Facial Image Encryption Using Enhanced Xor Operation for Secured Transimssion on Cloud Storage

Pranali Dahiwal[1], Anagha Kulkarni[2]

[1] *Research Scholar, Vishwakarma Institute of Information Technology, S.P.Pune University*

[2] *Cummins College of Engineering for Women, Pune, India*

Abstract:- The study highlights the significance of security and privacy in image transmission over cloud platforms, especially considering the sensitive nature of personal information involved in facial image recognition. To address this concern, the study proposes the use of image encryption, with a focus on optimising transmission time, which is crucial for real-time facial image identification and authentication. Initially, the author segmented the images into smaller parts, with segment sizes of 3x1, 3x2, and 3x3. This segmentation facilitates efficient processing and transmission and post that the proposed study uses the XOR encryption technique for encrypting images. XOR encryption is chosen for its simplicity and computational efficiency. An experiment was conducted to evaluate the proposed method. Overall, the study contributes to the field of secure image transmission over cloud platforms, particularly in the context of facial image recognition. By leveraging XOR encryption and optimizing segmentation techniques, the proposed method offers a promising solution for ensuring both security and efficiency in image transmission processes.

Keywords*:* AWS, Cloud, Image Encryption, XOR, Segmentation, Time Complexity.

1. Introduction

Biometric authentication systems, including face recognition, offer several advantages over conventional password-based systems. Firstly, biometric traits are unique to each individual, making them difficult to forge or replicate. This uniqueness enhances security as it mitigates the risk of unauthorized access due to stolen or guessed passwords [1][2]. Additionally, since biometric traits are inherent to individuals, there is no need to remember or manage passwords, which can be forgotten, shared, or stolen.

Furthermore, the registration process in biometric systems involves capturing and storing biometric data, which acts as a barrier against false authentication attempts[3]. This registration step helps ensure that only authorized individuals can access the system, enhancing security.

However, biometric authentication systems also have limitations, with one of the most significant being their susceptibility to spoofing attacks. Spoofing attacks involve presenting false biometric information to the system to gain unauthorized access[4]. Synthesis, where attackers fabricate biometric data, is one form of spoofing attack[5]. Additionally, replay attacks, where captured biometric data is replayed to the system, can also be considered spoofing attacks[6][7].

In a public cloud-based facial authentication system, the vulnerability to spoofing attacks is heightened due to the remote nature of the system and the potential lack of physical security measures. Attackers may attempt to intercept or manipulate biometric data as it is transmitted over the internet, increasing the risk of successful spoofing attacks.

To mitigate the vulnerability to spoofing attacks in public cloud-based facial authentication systems, it is crucial to implement robust security measures such as encryption of biometric data during transmission, multi-factor authentication, continuous monitoring for suspicious activity, and regular updates to security protocols. Additionally, incorporating liveness detection techniques, which verify that

the biometric sample is from a live person and not a static or synthetic representation, can help enhance the resilience of the system against spoofing attacks.

The paper proposes a novel method for enhancing the security and efficiency of face recognition systems deployed on public cloud platforms like Amazon Web Services (AWS). The proposed methodology integrates image encryption techniques with the recognition process to protect against spoofing attacks on facial images used for authentication.

Here's a breakdown of the proposed methodology:

Image Encryption: Pre-processed facial images are encrypted using various encryption algorithms, with XOR encryption being highlighted. XOR encryption is applied to the segmented grid of the image. This encryption process aims to protect the facial features extracted from the images, making it difficult for attackers to manipulate or spoof the images.

Segmentation Approach: The facial images are divided into segmented grids (e.g., 3x1, 3x2, 3x3) before encryption. This segmentation approach helps in enhancing the security and integrity of the encrypted images. It ensures that even if a portion of the image is compromised, the entire image remains protected, thereby reducing the risk of successful spoofing attacks.

Integration with Recognition Process: The encrypted facial images are then used in the recognition process. During authentication, the classifier needs to correctly identify and decrypt the submitted input using the appropriate encryption grid and techniques. This integration ensures that only legitimate users with access to the correct encryption keys can gain authentication.

Time Complexity Analysis: The paper evaluates the time complexity of the encryption and decryption processes. It demonstrates that the proposed method incurs minimal overhead in terms of processing time, ensuring that the authentication process remains efficient even with the added encryption layers.

The main contribution of the paper lies in its innovative approach to image authentication, which leverages segmentation and advanced encryption techniques specifically tailored for cloud platforms. By integrating encryption directly into the recognition process, the proposed methodology aims to enhance the security of facial authentication systems against spoofing attacks while maintaining low-time complexity for encryption and decryption operations.

