

A Novel Facial Encryption System for Social Media

Xin Liu

University of Science and Technology Beijing, Haidian District, Beijing, 100083,
China

U202341641@xs.ustb.edu.cn

Abstract. In modern society, the importance of facial encryption technology has become increasingly evident. However, existing encryption techniques generally suffer from a significant issue: excessive encryption levels create too much noise, which not only attracts the attention of hackers but may also impair the judgment of facial movements. To address this issue, this paper proposes a detail encryption system which contains two parts: (1) facial detection based on the Viola–Jones object detection framework, and (2) AES-supported detail encryption. The facial detection part aims at localizing the facial features which are appropriately encrypted. Experimental comparisons show that the face images processed by the detail encryption technique obscure distinct facial features. This finding indicates that while the detail encryption technique significantly reduces facial recognizability, it does not overly impair the perception of facial movements.

Keywords: Image encryption, Data security, Social media, Face recognition.

1. Introduction

With the rapid development and widespread adoption of internet technology, information security has become an increasingly prominent issue and a critical challenge that demands urgent attention in modern society. While the internet's widespread use has significantly facilitated people's lives and work—making information access, communication, and dissemination unprecedentedly convenient and efficient—it has also introduced unprecedented information security risks [1-2]. The necessity for robust measures to secure visual information is evident. First, the proliferation of the internet has greatly increased the exposure of personal information. Users engage in various online activities, such as shopping, socializing, and entertainment, which require them to provide extensive personal information. If this information falls into the hands of malicious actors, it could be used for identity theft, online fraud, or aggressive marketing, leading to severe financial losses and psychological distress for users. Secondly, businesses and organizations face significant information security challenges. With the acceleration of digital transformation, more business operations and data have migrated online. However, the complexity and openness of the internet environment make the information systems of enterprises and organizations vulnerable to various forms of cyberattacks, such as hacking, virus transmission, and data breaches. These attacks can result in business disruptions, data loss, legal risks, and severe reputational damage. Furthermore, the widespread adoption of emerging technologies such as the Internet of Things (IoT), cloud computing, and big data has made information security issues more complex and diversified. The extensive use of IoT devices has expanded the attack surface, allowing hackers to exploit these

devices for large-scale cyberattacks. The popularity of cloud computing has made data management and protection more challenging, as businesses and organizations must contend with the security capabilities of cloud service providers and issues such as cross-border data flows. The use of big data technology has further increased the risk of data breaches, as hackers can analyze vast amounts of data to identify system vulnerabilities and weaknesses. The importance of information security is indisputable, as it is vital to protecting personal privacy, safeguarding corporate assets, ensuring national security, and maintaining social order.

However, in today's increasingly digital and visual era, the importance of image security has become even more pronounced. In certain contexts, image security may be even more critical than traditional information security. As a significant carrier of information, images possess unique advantages in information transmission, recording, analysis, and presentation due to their intuitive and vivid nature [3]. Implementing digital image scrambling and grayscale transformation, as well as embedding useful information within images, enables content-based digital image protection and hidden information security for images. However, these advantages come with inherent risks. On one hand, images may contain vast amounts of sensitive information, such as personal identities, geographic locations, and biometric data. On the other hand, images may also become tools for spreading misinformation, misleading the public, and destabilizing social order. Thus, securing images is not only about protecting information but also about maintaining social order and public safety. Compared to traditional textual data, image data presents greater complexity and is harder to tamper with. Once an image is altered or forged, its authenticity is often difficult to verify through simple means. This introduces higher risks in fields where images are crucial, such as courtroom evidence, news reporting, and advertising. Consequently, securing images requires more precise and professional technical methods, such as digital watermarking, image encryption, and blockchain technology, to ensure image integrity and authenticity. Furthermore, with the rapid development of emerging technologies like artificial intelligence and the Internet of Things, the application scope of image data is set to expand, making image security issues more complex and diverse. For example, video images captured by cameras in smart home systems may involve the privacy of household members, and in autonomous vehicles, the accuracy of image recognition technology is directly related to the safety of passengers and pedestrians. Therefore, strengthening image security protection is not only a necessity for technological advancement but also an inevitable requirement for societal progress. To ensure the security of image information, existing image encryption methods are generally divided into two categories: classical encryption methods and modern cryptography-based encryption methods.

