WHAT IS CLAIMED IS:

1. A video file encryption method, comprising:

obtaining a to-be-encrypted video file and an encryption key,

encrypting the video file using the encryption key to obtain an encrypted video file,

obtaining scanned non-hidden partitions of a mobile terminal and an extended memory of the mobile terminal for storing user data,

determining a partition storing the to-be-encrypted video file among the non-hidden partitions, and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file.

2. The method of claim 1, comprising:

scanning the non-hidden partitions of the mobile terminal and the extended memory of the mobile terminal, and

creating a folder in each of the partitions from the scan.

3. The method of claim 1, wherein encrypting the video file using the encryption key to obtain the encrypted video file comprises:

reading header data having a length equal to a first length and stored in a header of the to-be-encrypted video file,

encrypting the header data using the encryption key to obtain ciphertext, and

obtaining the encrypted video file in accordance with the ciphertext and remaining non-header data in the to-be-encrypted video file.

4. The method of claim 3, wherein obtaining the encrypted video file in accordance with the ciphertext and the remaining non-header data in the to-be-encrypted video file comprises:

obtaining a header data storage area in the to-be-encrypted video file,

obtaining, based on the header data storage area, a designated header data storage area having a second length and a ciphertext storage area, the second length less than the first length, the designated header data comprising the storage area for storing the encryption key and an encryption ID,

generating the designated header data while maintaining the remaining non-header data in the to-be-encrypted video file, writing the designated header data and the

encryption key into respective corresponding storage areas to obtain the encrypted video file.

5. The method of claim 4, wherein obtaining, based on the header data storage area, the designating header storage area having the second length comprises:

starting from a start point of the header data in the storage area for the to-be-encrypted video file, obtaining a storage area having the second length for storing data as the designated header data storage area.

6. The method of claim 4, wherein obtaining the ciphertext storage area based on the header data storage area, comprises:

obtaining a length of the ciphertext, and determining whether the length of the ciphertext is greater than a difference between the first length and the second length,

if the length of the ciphertext is less than or equal to the difference, subtracting the designated header storage area from the header area storage area to obtain the ciphertext storage area,

if the length of the ciphertext is greater than the difference, subtracting the header data storage area from the designated header data storage area to obtain a partial ciphertext storage area having a length equal to the difference, obtaining a storage area for the to-be-encrypted video file, starting from the end point of the storage area for the to-be-encrypted video file, obtaining a storage area having a length of a remaining part of the ciphertext to obtain a remaining ciphertext storage area.

7. The method of claim 1, wherein determining a partition storing the to-be-encrypted video file among the non-hidden partitions and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file, comprise:

obtaining inode information associated with the to-be-encrypted video file, the inode information comprising a storage path, the inode information corresponding to video data in the video file,

allocating, in accordance with the storage path associated with the to-be-encrypted video file, one of the partitions for storing the to-be-encrypted video file,

calculating, in accordance with the folder of the partition for storing the to-be-encrypted video file, a storage path associated with the encrypted video file so that the storage path associated with the encrypted video file points to the folder in the partition

for storing the to-be-encrypted video file, obtaining inode information associated with the encrypted video file, and

moving the encrypted video file to the folder of the partition for storing the to-be-encrypted video file by changing the inode information associated with the to-be-encrypted video file to the inode information associated with the encrypted video file.

8. The method of claim 7, comprising:

establishing a correspondence between the inode information associated with the to-be-encrypted video file and the inode information associated with the encrypted video file.

9. A video file decryption method, comprising:

obtaining a to-be-decrypted video file and a decryption key,

decrypting the to-be-decrypted video file using the decryption key to obtain a decrypted video file, and

determining a pre-encryption storage location of the to-be-decrypted video file and moving the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file.