Overall, this paper presents a promising avenue for improving the security of face recognition systems deployed on public cloud platforms, addressing the critical need for robust authentication mechanisms in cloud-based environments.

The outline of our paper is arranged as follows: Section 2 contains the literature review. Section 3 focuses on the methodologies used in the proposed work. We detail the results of our proposed system in Section 4. Finally, Section 5 refers to the conclusion of the paper.

2. Related Work

In the security system of digital information, especially on cloud platforms, encryption technology is a very common technique and method. Encryption technology can be used to encrypt the original data. If the security and reliability of the encryption method are high enough, then the security of digital information can be protected[8][9][10][11]. Therefore, research on digital image encryption technology and methods is an important direction for digital image security protection.

According to M. T. Elkandoz et.al., an image encryption scheme was proposed. The proposed scheme is based on chaotic maps. The chaotic maps used in this scheme are the Arnold map, the 2D logistic sine map, and the congruential generator. The algorithm starts by shuffling the image pixels using the Arnold map. Then, the 2D logistic sine map and congruential generator were used to generate a 256-bit key. The shuffled image data is then

XORed with the 256-bit key generated from the sine map and congruential generator to produce the final encrypted image. The proposed algorithm's performance is comparable to the counterpart schemes described in the literature[12].

I. Younas and M. Khan proposed a scheme that is based on simplicity. They followed Shannon’s rules of confusion and diffusion in the simplest and easiest possible way. The simplicity of the algorithm comes from the use of two simple boolean operations. However, its strength comes from using large keys during encryption. These two boolean operations are the XOR operation and the rotation operation. They perform these two operations on the pixels of an image, starting with a sequential XORing operation on all of the bit pixels of the image, followed by a circular clock-wise rotation of the bits. These two operations are repeated iteratively until the final encrypted image is achieved. The security of the proposed method has been evaluated using three measures: key space analysis, key sensitivity analysis, and statistical analysis. The results show that the proposed method is an effective encryption method that can be applied in different fields of image encryption[13].

S. Kanwal et.al in the their studies proposed a new technique for the development of an s-box. The modified s-box is based on a multiplicative group of nonzero elements of the Galois field of order 256. The proposed technique uses exponential and Tinkerbell chaotic maps to transform a plain image into a ciphered one. Multiple tests were performed on the proposed method, such as MSE and PSNR. The MSE value of the proposed technique is 8053, and the PSNR value is 9.3214. The results of this paper show that the proposed s-box construction mechanism is efficient and provides secure, real-time communications[14].

A novel approach to encrypting digital images is proposed by F. Khan et.al. The proposed scheme is based on matrix reordering (MR), which is a scanning operation, and XOR operations. Firstly, the MR is used to perform permutations on the bit pixels of the image. Then, a scan pattern is obtained from the MR, which describes how the bit pixels will be rearranged. Secondly, the linear congruential generator is used to generate the pseudorandom bit stream that will be used in the XOR operation. Finally, the rearranged bit pixels of an image are XORed with the bit stream generated from the linear congruential generator to generate the final encrypted image. The proposed scheme was evaluated using a histogram, correlation, cut test, dispersion test, visual testing, and speed test. The results show that the correlation value is close to zero, which means that the relationship between the original image and the encrypted image is very low. The cut test, dispersion test, and speed test show that the proposed scheme can be used in real-time applications. To conclude, the proposed scheme has proven to be resistant to statistical and differential attacks and can be used in real-time applications[15].

A new technique of image encryption is proposed by the A. Sinha and K. Singh. This technique was composed of two main parts, which were encoding and digital signature. This proposed scheme starts by encoding an image, the encoding is using Bose-Chaudhuri Hochquenghem (BCH), and then the digital signature of the original image was added to the encoded version of the image. The added digital signature can be used to verify the authenticity of the image. This proposed scheme provides three layers of security. Firstly, an error control code was used in encoding the original image, which was very difficult to break. Secondly, the digital signature was added to the encoded image, which verifies the authenticity of the image. Finally, there was no need to transmit the keys separately. A digital correlation technique can be used to verify the authenticity of the decrypted image. Transmission of digital images over unsecured channels of communication poses a major risk of revealing confidential data to unauthorised people[16].

M. T. Elkandoz and W. Alexan identified that developing an image encryption algorithm using chaotic maps was proven to be most effective because chaotic maps possess some characteristics such as ergodicity and sensitivity to control parameters and initial conditions. The proposed algorithm by the author starts by shuffling the pixels of the plain image to create confusion. Then, the shuffled image was diffused by XORing its pixels with a secret key. This secret key was generated from a combination of different chaotic maps, which were the Arnold cat map, the Bernoulli map, and the Tent map. Multiple metrics have been used to evaluate the performance of the proposed scheme. The results proved that the proposed scheme was able to oppose any type of attack, such as visual, differential, and brute-force attacks. It also shows that the proposed scheme has superior security performance when compared to some of the other image encryption schemes[17].