2. Literature Review

Classical encryption methods include substitution encryption and transformation encryption [4]. The former involves replacing pixel values or pixel blocks in an image with other values or blocks. For instance, a simple substitution cipher, such as a variant of the Caesar cipher, can be used to alter pixel values. Substitution encryption is a classic technique in which each character or group of characters in plaintext is replaced by another character or group in the ciphertext. In substitution encryption, each letter or symbol in the plaintext alphabet has a corresponding letter or symbol in the ciphertext. The encryption process involves mapping plaintext letters to ciphertext letters according to a certain rule, while the decryption process reverses this mapping. For example, the Caesar cipher [5] is a basic form of substitution encryption that shifts each letter in the alphabet forward or backward by a fixed position. The key to substitution encryption lies in the key itself—that is, the mapping rule—and only individuals who know the key can correctly decrypt the information. The latter method, transformation encryption, alters the position of image pixels using mathematical transformations, such as matrix transformations. For instance, affine transformations or geometric transformations of an image can be employed to achieve encryption.

Encryption methods based on modern cryptography include symmetric key encryption, asymmetric key encryption, and chaotic encryption. The first method uses the same key for both encryption and decryption. Common algorithms include DES and AES. In image encryption, the entire image or pixel

values within the image can be treated as data blocks for encryption. The second method uses a pair of keys—a public key and a private key. The public key encrypts the data, while the private key decrypts it. RSA and ECC (Elliptic Curve Cryptography) are two well-known asymmetric encryption algorithms. Since asymmetric encryption algorithms typically handle smaller data volumes, they are often used to encrypt image keys rather than the entire image. The third method, chaotic system encryption, utilizes the sensitivity of chaotic systems to initial conditions and their seemingly random yet deterministic nature to encrypt images [6]. Chaotic systems are extremely sensitive to initial conditions; even minor changes can produce completely different output sequences, a feature used in cryptography to generate key streams. Although chaotic system behavior appears random, it is actually generated by deterministic dynamic rules, making chaotic sequences difficult to predict. Chaotic encryption plays an irreplaceable role in certain specific application fields, such as lightweight encryption requirements or environments with hardware resource constraints. In such cases, chaotic encryption may provide a unique solution.

Currently, one of the fundamental methods widely discussed and considered highly valuable for in-depth research is the chaos-based encryption method in modern cryptography mentioned above. Chaotic encryption primarily leverages sequences generated by iterative chaotic systems as factor sequences for encryption transformations. The theoretical basis for chaotic encryption is the self-similarity of chaos, meaning that locally selected chaotic key sets are similar in distribution to the whole. Chaotic systems' extreme sensitivity to initial conditions, complex dynamic behavior, and non-compliance with probability statistical principles result in quasi-random sequences. These sequences, characterized by complex structures, provide good randomness, correlation, and complexity, making chaotic systems difficult to reconstruct, analyze, and predict. Chaotic mapping is the core element of chaotic encryption, determining the generation of the encryption sequence. Common chaotic maps include Logistic, Henon, and Lorenz maps. These maps are typically nonlinear and produce complex dynamic behavior, rendering the encryption process unpredictable and difficult to break. By selecting a specific chaotic map and initial conditions, chaotic sequences are generated iteratively. This sequence serves as the key sequence in the encryption process. The generation of chaotic sequences requires sufficient randomness and complexity to withstand various cryptographic attacks. In the encryption process, the data to be encrypted (such as text or images) undergoes a form of operation (e.g., XOR or modular addition) with the generated chaotic sequence, resulting in encrypted data. The encryption process ensures that every part of the data is influenced by the chaotic sequence, achieving effective confusion and diffusion. Decryption is the reverse of encryption. Upon receiving the encrypted data, the recipient generates the same chaotic sequence using identical chaotic mapping and initial conditions. They then apply the inverse operation on the encrypted data with the chaotic sequence to retrieve the original data. Many scholars are also exploring more advanced image encryption methods based on chaotic systems, such as two-dimensional parameter polynomial chaotic systems [7], cascaded chaotic systems [8], and modular chaotic models implemented with FPGA [9].

