

Review Article

Strengthening Image Archiving: A Reliable Approach

Vinod Choudhary¹, Shreyas Dhavle²

^{1,2}Research Scholar, MCA, Thakur Institute of Management Studies, CareerDevelopment & Research (TIMSCDR), Mumbai, India

I N F O

Corresponding Author:

Shreyas Dhavle, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR), Mumbai, India.

E-mail Id:

shreyashdhavle@gmail.com

Orcid Id:

<https://orcid.org/0009-0004-2457-5447>

How to cite this article:

Choudhary V, Dhavle S. Strengthening Image Archiving: A Reliable Approach. *J Adv Res Image Proc Appl* 2024; 7(1): 16-18.

Date of Submission: 2024-02-23

Date of Acceptance: 2024-03-27

A B S T R A C T

A robust backup system is essential for preserving critical files against unforeseen events. Data security is also crucial for protecting confidential information. Therefore, backup systems must prioritize security measures. Encryption is a popular method for ensuring data confidentiality. This paper presents new computer software that allows users to store and retrieve encrypted image backups in a secure and user-friendly way. People can easily put their pictures into the system and take them out whenever they want. They can also see small preview pictures of the ones they uploaded. When someone adds a picture, the system makes it all secret using a special method called the Advanced Encryption Standard (AES). This secret picture is kept safe in the system's storage. When someone wants to get their picture back, the system automatically un-secrets it, giving a smooth and easy experience for the user.

Keywords— Robust; Advanced Encryption Standard

Introduction

Backing up your image files is essential to protect them from loss or damage. Unexpected events such as system crashes, hardware failures, or natural disasters can strike at any time, and it is important to have a reliable backup plan in place.

In addition to the risk of data loss, image files can also be vulnerable to unauthorized access. To protect your privacy and sensitive information, it is important to encrypt your image backups.

Encrypted image backup software provides a secure and convenient way to protect your image files. This type of software encrypts your images using a strong encryption algorithm, such as AES, before storing them on your computer or in the cloud. This makes it virtually impossible for unauthorized users to access your images, even if they are able to gain access to the backup files themselves.

Encrypted image backup software is easy to use and typically offers a variety of features, such as:

- Automatic backup scheduling
- Support for multiple backup destinations
- Easy file retrieval
- Thumbnail preview of backed-up images
- Password protection

This introduction is longer and more informative than my previous one, but it avoids repeating myself. I have added new information about the benefits of encrypted image backup software, as well as some common features that these software programs offer. I have also tried to make the introduction more engaging and readable by using more active and descriptive language.

Literature Review

Data backup and security systems with encryption are essential for all organizations. They protect data from

loss and unauthorized access, which can have significant financial and reputational consequences.

Traditional backup methods, such as full backups, can be slow and inefficient, especially for large datasets. Newer methods, such as incremental and differential backups, are faster and more efficient because they only back up the data that has changed since the last backup.

Data compression can also save time and space when backing up data. By compressing the data before backing it up, organizations can reduce the size of the backup files, which can make them faster to back up and restore.

Encryption is a critical part of data security. It scrambles data so that it can't be read without the encryption key. This makes it impossible for unauthorized users to access the data, even if they have physical access to the backup files.

Advanced Encryption Standard (AES) is a popular encryption algorithm that is used by many backup systems. Many backup systems offer additional features, such as:

- **Data compression:** This can reduce the size of the backup files, which can make them faster to back up and restore.
- **Hash tables for indexing:** This can improve the performance of the backup system by making it faster to find and restore specific files.
- **Faster access on cloud:** Some backup systems offer the ability to store backups in the cloud, which can provide faster access to the data if it is needed to recover from a disaster.
- **Anti-virus protection:** Some backup systems offer anti-virus protection to help protect the backup data from malware infection.
- **Sharing of files on a network:** Some backup systems allow users to share files on a network, which can be useful for collaboration and disaster recovery.
- **Access to multiple users:** Some backup systems allow multiple users to access the backup data, which can be useful for organizations with multiple users who need to access the data.
- **Data restoration to a previous version:** Some backup systems allow users to restore files to a previous version, which can be useful if a file is accidentally corrupted or deleted.

Organizations should choose a backup system that meets their specific needs. Some factors to consider include the size and complexity of the data environment, the budget, and the specific features that are needed.

Methodology

The Advanced Encryption Standard (AES) algorithm is a symmetric key block cipher that is widely used due to

its mathematical efficiency and security. It encrypts and decrypts data by using the same key.