A. V Diaconu and K. Loukhaoukha proposed an image encryption scheme that was based on Rubik's cube principle. Rubik's cube principle was used to permute the pixels of the original image. The second step of the algorithm uses the XOR operation to create confusion between the original and ciphered images. The odd rows and columns of the image are XORed using a secret key. The same key was rearranged and used for the XORing of the even rows and columns of the image. Various experimental and statistical tests have been performed to evaluate the performance of the proposed scheme[18].

A new three-step image encryption algorithm was introduced by W. Alexan et.al. The first step of the algorithm utilises the Fibonacci sequence, the second step utilises an s-box, and the third step utilises a Tan-Bessel function. Multiple performance evaluation metrics were used to evaluate the performance of the proposed scheme, such as MSE, PSNR, and information entropy[19].

S. H. Kamali et.al. developed a new image encryption scheme that is a modified advanced encryption standard algorithm. The modification made to the AES algorithm was based on shift and row transformations. Shift and row transformations state that if the values of the first row and column were even, the first and fourth rows remain unchanged. Then, each byte in the second and third rows was shifted cyclically to the right. However, if the first and third rows remain unchanged, each byte of the second and fourth rows was shifted to the left. The proposed scheme has a strong performance against statistical attacks due to its complexity. The encryption time of the proposed scheme is 8.565 ms, which shows how fast the algorithm is and how it can be used for real-time encryption[20].

P. Dahiwal and A. Kulkarni proposed the Advanced Encryption Standards (AES) and the XOR technique for secure image encryption. The author proposed utilising the XOR encryption technique to encrypt segmented images. The researchers conducted picture transmission experiments employing 3*1, 3*2, and 3*3 images that were segmented with an encryption method and discovered that the suggested XOR-based image segmentation surpassed the existing AES approach in terms of time complexity[21].

Huixue Jia et.al. categorized image properties using multilayer homomorphic encryption and image data partitioning. A novel partitioning method suggested by the author helps to reduces computer complexity and improves classification accuracy. The author had increased data security and privacy using partitioned image-specific, homomorphic encryption. The proposed compound encryption method leverages homomorphic computing to decrease computational and storage overheads and solve encryption's inherent complexity. Computing efficiency, storage and transmission cost reduction, security, and privacy are better with the proposed solution. This research provides an innovative and effective technique to image feature classification in cloud computing and big data[22].

Yuxi Mi et.al presented an in-depth study of the privacy protection of face images. Based on the observations on model perception and training behaviour, the author presented two methodological advances, pruning low-frequency components and using randomly selected channels, to address the privacy goal of concealing visual information and impeding recovery. The author proposed their findings into a novel privacy-preserving face recognition method, named Partial Face. Extensive experiments demonstrate that Partial Face effectively balances privacy protection goals and recognition accuracy[23].

To address the privacy preservation of facial images on social media, Xin Dong et.al proposed the frequency-restricted identity-agnostic (FRIA) framework to encrypt face images with frequency-restricted and identity-agnostic attacks to address the face privacy leakage problem. FRIA outperforms other state-of-the-art methods in generating more natural encrypted faces while attaining high black-box attack success rates of 96%. In addition, Experiments on real-world black-box commercial API further reveal the potential of FRIA in practice[24].

For the face Recognition Integration Platform (FRIP), Sei Nakanishi et al. examined the reaction time of face recognition engines during authentication using homomorphic encryption. The response time surpasses 3 s with 120 registrants with the current implementation. Maximum cluster size should be under 120. Calculating the Euclidean distance between encrypted face characteristics took up most of the response time for each step. Parallel processing with clustering was also studied to minimize reaction time. Five clusters were needed for parallel processing when the realistic maximum for facial recognition engines was 500. The evaluation showed that homomorphic encryption provided useful insight into FRIP design[25].

Heping Wen et.al. presented a safe picture encryption technique combining chaos-based block permutation and weighted bit planes chain diffusion based on a variant structure of classical permutation-diffusion to address the security issue with image encryption technology. Divide a picture into sub-blocks, block scrambling, block rotation and inversion, negative-positive transformation, and colour component shuffling are consecutively conducted with chaotic plaintext association during the permutation phase. The chain diffusion step used various encryption algorithms for the high and low 4-bit planes based on picture information weight. The method meets confusion, diffusion, and avalanche cryptographic criteria and has outstanding numerical statistical qualities with a vast cryptographic space, according to theoretical and empirical assessments[26].