10. The method of claim 9, wherein decrypting the to-be-decrypted video file using the decryption key to obtain the decrypted video file comprises:

reading header data having a second length and stored in a header of the to-be-decrypted video file and obtaining a ciphertext storage area in accordance with the header data,

reading the ciphertext in accordance with the ciphertext storage area,

decrypting the ciphertext using the decryption key to obtain an plaintext, the decrypted ciphertext having a first length greater than a second length, and

obtaining the decrypted video file in accordance with the decrypted ciphertext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext.

11. The method of claim 10, wherein obtaining the decrypted video file in accordance with the plaintext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext comprises:

obtaining a to-be-decrypted video file storage area,

starting from a start point of the to-be-decrypted video file storage area, obtaining a storage area having a first length as a plaintext storage area,

maintaining the remaining data in the to-be-decrypted video file, overwriting the plaintext storage area with plaintext to obtain the decrypted video file.

12. The method of claim 10, wherein the to-be-decrypted video file comprises a preview-required video file, the method comprising:

reading the plaintext of the first length and the remaining data, and making a streaming video from the plaintext and the remaining data to be provided to a streaming media to be played.

13. The method of claim 9, wherein determining the pre-encryption storage location of to-be-decrypted video file and moving the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file comprise:

obtaining inode information associated with the to-be-decrypted video file,

obtaining an established correspondence between inode information associated with a to-be-encrypted video file and inode information associated with an encrypted video file,

obtaining, from the established correspondence, pre-encryption inode information corresponding to the inode information associated with the to-be-encrypted video file, the pre-encryption inode information comprising the to-be-encrypted video file and a pre-encryption storage path,

moving the decrypted video file to a storage location indicated by the pre-encryption storage path by changing the inode information associated with the to-be-decrypted video file to the pre-encryption inode information.

14. A video file encryption device, comprising:

a first obtaining module that obtains a to-be-encrypted video file and an encryption key,

an encryption module that encrypts the to-be-encrypted video file using the encryption key to obtain an encrypted video file,

a second obtaining module that obtains scanned non-hidden partitions of a mobile terminal and an extended memory of the mobile terminal for storing user data, and

a first moving module that determines a partition storing the to-be-encrypted video file among the non-hidden partitions and moves the encrypted video file to a folder in the partition storing the to-be-encrypted video file.

15. The device of claim 14, comprising:

a scanning module that scans the non-hidden partitions of the mobile terminal and the extended memory of the mobile terminal, and

creates a folder in each of the scanned partitions.

16. A video file decryption device, comprising:

a third obtaining module that obtains a to-be-decrypted video file and a decryption key,

a decryption module that decrypts the to-be-decrypted video file using the decryption key to obtain a decrypted video file, and

a second moving module that determines a pre-encryption storage location of to-be-decrypted video file and moves the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file.

17. The device of claim 16, wherein the decryption module comprises:

a second read sub-module that reads header data having a second length and stored in a header of the to-be-decrypted video file, obtaining a storage area of ciphertext in accordance with the header data,

a third read sub-module that reads the ciphertext in accordance with the storage area of the ciphertext,

a decryption module that decrypts the ciphertext using the decryption key to obtain an plaintext, the plaintext having a first length greater than a second length, and

an overwriting sub-module that obtains the decrypted video file in accordance with the plaintext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext.

18. A mobile terminal, comprising the video file encryption device of any one of claims 14-21 and the video file decryption device of any one of claims 22-26.

19. A non-transitory computer-readable medium of a device, the medium storing a program which, when executed by a processor, performs the steps of:

obtaining a to-be-encrypted video file and an encryption key,

encrypting the video file using the encryption key to obtain an encrypted video file,

obtaining scanned non-hidden partitions of a mobile terminal and an extended memory of the mobile terminal for storing user data,

determining a partition storing the to-be-encrypted video file among the non-hidden partitions, and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file.

20. A non-transitory computer-readable medium of a device, the medium storing a program which, when executed by a processor, performs the steps of:

obtaining a to-be-decrypted video file and a decryption key,

decrypting the to-be-decrypted video file using the decryption key to obtain a decrypted video file, and

determining a pre-encryption storage location of the to-be-decrypted video file and moving the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file.