The method is as follows:

1. The user selects an image to encrypt and uploads it to the system.
2. The system encrypts the image using the AES algorithm and saves the encrypted image file on the user's system.
3. To view the original image, the user logs into the system and downloads the encrypted image file.
4. The system decrypts the encrypted image file and saves the original image file in the user's downloads folder.

The following steps are involved in the encryption process:

1. **Sub Bytes:** This step uses a predefined substitution table (S-Box) to replace each byte in the image with a different byte.
2. **Shift Rows:** This step shifts the rows of the image to the left by a certain number of positions.
3. **Mix Columns:** This step mixes the columns of the image using a predefined mathematical function.
4. **Add Round Key:** This step adds a round key to the image. The round key is generated using the AES algorithm key.

The decryption process is the reverse of an encryption process. The following steps are involved in the decryption process:

1. **Add Round Key:** This step subtracts the round key from the image.
2. **Mix Columns Inverse:** This step mixes the columns of the image using the inverse of the predefined mathematical function used in the encryption process.
3. **Shift Rows Inverse:** This step shifts the rows of the image to the right by a certain number of positions.
4. **Sub Bytes Inverse:** This step replaces each byte in the image with its original value using the inverse of the S-Box used in the encryption process.

The proposed method is effective in encrypting and decrypting images. The encrypted images are secure and cannot be accessed without the AES algorithm key.

Future Work

In this paper, we have introduced a system designed to encrypt image files during the backup upload process and decrypt them upon download, ensuring a secure approach for robust data protection. It's important to highlight that the size of the image file stays the same throughout the encryption process. This ensures data integrity by keeping the original dimensions of the image intact, all while meeting strict security standards. With the continuous growth in the number of files requiring backup, the size of the data becomes increasingly significant.

A widely adopted method for improving security and saving storage space involves compressing and encrypting files. Additionally, integrating a One- Time Password (OTP) verification module can provide an additional layer of user authentication, strengthening the overall security of the system.

Conclusion

In conclusion, this paper has demonstrated the effectiveness of an image backup system and provided insights into the functioning of the AES algorithm. By employing AES, we have achieved the successful encryption and decryption of images. This implies that an image remains secure until a specific process is employed to decrypt it. Hence, the utilization of AES for securing image files has been validated. So, using AES to lock up image files is a good and proven idea. The method proposed in this paper introduces an innovative approach that markedly improves the speed and efficiency of image file encryption. By incorporating advanced techniques, this approach facilitates a quicker and more streamlined encryption process, ultimately optimizing the overall performance of image file security. A notable strength of AES lies in its flexibility regarding key sizes, and its speed and efficiency render it well-suited for real-time image encryption applications. The AES algorithm's use of keys that provide robust encryption, coupled with substitutions and permutations for swift software implementation, makes it a preferred choice for real-time applications due to its versatile implementation options.

References

1. Chervenak A, Vellanki V, Kurmas Z. Protecting file systems: A survey of backup techniques. In Joint NASA and IEEE Mass Storage Conference 1998 Mar 23 (Vol. 99).
2. Nechvatal J, Barker E, Bassham L, Burr W, Dworkin M, Foti J, Roback E. Report on the development of the Advanced Encryption Standard (AES). Journal of research of the National Institute of Standards and Technology. 2001 May;106(3):511.
3. Hafsa A, Sghaier A, Malek J, Machhout M. Image encryption method based on improved ECC and modified AES algorithm. Multimedia Tools and Applications. 2021 May;80:19769-801.
4. Gamido HV, Sison AM, Medina RP. Implementation of modified AES as image encryption scheme. Indonesian Journal of Electrical Engineering and Informatics (IJEI). 2018 Sep 1;6(3):301-8.
5. Sachdev A, Bhansali M. Enhancing cloud computing security using AES algorithm. International Journal of Computer Applications. 2013 Jan 1;67(9).
6. Wankhede IU, Sirsat SR. Securing Cloud Data Storage through Encryption. International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCE). 2015:21.
7. Daniel A, Momoh MO. A computer security system for cloud computing based on encryption technique. Computer Engineering and Applications Journal. 2021 Feb 1;10(1):41-54.
8. Gu Z, Li H, Khan S, Deng L, Du X, Guizani M, Tian Z. IEPSBP: a cost-efficient image encryption algorithm based on parallel chaotic system for green IoT. IEEE Transactions on Green Communications and Networking. 2021 Jul 8;6(1):89-106.
9. Xu J, Zhao C, Mou J. A 3D image encryption algorithm based on the chaotic system and the image segmentation. IEEE Access. 2020 Jun 30;8:145995-6005.