The author unified the task of anonymization and visual identity information hiding and propose a novel face privacy protection method based on diffusion models, dubbed Diff-Privacy. Specifically, they trained their proposed multi-scale image inversion module (MSI) to obtain a set of SDM format conditional embeddings of the original image. Based on the conditional embeddings, they designed corresponding embedding scheduling strategies and construct different energy functions during the denoising process to achieve anonymization and visual identity information hiding. Extensive experiments have demonstrated the effectiveness of the proposed framework in protecting facial privacy[27].

E. Abusham et.al proposed an image encryption scheme to counter spoofing attacks by integrating it into the pipeline of Linear Discriminant Analysis (LDA) based face recognition. The encryption scheme uses XOR pixels substitution and cellular automata for scrambling. A single key was used to encrypt the training and testing datasets in LDA face recognition system. For added security, the encryption step requires input images of faces to be encrypted with the correct key before the system can recognize the images. An LDA face recognition scheme based on random forest classifiers has achieved 96.25% accuracy on ORL dataset in classifying encrypted test face images. In a test where original test face images were not encrypted with keys used for encrypted feature databases, the proposed system achieved 8.75% accuracy only showing it was capable of resisting spoofing attacks[28].

Majed Alsafyani et al. developed a revolutionary face feature encryption method that integrates image optimization, cryptography, and deep learning (DL) architectures. Managing the initial standards of the 5D conservative chaotic technique using an optical chaotic map improved key security. Facial image encryption and decryption were completed with a secure Crypto General Adversarial neural network and chaotic optical map. One "hidden factor" in the machine learning (ML) encryption approach was the target field. A modernizing network decrypted an image to a unique image. A region-of-interest (ROI) network extracts involved things from encrypted photos to simplify data mining in a private context. The suggested study shows that the recommended implementation improves security without compromising image quality. Experimental findings reveal that the proposed model outperforms existing models in PSNR (92%), RMSE (85%), SSIM (68%), MAP (52%), and encryption speed (88%)[29].

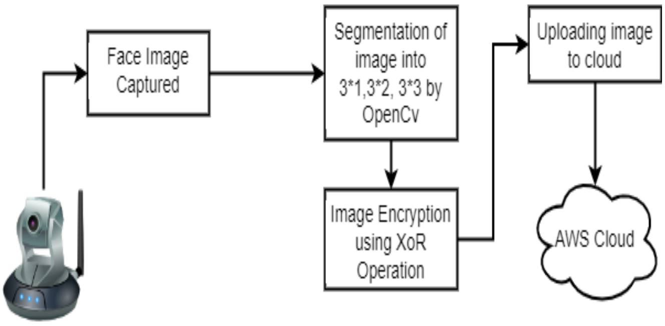
Face Image Captured
Segmentation of image into 3*1,3*2, 3*3 by OpenCv
Uploading image to cloud
Image Encryption using XoR Operation
AWS Cloud

Fig 3.1. System Architecture

P. Y. Chen et.al used blockchain architecture to create a third-party-free information transfer and communication system for unmanned stores. The author employed distributed ledgers and encryption/decryption. Google's Face Net verified retail customers' IDs. Face Net's precision and simplicity make it ideal for unmanned retail identification verification. A face picture library was needed for facial recognition. For encryption and decryption, author had utilized RSA encryption technique. P2P networks broadcasted messages using a directed acyclic graph to avoid endless cycles. The system uses a sidechain as its major endpoint design to benefit from a centralized network while retaining ledger impartiality regulated by lower-authority users to avoid transaction record tampering[30].

Xiao Yang et.al developed a technique that can encrypt the personal photos such that they can protect users from unauthorized face recognition systems but remain visually identical to the original version for human beings. To achieve this, the author(s) proposed a targeted identity-protection iterative method (TIP-IM) to generate adversarial identity masks which can be overlaid on facial images, such that the original identities can be concealed without sacrificing the visual quality. Extensive experiments demonstrated that TIP-IM provides 95%+ protection success rate against various state-of-the-art face recognition models under practical test scenarios. Besides, they also showed the practical and effective applicability of the proposed method on a commercial API service[31].