However, in smart home applications, a significant drawback exists in facial encryption: encrypted facial images often display strong features with excessive noise, making them highly susceptible to hacker attacks. Hackers may analyze these encryption methods to break the encrypted images. Considering the characteristics of chaos-based encryption mentioned above, this paper proposes a chaotic system-based image encryption method. This encryption approach obscures specific facial features without hindering facial recognition or the assessment of facial movements, thus significantly reducing hacker attention. This encryption scheme not only protects user privacy but also meets the image processing and transmission requirements of smart home systems. The face-blurring technique involves two steps. The first step is facial recognition monitoring, which uses the Viola–Jones object detection framework to achieve precise facial localization. The second step is detail encryption [10], which incorporates advanced AES encryption technology. For example, an 8-bit image only has 4 bits encrypted, achieving the dual goals of protecting personal facial privacy and maintaining the ability to interpret facial behavior, which greatly benefits smart home applications.

3. Proposed System

The system proposed in this paper aims to encrypt key facial feature details without transforming the entire face into a noise-like image, creating a clear security enhancement mode. The system consists of two parts: (1) face detection and (2) facial detail encryption, as shown in Figure 1.

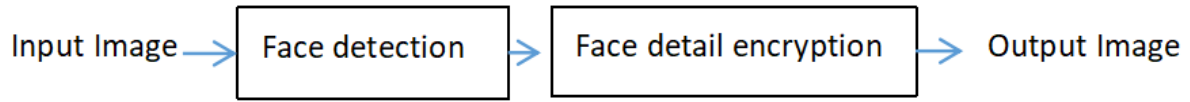


Figure 1. The proposed face encryption system.

3.1. Face Recognition

Detecting and recognizing faces is the foundational step in realizing this concept and is one of the most commonly used basic detection methods in smart homes [11-15]. This detection process primarily uses the Viola–Jones object detection framework, an efficient and accurate face detection algorithm. Below is a detailed analysis of the Viola–Jones framework: The Viola–Jones framework is a machine learning-based approach that achieves real-time face detection by integrating various techniques. Its core idea is to use simple rectangular features (Haar-like features) and an efficient machine learning algorithm (such as AdaBoost) to build classifiers, enabling rapid face detection in images. The detection process is as follows: 1. Preprocessing the Image: Preprocessing the image before face detection can improve detection accuracy and efficiency. Preprocessing steps include grayscale conversion, histogram equalization, normalization, and median filtering, which help eliminate noise and interference in the image. 2. Constructing the Integral Image: By traversing the image once, an integral image is constructed. 3. Sliding Window Detection: Using sliding windows of different sizes and scales, the window slides over the integral image, calculating Haar-like features within each window. These features are simple, computationally efficient, and highly sensitive to edges and lines within the image. 4. Feature Selection and Classification: The AdaBoost algorithm selects the most discriminative features and uses them to build a classifier that categorizes each sliding window. In each iteration, the algorithm dynamically adjusts the training sample weights based on the results of the previous weak classifier. Misclassified samples are given higher weights, while correctly classified samples are given lower weights. This adjustment ensures that the new weak classifier focuses more on difficult-to-classify samples, thereby enhancing overall classification performance. A strong classifier is formed by continuously training and combining these weak classifiers. 5. Cascade Detection: Multiple classifiers are cascaded together for detection. Each classifier is meticulously designed and trained to quickly filter out non-face regions. 6. Post-Processing: In multi-face detection scenarios, multiple overlapping bounding boxes may be detected. Non-Maximum Suppression (NMS) is applied to remove redundant, highly overlapping boxes, retaining the optimal face detection box.



Figure 2. Facial Detection Process.

