each client is retrieved from a key generator, which is consider as a third party. As shown in the figure below, client device sends his id to the private key generator key. ID is sent encrypted using the public key of PKG.

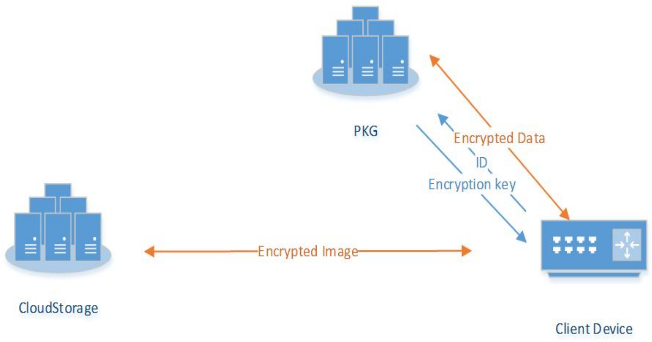

Figure 4: Image ECC-based encryption approach

The client sends it unique identification number (ID) to the PKG. when that unique ID is received by PKG, it then generates a unique number and store it in a local table mapping it to the client ID for future use. This unique number (X_n) is used to generate a unique password (P_n) for this client which is stored. Where

$$P_n = H(K_v \oplus X_n \oplus ID) \qquad (1)$$

Generated password (P_n) is stored as an ECC point($P_n^{\ c}$) using ECC generation point G where

$$P_n^{\ c} = P_n\ x\ G \qquad (2)$$

Generated password ($P_n^{\ c}$) and is then sent to client.

When the client receive password sent by the PKG, it generates a random number R and use this random number to calculate the two parameters S_1 and S_2 using the following equations:

$$S_1 = R\ x\ G \qquad (3)$$

$$S_2 = H(R\ x\ P_n^{\ c}) \qquad (4)$$

After calculating these two parameters client send it with device unique ID to the PKG for client authentication and encryption key generation.

When the PKG receives S_1, S_2 and ID from the client which asks for authentication it recalculate the password for this client P_n using the previously generated random number (X_n) and the device ID using equation 1. Then its password is authenticated using the following equation where the value of S_2 is retrieved using both S_1 and P_n.

$$S_2 = H\ (S_1\ x\ P_n) \qquad (5)$$

If calculated value of S_2 equals the sent value of S_2 then the client is authenticated. When client is authenticated an encrypted key is agreed between client and PKG to encrypt images. Encryption key can is calculated based on the following equation:

$$E_{key} = H\ (P_n^{\ c} | S_2 | ID) \qquad (6)$$

4. EXPERIMENTAL RESULTS

To investigate the performance of the proposed image encryption approach, it was compared with an enhanced Image Encryption Technique using DES algorithm with Random Image overlapping and random key Generation is proposed in [21]. The proposed approach is implemented using Python programming language, where it provides a wide range of encryption libraries, which can be used efficiently to implement the proposed approach.

Implementation is conducted using python on i7 CPU 2.20GHz HP laptop with 16 GB RAM, which installed on Ubuntu 18.04. To implement ECC encryption, py-seccure [26] which a Simple Elliptic Curve Cryptography for Python compatible with the excellent SECCURE command-line utility is used.

To evaluate the performance of our proposed image encryption method, BraTS database is the simulation dataset from Multimodal Brain Tumor Segmentation [27]. BraTS datasets involve multi-contrast MRI images for thirty glioma conditions, including active tumor and edema expert annotations. These images datasets can be viewed MIPAV [28] and can be exported to BMP extension. Twenty images have been selected randomly from that data set, figure 5 demonstrates a collection of images that are used in the simulation.