Luoyin Feng et.al proposed an image recognition and encryption algorithm based on an artificial neural network and multidimensional chaotic sequence. It adopts the combination of high-dimensional chaos and one-dimensional chaos to enhance the security of the key. And, complete the image encryption in the DWT-DCT transform domain and use PCA and BP neural network to achieve face recognition. Then, the key sensitivity, algorithm recognition rate, and robustness of the encryption algorithm were analyzed and tested. Finally, the algorithm recognition rate and robustness of the three encrypted face recognition algorithms and unencrypted face recognition were compared and analyzed. The results show that the recognition rate of the face recognition method using transform domain encryption was not much different from that of the unencrypted face recognition method, and it has good robustness. And, after encryption, the security of face image data on the Internet was greatly improved[32].

3. Methodologies

This section describes the methodologies of image encryption and compression techniques for the face recognition system used in this research work. Figure 3.1 describes the detailed system architecture of image encryption and transmission over cloud system.

The outlined process describes the methodology for image encryption and transmission in the context of a face recognition system, specifically utilizing Amazon Web Services (AWS) for cloud storage. Here's a breakdown of the steps involved:

A. **Face Image Capture:** The process begins with capturing the face image using the camera attached to the user's desktop or laptop. This step involves acquiring the raw image data of the user's face.

B. **Image Segmentation**: The original face image is segmented into different combinations of grids, such as 3x1, 3x2, and 3x3. This segmentation process divides the face image into smaller sections or blocks.

C. **Encryption Technique Application:** Following segmentation, an encryption technique, specifically XOR encryption operations, is applied to each segmented image block. XOR encryption involves applying the XOR operation between the segmented image data and a cryptographic key. This step aims to protect the confidentiality of the facial features by scrambling the pixel values.

D. **Cloud Upload**: Once encrypted, the segmented images are uploaded to the cloud storage service provided by Amazon Web Services (AWS). AWS offers various storage options, such as Amazon S3 (Simple Storage Service), which provide scalable and secure storage for digital assets like images.

E. **Storage and Management:** Within the AWS cloud infrastructure, the encrypted segmented images are stored securely. Access controls and permissions can be applied to restrict access to authorized users or systems, ensuring the confidentiality and integrity of the stored images.

F. **Access and Retrieval**: Authorized users or systems can access the encrypted images stored in the AWS cloud for further processing or recognition tasks. Access to the stored images is governed by authentication mechanisms and access control policies implemented within the AWS environment.

G. **Decryption and Recognition:** When required, the encrypted segmented images can be retrieved from the AWS cloud, decrypted using the appropriate decryption keys, and then processed for face recognition tasks. Decryption reverses the encryption process, allowing the original facial features to be reconstructed and used for recognition purposes.

By following this methodology, the face recognition system can ensure the secure transmission and storage of facial images on the AWS cloud, leveraging encryption techniques to protect sensitive data while facilitating efficient access and retrieval for recognition tasks.

3.1 XOR Encryption and Decryption

The XOR cipher is indeed a simple yet powerful cryptographic method that relies on the bitwise exclusive OR operation. It is commonly used due to its simplicity and computational efficiency. Here are some key principles and characteristics of the XOR cipher:

A. Encryption and Decryption:

a. To encrypt a plaintext message M, the message is XORed with a secret key K to produce the encrypted message E, denoted as $M \oplus K = E$.

b. Similarly, to decrypt the encrypted message E, it is XORed again with the same secret key K, resulting in the original plaintext message M, expressed as $E \oplus K = M$.

c. This makes XOR cipher a symmetric encryption algorithm, where the same key is used for both encryption and decryption, simplifying the implementation.

B. Key Length and Security:

a. If the key is shorter than the message and repeated, the encryption is vulnerable to frequency analysis, where patterns in the plaintext become apparent in the ciphertext.

b. However, if the key is as long as the message and used only once, breaking the encryption becomes impractical due to the sheer number of possible keys (2^N for an N-bit key).

c. Sharing a long key securely can be challenging, but using a pseudo-random number generator (RNG) to produce a stream of keys can mitigate this issue, requiring only the initial seed to be shared.

C. Properties of XOR Operation:

a. $A \oplus 0 = A$: XORing any value with 0 results in the original value.

b. $A \oplus A = 0$: XORing any value with itself results in 0.

c. $(A \oplus B) \oplus C = A$ if and only if $B \oplus C = 0$: XORing A with the result of XORing B and C is equivalent to XORing A with B.

d. $(B \oplus A) \oplus A = B$ if and only if $B \oplus A = B$: XORing B with the result of XORing A and A is equivalent to XORing B with 0, resulting in B.