3.2. Face Detail Encryption

This detail encryption technique is the critical step in this concept.

a. Image Preprocessing: Ensure the image is 8-bit, meaning each pixel's color value is represented by one byte (8 bits), typically ranging from 0 to 255.

b. Selecting Bits to Encrypt: Decide on the 4 bits to encrypt. For example, either the high 4 bits or the low 4 bits of each pixel can be encrypted. If the goal is to make the encrypted image unrecognizable to human observers, encrypting the bits that most affect the visual appearance is advisable. In some cases, encrypting the lower bits can produce more noticeable visual changes since these bits usually influence color details. There are various approaches to selecting bits: fixed bit encryption—always

encrypting the high or low 4 bits of each pixel—or content-based selection, where bits containing the most information are encrypted based on image content analysis.

c. Generating the Key: Generate an encryption key to encrypt the selected 4 bits. The key can be random or algorithmically generated. Initially, a pseudo-random sequence is generated as the initial key using a random number generator. This sequence is then passed through an AES encryptor to produce a more complex key, followed by reading the image data requiring encryption.

d. Encryption Process: For each pixel in the image, perform the following steps: Extract the low or high 4 bits (as previously selected) of the 8-bit pixel value. Encrypt the extracted 4 bits using the key and an encryption algorithm (such as XOR). Replace the encrypted 4 bits back into the original pixel, while the remaining bits remain unchanged. Store or transmit the encrypted image: save the encrypted image as a file or transmit it over a network. 5. Decryption Process: During decryption, use the same key and encryption algorithm to reverse the encrypted 4 bits, restoring the original 4-bit values. Reintegrate the decrypted 4 bits back into each pixel to obtain the decrypted image. To illustrate with a simplified example, suppose we choose to encrypt the low 4 bits of each pixel: Assume the pixel value is 11111111 (8 bits), and this algorithm selects the low 4 bits for encryption. Extract the low 4 bits: 1111. Perform XOR encryption with the key (assumed to be 1010): $1111 \text{ XOR } 1010 = 0101$. Replace the encrypted low 4 bits, 0101, back into the original pixel, resulting in an encrypted pixel value of 11110101.



Figure 3. Detail Encryption Technique Implementation Process.

4. Experimental Result

In this section, some experimental result will be shown to verify the potential and benefits of the proposed method. Also, further discussion about application and challenge will be presented.

4.1. Experiment Result

This experiment cleverly integrates the classic Viola–Jones object detection framework with advanced AES encryption technology, creating a novel image processing method. Within this framework, the algorithm focuses on the precise identification and encryption of localized facial features in the image. For example, consider a local pixel in the image with an original pixel value of 11001110 (8 bits). To protect personal privacy, the algorithm encrypts this portion of the information. The specific operation involves extracting the low 4 bits of the pixel value, which are 1110. Then, using a hypothetical key (1010), the extracted 4 bits undergo an XOR encryption operation. After encryption, the pixel value changes to 11000100. Below is an experiment based on this encryption.