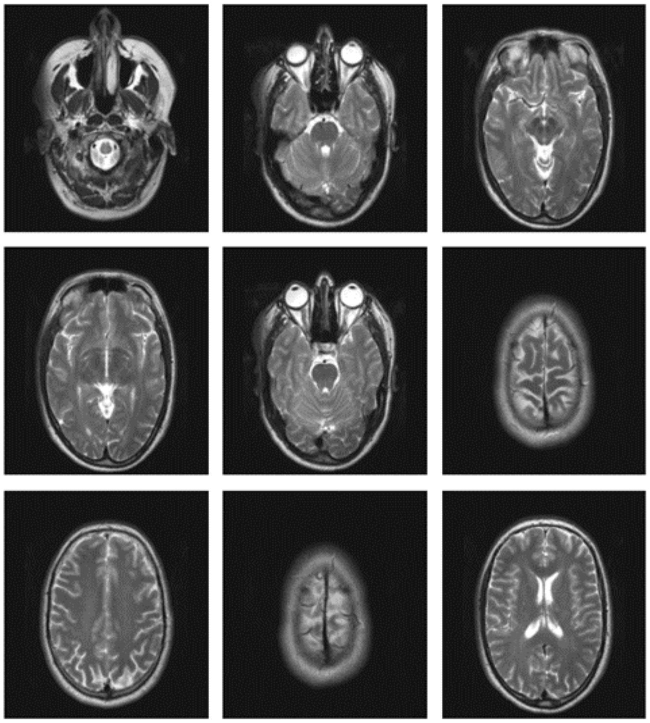

Figure 5: Sample of simulation images

To evaluate the performance of the proposed approach against DES-encryption based approach, two different evaluation metrics have been used. Processing time and encrypted image size. The image process represents the whole time required to encrypt the image; on the other hand, encrypted image size is the size of the image after being encrypted.

4.1 DES Based Encryption

The encrypted image using DES approach does not change where it was the same as the original BMP image. On the other hand, the processing time is ranged between 25 to 27 seconds based on the details of the image, as shown in figure 6**Error! Reference source not found.**.

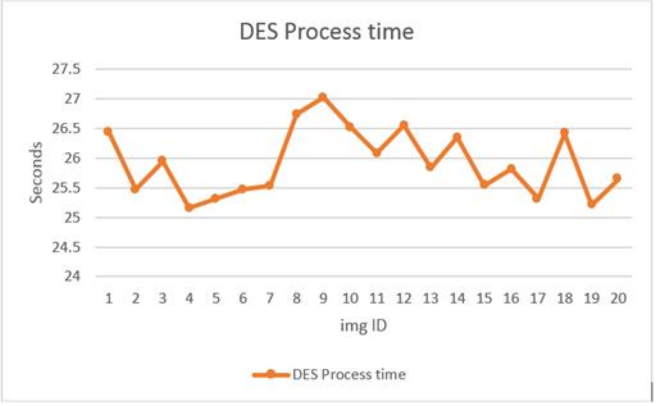

Figure 6: DES encryption approach processing time

4.2 ECC Based Encryption

On the other hand, the ECC encryption time is much less than the processing time of DES encryption, as shown in figure 7, the encryption time of ECC approach is between 0.01 and 0.014 seconds while the encryption is much more complicated.

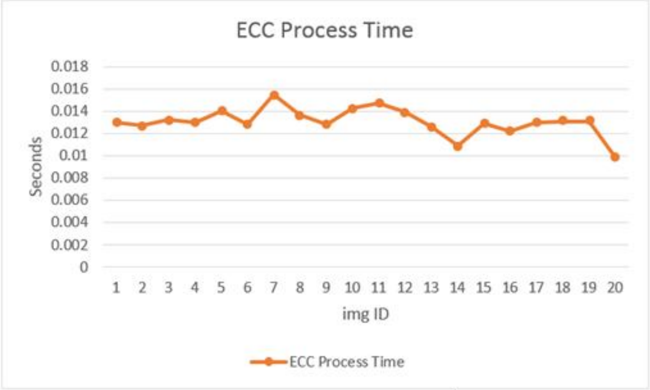

Figure 7: ECC encryption time processing time

The size of the compressed and encrypted image using the ECC-based approach has significantly decreased the image size; the size of the image ratio has decreased to 72% of its initial size, as shown in figure 8. That demonstrates that the proposed mechanism can fit with the requirement of cloud-based storage where the image size is decreased while encoded using a highly secure algorithm.