D. XOR Algorithm:

Algorithm: EncryptMessage (M, K)

Input:

M: Plaintext message

K: Secret key

Output:

E: Encrypted message

```
1.  Initialize E as an empty string
2.  key_length ← length of K
3.  For i from 0 to length of M - 1 do
    a.  plaintext_char ← ASCII value of M[i]
    b.  key_char ← ASCII value of K[i % key_length]
    c.  encrypted_char ← plaintext_char XOR key_char
    d.  Append character representation of encrypted_char to E
4.  Return E
```

4. Results and Discussion

The results were drawn by segmentation of the image into different matrices like 3*1,3*2 and 3*3 which means the image gets segmented into 3,6 & 9 segments. After segmentation, the XOR Encryption algorithms are applied to images for secure transmission over cloud as described in section 3.0

4.1 Experimental Setup:

a) All measurements and experiments are conducted on a single core of an Intel Core i5 CPU running at 2600 MHz, with 8 GB RAM.

b) The experiments are carried out using the NETBEANS 8.2 Integrated Development Environment (IDE), with Java as the programming language. This implies that the encryption and segmentation algorithms are implemented using Java programming language within the NETBEANS environment.

We used the AWS cloud to upload the facial images for encryption using XOR. Our findings are summarized in Tables I for XOR encryption mechanisms.

Table I: XOR Encryption

XOR	Initial Image Size (KB)	Final Image Size (KB)	Execution Time (ms)
3*1	51.3	52.7	4362
3*2	52.8	56.2	5114
3*3	52.4	61.7	5161

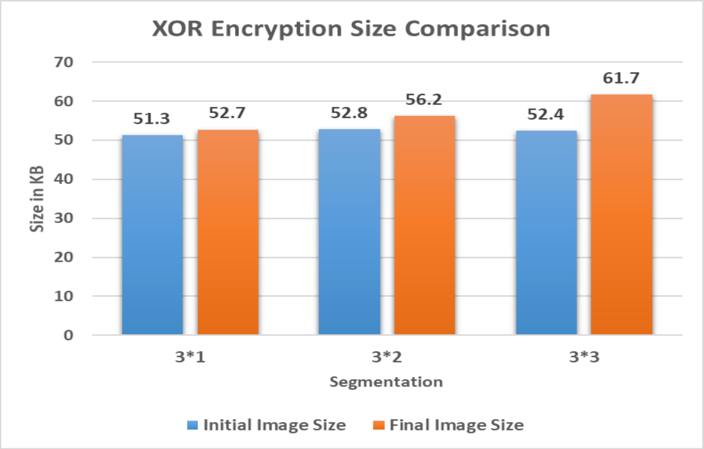

Fig 4.1. XOR Encryption

From analysis of Table I and Figure 4.1, it shows that the original file was encrypted using XOR operations with 3*1,3*2,3*3 Segmentation and the encrypted file size is slightly bigger in size compared to the original size.

Table II: Execution Time

Segmentation	XOR-Execution Time(ms)
3*1	55
3*2	60
3*3	75

In Table II, we show the execution time required for XOR image encryption technique for transmission of 3 segmented images on cloud platform. It is observed that in all 3 segmentation matrices, the XOR image encryption mechanism has less time needed to encrypt the image. In our performance analysis, the most important point is the time complexity for secured image authentication on the cloud, in that regard the XOR encryption considerably faster. Figure 4.2 shows that the XOR image encryption time ranges from just 55 ms to 75 ms for 3*1,3*2 and 3*3 image segmentation technique respectively. The proposed algorithm of XOR with image segmentation has been proven to be way faster and efficient for image transmission.

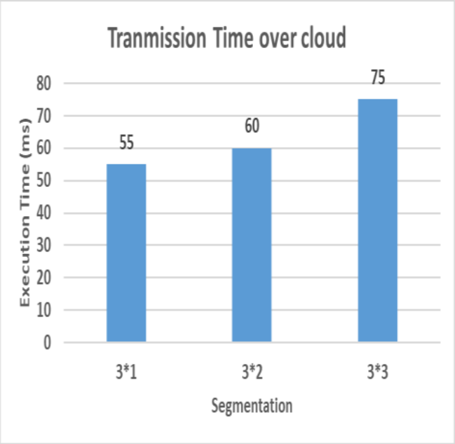

Fig 4.2. Transmission Time over Cloud

5. Conclusion

The research presents efficient methodologies for ensuring secure transmission of images across cloud networks through the use of compression, encryption, and image segmentation algorithms. Specifically, XOR image encryption algorithms are proposed and implemented in the study. The key highlights of the research findings are as follows:

Image Segmentation: The images are initially divided into matrices of sizes 3x1, 3x2, and 3x3. This segmentation approach breaks down the images into smaller parts, facilitating efficient processing and transmission.