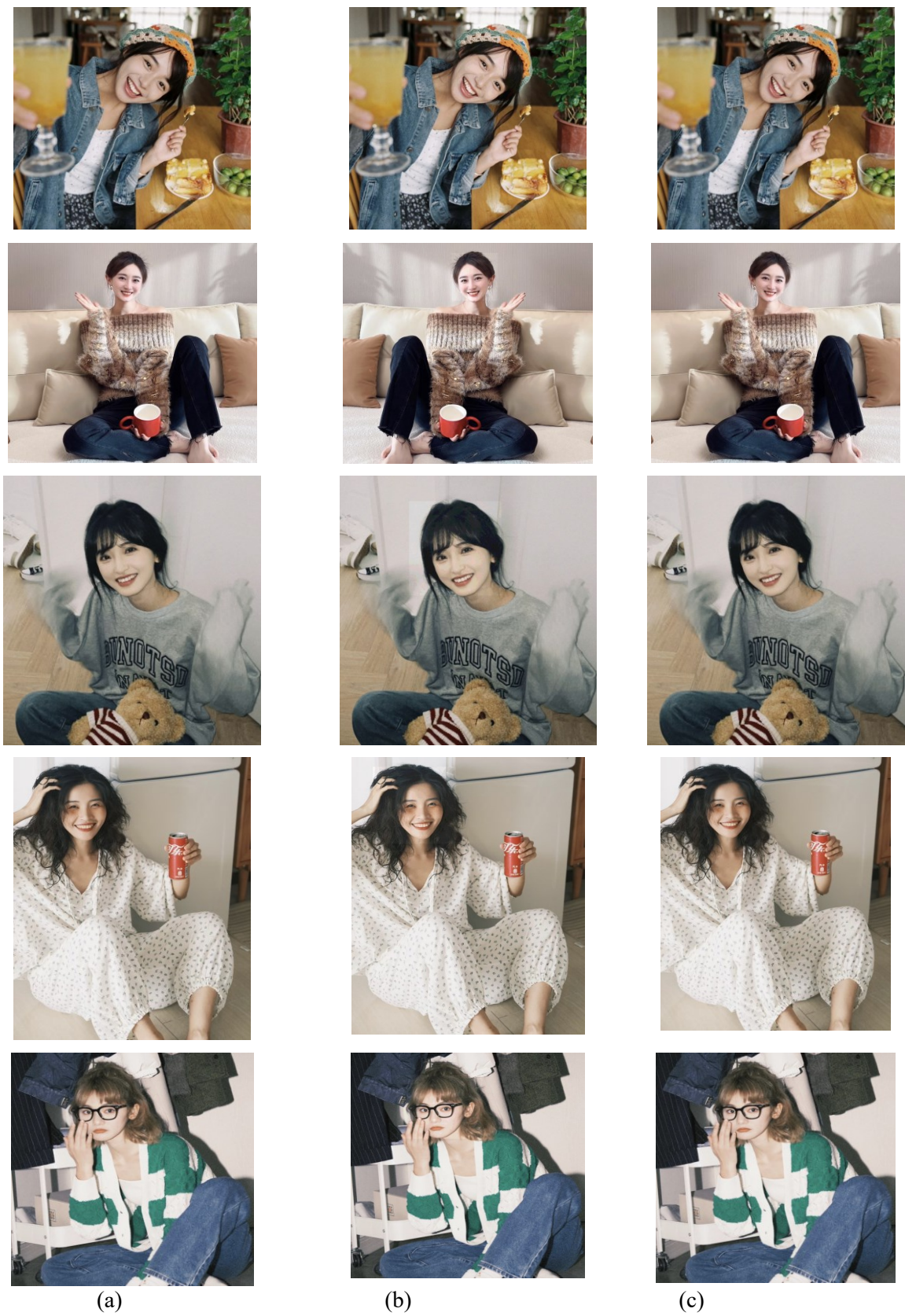


Figure 4. Experimental result: (a) original image; (b) encrypted image; (c) decrypted image.

As shown in Fig. 4, the encryption results of the experiment fully demonstrate the practicality and effectiveness of this method in real-world applications. First, the image is transformed into a grayscale image, and the encrypted pixel value and the scrambled image are combined into a ciphertext image by using the algorithm of chaotic system encryption. It's worth noting that we use an 8-bit, 6-bit encryption method. Through this encryption technique, the algorithm successfully blurs the local facial features of the target, ensuring the security of personal privacy. Notably, this encryption method does not impact the overall image outline or interfere with motion judgment, maintaining a high level of image readability. The experiment results not only present a novel approach to privacy protection but also effectively fulfill the initial design concept of this paper—protecting personal privacy without compromising the image's utility.

4.2. Innovation Point Review

This paper presents an innovative 8-bit 6-bit image encryption method, designed to solve the limitations of traditional solutions, and improve the security and practicality of smart home image data.

A: Reduce the data volume and improve the transmission efficiency

The traditional 8-bit image encryption method produces the same amount of data as the plaintext images, which leads to inefficient data transmission, especially when the network bandwidth is limited. The present scheme reduces the 8-bit image to 6 bits, thus significantly reducing the amount of data. For example, for an 8-bit grayscale image with a resolution of 640x480, the amount of data is 307,200 bytes. With the 6-bit encryption scheme, the amount of data is only 230,400 bytes, down by 25 percent. This can not only improve data transmission efficiency, but also reduce storage costs.