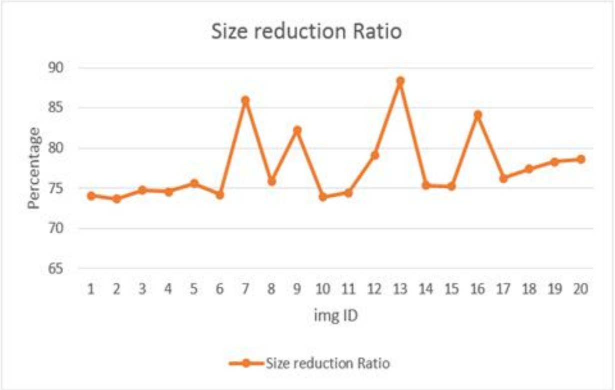

Figure 8: image size decreasing ratio using ECC based compression and encoding approach.

4.3 The Histogram Security Analysis of ECC Approach

The process of security analysis of an image cryptographic processing is a critical issue to ensure the strength of the cryptographic approach. In this section, we discuss the histogram analysis of the implemented approach. The image Histogram demonstrates the frequency of each pixel, which indicates the content of that image. A good cipher image has a uniform frequency distribution of the pixel values. Figure 9 shows the histogram of three images of the simulation image group in two different states: plain image and cipher image respectively. As demonstrated, the plain image frequency distribution of pixels varies a lot representing the content of the image; however, the cipher image histogram is represented by straight line with no varies, which proves that the generated cipher image is ultimately unresolvable and has no indication.