XOR Encryption: The XOR encryption algorithm is applied to encrypt the segmented images. This cryptographic technique ensures the confidentiality and integrity of the image data during transmission over the cloud network.

Exceptional Speed: The research findings indicate that the proposed XOR encryption technology, combined with image segmentation, achieves exceptional speed in transmitting data securely via cloud networks. The time taken for encryption falls within the range of 50-65 milliseconds, demonstrating high efficiency.

Implications for Cloud Authentication: The rapid transmission speed of encrypted images suggests potential applications in cloud-based authentication systems. The quick encryption process enables prompt authentication, which is crucial in various industries where facial cognitive authentication techniques are in demand.

Overall, the research contributes to the advancement of secure image transmission methodologies in cloud environments. The combination of image segmentation and XOR encryption offers a practical solution for ensuring data security while maintaining efficient transmission speeds. The findings hold promise for enhancing authentication processes and meeting the needs of industries relying on facial cognitive authentication techniques.

References

[1] X. Wang, Z. Yan, R. Zhang, and P. Zhang, “Attacks and defenses in user authentication systems: A survey,” J. Netw. Comput. Appl., vol. 188, p. 103080, Aug. 2021, doi: 10.1016/J.JNCA.2021.103080.

[2] O. MuhtahirO., A. Adeyinka O., and A. Kayode S., “Fingerprint Biometric Authentication for Enhancing Staff Attendance System,” Int. J. Appl. Inf. Syst., vol. 5, no. 3, pp. 19–24, Feb. 2013, doi: 10.5120/IJAIS12-450867.

[3] B. Zhou, Z. Xie, and F. Ye, “Multi-Modal Face Authentication using Deep Visual and Acoustic Features,” IEEE Int. Conf. Commun., vol. 2019-May, May 2019, doi: 10.1109/ICC.2019.8761776.

[4] D. R. Kisku and R. D. Rakshit, “Face Spoofing and Counter-Spoofing: A Survey of State-of-the-art Algorithms,” Trans. Eng. Comput. Sci., vol. 5, no. 2, pp. 31–31, May 2017, doi: 10.14738/TMLAI.52.3130.

[5] A. Adler and S. A. C. Schuckers, “Biometric Vulnerabilities, Overview,” Encycl. Biometrics, pp. 271–279, 2015, doi: 10.1007/978-1-4899-7488-4_65.

[6] P. Nagarsheth, E. Khoury, K. Patil, and M. Garland, “Replay Attack Detection Using DNN for Channel Discrimination,” Proc. Annu. Conf. Int. Speech Commun. Assoc. INTERSPEECH, vol. 2017-August, pp. 97–101, 2017, doi: 10.21437/INTERSPEECH.2017-1377.

[7] M. Witkowski, S. Kacprzak, P. Zelasko, K. Kowalczyk, and J. Gałka, “Audio Replay Attack Detection Using High-Frequency Features,” Proc. Annu. Conf. Int. Speech Commun. Assoc. INTERSPEECH, vol. 2017-August, pp. 27–31, 2017, doi: 10.21437/INTERSPEECH.2017-776.

[8] R. M. Redlich and M. A. Nemzow, Digital information infrastructure and method for security designated data and with granular data stores: US, US9734169 [P]. 2017.

[9] Z. Han, S. Huang, H. Li, and N. Ren, “Risk assessment of digital library information security: A case study,” Electron. Libr., vol. 34, pp. 471–487, Jun. 2016, doi: 10.1108/EL-09-2014-0158.

[10] C. Zhou, Y. Guo, W. Huang, H. Jiang, B. Li, and J. Chen, “Information security defense method of electric power control system based on digital watermark,” no. Icmemtc, pp. 174–179, 2016, doi: 10.2991/icmemtc-16.2016.32.

[11] E. Chisanga and E. K. Ngassam, “Towards a conceptual framework for information security digital divide,” 2017 IST-Africa Week Conf. IST-Africa 2017, Nov. 2017, doi: 10.23919/ISTAFRICA.2017.8102398.

[12] M. T. Elkandoz, W. Alexan, and H. H. Hussein, “Logistic Sine Map Based Image Encryption,” Signal Process. - Algorithms, Archit. Arrange. Appl. Conf. Proceedings, SPA, vol. 2019-September, pp. 290–295, Sep. 2019, doi: 10.23919/SPA.2019.8936718.

[13] I. Younas and M. Khan, “A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System,” Entropy 2018, Vol. 20, Page 913, vol. 20, no. 12, p. 913, Nov. 2018, doi: 10.3390/E20120913.

[14] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, “Analytic Study of a Novel Color Image Encryption Method Based on the Chaos System and Color Codes,” Complexity, vol. 2021, 2021, doi: 10.1155/2021/5499538.