B: Enhance security

Traditional 8-bit image encryption methods usually use symmetric encryption algorithms, such as AES, DES, etc. However, the security of these algorithms depends on the confidentiality of the keys, and once the key is leaked, the entire encryption system will face great risks.

This scheme uses a nonlinear encryption algorithm based on chaos theory to map the 8-bit images to a 6-bit cipher space. The algorithm has the following advantages:

Large key space: The 6-bit ciphertext space has 64 possible combinations, far more than the 256 combinations of the 8-bit images, which makes violent cracking more difficult.

High key sensitivity: a chaotic system is very sensitive to the initial conditions, and even small changes in the key can lead to completely different encryption results.

Strong anti-attack ability: the chaotic system has good randomness and unpredictability, and can effectively resist various attacks, such as differential attack, linear attack, etc.

C: Compatible with the existing smart home systems

The 6-bit ciphertext images generated by this scheme can be seamlessly integrated with the existing smart home systems. For example, 6-bit ciphertext images can be transmitted to the cloud for storage and analysis, or decrypted and displayed on a local device. This scheme proposes an innovative method of 8-bit image encryption and 6-bit encryption, which has the advantages of reducing data volume, improving transmission efficiency, enhancing security, and being compatible with existing systems. And the image content of the face is slightly encrypted, which not only protects the portrait right of the character, but also does not affect the judgment of the character's action, so as not to affect the investigation of a certain situation. This avoids the infringement of others' portrait rights when private individuals install surveillance and call surveillance.

5. Discussion

To meet the demand for encryption technology in the smart home market and reduce the likelihood of hacker attacks, the above-described technique employs and successfully tests an 8-bit pixel encryption method where only 4 bits are encrypted. This approach lowers facial recognizability while reducing interference with the assessment of human actions. Through this precise and appropriate encryption treatment, the algorithm protects user privacy while preserving the normal functionality of smart home systems. Following multiple experiments and image comparisons, the facial images processed by the

detail encryption technique do not clearly reveal individual facial features, making it challenging to identify individuals based solely on the encrypted image. However, one can still deduce the general facial outline and behavior of the person. These results demonstrate that the detail encryption technique reduces facial recognizability without significantly affecting the ability to judge facial actions. Additionally, due to reduced noise, the encrypted areas are less conspicuous, thereby enhancing the overall security of the image.

The detail encryption technique allows users to record the entry and exit of family members while safeguarding the privacy of this information. Moreover, for high-end users seeking enhanced security protection, the detail encryption technique offers a satisfactory solution. In summary, detail encryption technology has achieved not only technical breakthroughs but also demonstrated strong applicability and significant effectiveness in practical applications. As the smart home market continues to grow, detail encryption technology is expected to become an essential tool for protecting user privacy, ensuring the secure operation of smart home systems.

6. Conclusion

In the smart home field, this paper identifies a pressing market need for a technology that can protect user privacy without impeding normal usage. To address this need, this paper introduces an innovative adaptation of existing facial encryption technology, combining face detection supported by the Viola–Jones object detection framework with AES encryption technology to develop the detail encryption technique.

A common issue with current facial encryption technologies is excessive encryption, which produces high levels of image noise. This not only attracts hacker attention but also often hinders the ability to interpret facial movements. To solve this problem, this paper proposes the detail encryption technique, which uses an 8-bit pixel to encrypt 6 bits, reducing facial recognizability while minimizing interference with the judgment of facial actions. The implementation of detail encryption relies on the integration of two key technologies: (1) the Viola–Jones object detection framework, which precisely delineates the facial features that require encryption, and (2) AES encryption, which efficiently encrypts these localized features. Moreover, detail encryption technology has a wide range of applications in the smart home sector. With the growing adoption of smart home systems [15], more households are beginning to use devices with cameras and facial recognition functions, such as smart door locks and security monitoring systems. While these devices offer convenience, they also pose privacy risks. Detail encryption can effectively protect users' facial features, reducing the risk of privacy breaches. Additionally, the increasing rigor of data protection regulations, such as the EU's GDPR and China's Personal Information Protection Law, has set higher standards for the protection of personal and sensitive data. Detail encryption helps smart home systems operate in compliance with these regulations, avoiding legal risks and penalties. Advances in Technology: The continuous development of image processing and encryption technologies has made efficient and secure image encryption feasible. Detail encryption technology is a product of this progress, achieving high-efficiency encryption while maintaining image quality. Different users have varying needs for smart home systems.