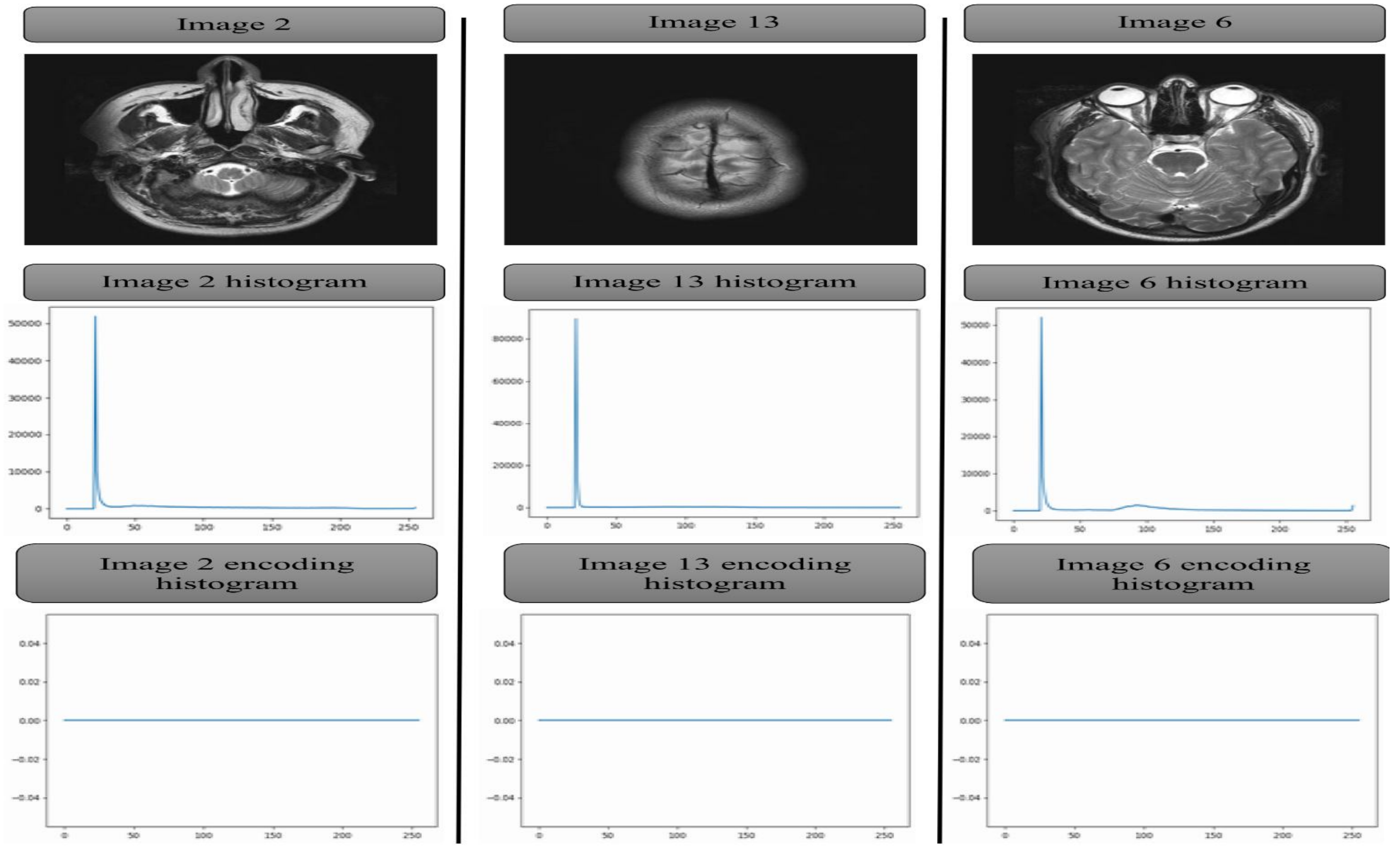

Figure 9: Histogram analysis of ECC based approach

5. CONCLUSION

In this paper, the implementation process of an ECC based encryption and processing approach is presenting. The proposed approach is one of the core modules of a privacy-preserving approach for storing the medical image in the cloud. The proposed approach is implemented by using ECC cryptography mechanism with pixels grouping mechanism. The proposed approach generates a highly secure and encrypted image with reduced image size for cloud storing. The proposed approach has been compared with recently proposed approaches. Results show that the proposed approach performs faster, where lower processing time is required. The histogram security analysis illustrates the power of the encryption where the histogram of the encrypted message provides zero details.

REFERENCES

1. B.P. Santosh Kumar and K. Venkata Ramanaiah, *Effective ROI Extraction Methods for Hybrid Medical Image Compression.* International Journal of Advanced Trends in Computer Science and Engineering, 2019. **8**(2): p. 8. https://doi.org/10.30534/ijatcse/2019/29822019
2. Townsend, D.W. and T. Beyer, *A combined PET/CT scanner: the path to true image fusion.* The British journal of radiology, 2002. **75**(suppl_9): p. S24-S30.
3. Judenhofer, M.S., et al., *PET/MR images acquired with a compact MR-compatible PET detector in a 7-T magnet.* Radiology, 2007. **244**(3): p. 807-814. https://doi.org/10.1148/radiol.2443061756
4. Liu, G.-H. and J.-Y. Yang, *Content-based image retrieval using color difference histogram.* Pattern recognition, 2013. **46**(1): p. 188-198.
5. Yadav, N. and C. Poellabauer. *An architecture for personalized health information retrieval*. in *Proceedings of the 2012 international workshop on Smart health and wellbeing*. 2012. ACM. https://doi.org/10.1145/2389707.2389716
6. Cao, J., et al., *SAIL: Summation-based incremental learning for information-theoretic text clustering.* IEEE Transactions on Cybernetics, 2013. **43**(2): p. 570-584.
7. Anbarasi, M., et al. *Medical image retrieval from distributed environment*. in *Intelligent Agent & Multi-Agent Systems, 2009. IAMA 2009. International Conference on*. 2009. IEEE.
8. Satish, B., *A Methodical Study of Content Based Medical Image Retrieval in Current Days.* Global Journal of Computer Science and Technology, 2016.