[15] F. Khan, J. S. Khan, J. Ahmad, and M. Khattak, “A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S8 permutation,” J. Intell. Fuzzy Syst., vol. 33, pp. 1–13, Oct. 2017, doi: 10.3233/JIFS-17656.

[16] A. Sinha and K. Singh, “A technique for image encryption using digital signature,” Opt. Commun., vol. 218, no. 4–6, pp. 229–234, Apr. 2003, doi: 10.1016/S0030-4018(03)01261-6.

[17] M. T. Elkandoz and W. Alexan, “Image encryption based on a combination of multiple chaotic maps,” Multimed. Tools Appl., vol. 81, no. 18, pp. 25497–25518, Jul. 2022, doi: 10.1007/S11042-022-12595-8/METRICS.

[18] A. V Diaconu and K. Loukhaoukha, “An improved secure image encryption algorithm based on Rubik’s cube principle and digital chaotic cipher [J],” Math. Probl. Eng., vol. 2013, 2013, doi: 10.1155/2013/848392.

[19] W. Alexan, M. Elbeltagy, A. Aboshousha, and H. Hussein, Image Encryption Through Fibonacci Sequence, S-Box, and Tan Bessel Function. 2021.

[20] S. H. Kamali, M. Hedayati, R. Shakerian, and M. Rahmani, “A new modified version of Advanced Encryption Standard based algorithm for image encryption,” ICEIE 2010 - 2010 Int. Conf. Electron. Inf. Eng. Proc., vol. 1, 2010, doi: 10.1109/ICEIE.2010.5559902.

[21] P. Dahiwal and A. Kulkarni, “Facial Image Encryption & Compression for Secure Image Transmission on Cloud Storage,” Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 6s, pp. 615–621, Nov. 2023, Accessed: Mar. 08, 2024. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/4000

[22] H. Jia et al., “Efficient and privacy-preserving image classification using homomorphic encryption and chunk-based convolutional neural network,” J. Cloud Comput., vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00537-0.

[23] Y. Mi et al., “Privacy-Preserving Face Recognition Using Random Frequency Components,” Proc. IEEE Int. Conf. Comput. Vis., pp. 19616–19627, 2023, doi: 10.1109/ICCV51070.2023.01802.

[24] X. Dong, R. Wang, S. Liang, A. Liu, and L. Jing, “Face Encryption via Frequency-Restricted Identity-Agnostic Attacks,” MM 2023 - Proc. 31st ACM Int. Conf. Multimed., pp. 579–588, 2023, doi: 10.1145/3581783.3612233.

[25] S. Nakanishi, Y. Narusue, and H. Morikawa, “Response Time of Cloud-Based Facial Recognition System Utilizing Homomorphic Encryption,” IEICE Commun. Express, vol. 12, no. 12, pp. 603–606, 2023, doi: 10.23919/comex.2023col0010.

[26] H. Wen, Y. Lin, S. Kang, X. Zhang, and K. Zou, “Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion,” iScience, vol. 27, no. 1, p. 108610, 2024, doi: 10.1016/j.isci.2023.108610.

[27] D. For, “T Wilight S Hadows on the B Right F Ace P Aul D Ale,” pp. 1–20, 1996.

[28] E. Abusham, B. Ibrahim, K. Zia, and M. Rehman, “Facial Image Encryption for Secure Face Recognition System,” Electron., vol. 12, no. 3, 2023, doi: 10.3390/electronics12030774.

[29] M. Alsafyani, F. Alhomayani, H. Alsuwat, and E. Alsuwat, “Face Image Encryption Based on Feature with Optimization Using Secure Crypto General Adversarial Neural Network and Optical Chaotic Map,” Sensors, vol. 23, no. 3, 2023, doi: 10.3390/s23031415.

[30] P. Y. Chen, Y. C. Cheng, N. S. Pai, and Y. H. Chiang, “Applying Blockchain Technology and Facial Recognition to Unmanned Stores,” Sensors Mater., vol. 35, no. 6, pp. 2081–2100, 2023, doi: 10.18494/SAM4289.

[31] X. Yang et al., “Towards Face Encryption by Generating Adversarial Identity Masks,” Proc. IEEE Int. Conf. Comput. Vis., pp. 3877–3887, 2021, doi: 10.1109/ICCV48922.2021.00387.

[32] L. Feng and X. Chen, “Image Recognition and Encryption Algorithm Based on Artificial Neural Network and Multidimensional Chaotic Sequence,” Comput. Intell. Neurosci., vol. 2022, 2022, doi: 10.1155/2022/9576184