References

- [1] Kim, M., Jiang, X., Lauter, K., Ismayilzada, E., & Shams, S. (2022). Secure human action recognition by encrypted neural network inference. *Nature Communications*, 13, 4799.
- [2] Battula, T. K., Neerukattu, H., & Kukkala, A. (2024). DRPE image encryption with watermarking using 2D-FrFT and its invariance property: A fusion-based hybrid approach. In *Proceedings of the 5th International Conference on Image Processing and Capsule Networks (ICIPCN)* (pp. 17-22). Dhulikhel, Nepal. doi: 10.1109/ICIPCN63822.2024.00012.
- [3] Lei, Z., Li, L., & Xianwei, G. (2011). Design and realization of image encryption system based on SMS4 commercial cipher algorithm. In *Proceedings of the 4th International Congress on Image and Signal Processing* (pp. 741-744). Shanghai, China. doi: 10.1109/CISP.2011.6100292.

- [4] Chen, J., Chen, L., & Zhou, Y. (2021). Cryptanalysis of image ciphers with permutation-substitution network and chaos. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(6), 2494-2508. doi: 10.1109/TCSVT.2020.3021908.
- [5] Jain, A., Dedhia, R., & Patil, A. (2015). Enhancing the security of Caesar cipher substitution method using a randomized approach for more secure communication.
- [6] Guan, T., Zhang, D., Tang, S., & Zhang, X. (2023). A chaos-based data encryption method and system (Chinese Patent CN202310930274.X).
- [7] Hua, Z., Chen, Y., Bao, H., & Zhou, Y. (2022). Two-dimensional parametric polynomial chaotic system. *IEEE Transactions on Circuits and Systems I: Regular Papers*.
- [8] Zhou, Y., Hua, Z., Pun, C.-M., & Chen, C. L. P. (2015). Cascade chaotic system with applications. *IEEE Transactions on Circuits and Systems I: Regular Papers*.
- [9] Hua, Z., Zhou, B., & Zhou, Y. (2015). Sine-transform-based chaotic system with FPGA implementation. *IEEE Access*. Keywords: Ciphers, Encryption, Chaos, Kernel, Streaming media, Chosen-ciphertext attack, Permutation substitution, Bit-wise XOR, Image encryption.
- [10] Bedoui, M., Mestiri, H., Bouallegue, B., Hamdi, B., & Machhout, M. (2022). An improvement of both security and reliability for AES implementations.
- [11] Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 511-518. Cambridge, MA: Mitsubishi Electric Research Labs.
- [12] Shetty, A. B., Bhoomika, Deeksha, J., Rebeiro, J., & Ramyashree. (2021). Facial recognition using Haar cascade and LBP classifiers. *Global Transitions Proceedings*, 2(2), 330-335. <https://doi.org/10.1016/j.gltp.2021.08.044>.
- [13] Gašperov, B., & Kostanjčar, Z. (2021). Market making with signals through deep reinforcement learning. *IEEE Access*, 9, 61611-61622. doi: 10.1109/ACCESS.2021.3074782.
- [14] Kim, M., Jiang, X., Lauter, K., et al. (2022). Secure human action recognition by encrypted neural network inference. *Nature Communications*, 13, 4799. <https://doi.org/10.1038/s41467-022-32168-5>
- [15] Saxena, N., & Varshney, D. (2021). Smart home security solutions using facial authentication and speaker recognition through artificial neural networks. *International Journal of Cognitive Computing in Engineering*, 2, 154-164. <https://doi.org/10.1016/j.ijcce.2021.10.001>.