9. Aisen, A.M., et al., *Automated storage and retrieval of thin-section CT images to assist diagnosis: system description and preliminary assessment.* Radiology, 2003. **228**(1): p. 265-270.
10. Biswas R. and S. Roy, *Content Based CT Image Sign Retrieval using Fast Discrete Curvelet Transform and Deep Learning.* International Journal of Advanced Trends in Computer Science and Engineering, 2019. **8**(3): p. 854-863. https://doi.org/10.30534/ijatcse/2019/80832019
11. Napel, S.A., et al., *Automated retrieval of CT images of liver lesions on the basis of image similarity: method and preliminary results.* Radiology, 2010. **256**(1): p. 243-252.
12. Müller, H., et al., *Benefits of content-based visual data access in radiology*. Radiographics, 2005. **25**(3): p. 849-858.
13. Shini, S.G., T. Thomas, and K. Chithraranjan, *Cloud Based Medical Image Exchange-Security Challenges.* Procedia Engineering, 2012. **38**: p. 3454-3461. https://doi.org/10.1016/j.proeng.2012.06.399
14. Han, W., Y. Xu, and J. Gong. *A Secure JPEG Image Retrieval Method in Cloud Environment*. in *International Conference on Cloud Computing and Security*. 2016. Springer.
15. Wang, Y., et al., *Towards efficient privacy-preserving encrypted image search in cloud computing.* Soft Computing, 2019. **23**(6): p. 2101-2112.
16. Jayanthi, R. and K.J. Singh, *Image encryption techniques for data transmission in networks: a survey*. International Journal of Advanced Intelligence Paradigms, 2019. **12**(1-2): p. 178-191.
17. Zhang, Y.-Q. and X.-Y. Wang, *A new image encryption algorithm based on non-adjacent coupled map lattices.* Applied Soft Computing, 2015. **26**: p. 10-20. https://doi.org/10.1016/j.asoc.2014.09.039
18. Murillo-Escobar, M., et al., *A RGB image encryption algorithm based on total plain image characteristics and chaos.* Signal Processing, 2015. **109**: p. 119-131.
19. Ye, G. and X. Huang, *An efficient symmetric image encryption algorithm based on an intertwining logistic map.* Neurocomputing, 2017. **251**: p. 45-53.
20. Hua, Z. and Y. Zhou, *Image encryption using 2D Logistic-adjusted-Sine map.* Information Sciences, 2016. **339**: p. 237-253.
21. Shivhare, R., R. Shrivastava, and C. Gupta. *An Enhanced Image Encryption Technique using DES Algorithm with Random Image overlapping and Random key Generation*. in *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*. 2018. IEEE.
22. Anoop, M., *Elliptic curve cryptography.* An Implementation Guide, 2007.
23. Marzouqi, H., M. Al-Qutayri, and K. Salah, *Review of Elliptic Curve Cryptography processor designs.* Microprocessors and Microsystems, 2015. **39**(2): p. 97-112. https://doi.org/10.1016/j.micpro.2015.02.003
24. Murugan, C.A. and P. KarthigaiKumar, *Survey on image encryption schemes, bio cryptography and efficient encryption algorithms.* Mobile Networks and Applications, 2018: p. 1-6.
25. Hankerson, D. and A. Menezes, *Elliptic curve cryptography*. 2011: Springer. https://doi.org/10.1007/978-1-4419-5906-5_245
26. *SECCURE compatible Elliptic Curve cryptography*. 2020; Available from: https://pypi.org/project/seccure/.
27. *Multimodal Brain Tumor Segmentation* 2015; Available from: http://www2.imm.dtu.dk/projects/BRATS2012/data.html.
28. *Medical Image Processing, Analysis, and Visualization*. 2015; Available from: http://mipav.cit.nih.gov/.