What is claimed is:

1. A video file encryption method, comprising:

obtaining a to-be-encrypted video file and an encryption key,

encrypting the video file using the encryption key to obtain an encrypted video file,

obtaining scanned non-hidden partitions of a mobile terminal and an extended memory of the mobile terminal for storing user data, and

determining a partition storing the to-be-encrypted video file among the non-hidd en partitions, and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file,

wherein the determining a partition storing the to-be-encrypted video file among the non-hidden partitions and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file, comprise:

obtaining inode information associated with the to-be-encrypted video file, the inode information comprising a storage path, the inode information corresponding to video data in the video file,

allocating, in accordance with the storage path associated with the to-be-encrypted video file, one of the partitions for storing the to-be-encrypted video file,

calculating, in accordance with the folder of the partition for storing the to-be-encrypted video file, a storage path associated with the encrypted video file so that the storage path associated with the encrypted video file points to the folder in the partition for storing the to-be-encrypted video file, obtaining inode information associated with the encrypted video file, and

moving the encrypted video file to the folder of the partition for storing the to-be-encrypted video file by changing the inode information associated with the to-be-encrypted video file to the inode information associated with the encrypted video file.

2. The method of claim 1, comprising:

scanning the non-hidden partitions of the mobile terminal and the extended me mory of the mobile terminal, and

creating a folder in each of the partitions from the scan.

3. The method of claim 1, wherein encrypting the video file using the encryption key to obtain the encrypted video file comprises:

reading header data having a length equal to a first length and stored in a header of the to-be-encrypted video file,

encrypting the header data using the encryption key to obtain ciphertext, and

obtaining the encrypted video file in accordance with the ciphertext and remaining non-header data in the to-be-encrypted video file.

4. The method of claim 3, wherein obtaining the encrypted video file in accordance with the ciphertext and the remaining non-header data in the to-be-encrypted video file comprises:

obtaining a header data storage area in the to-be-encrypted video file,

obtaining, based on the header data storage area, a designated header data storage area having a second length and a ciphertext storage area, the second length less than the first length, the designated header data comprising the storage area for storing the encryption key and an encryption ID,

generating the designated header data while maintaining the remaining non-header data in the to-be-encrypted video file, writing the designated header data and the encryption key into respective corresponding storage areas to obtain the encrypted video file.

5. The method of claim 4, wherein obtaining, based on the header data storage area, the designating header storage area having the second length comprises:

starting from a start point of the header data in the storage area for the to-be-encrypted video file, obtaining a storage area having the second length for storing data as the designated header data storage area.

6. The method of claim 4, wherein obtaining the ciphertext storage area based on the header data storage area, comprises:

obtaining a length of the ciphertext, and determining whether the length of the ciphertext is greater than a difference between the first length and the second length,

if the length of the ciphertext is less than or equal to the difference, subtracting the designated header storage area from the header area storage area to obtain the ciphertext

storage area,

if the length of the ciphertext is greater than the difference, subtracting the header data storage area from the designated header data storage area to obtain a partial ciphertext storage area having a length equal to the difference, obtaining a storage area for the to-be-encrypted video file, starting from the end point of the storage area for the to-be-encrypted video file, obtaining a storage area having a length of a remaining part of the ciphertext to obtain a remaining ciphertext storage area.

7. The method of claim 1, comprising:

establishing a correspondence between the inode information associated with the to-be-encrypted video file and the inode information associated with the encrypted video file.

8. A video file decryption method, comprising:

obtaining a to-be-decrypted video file and a decryption key,

decrypting the to-be-decrypted video file using the decryption key to obtain a decrypted video file, and

determining a pre-encryption storage location of the to-be-decrypted video file and moving the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file,

wherein decrypting the to-be-decrypted video file using the decryption key to obtain the decrypted video file comprises:

reading header data having a second length and stored in a header of the to-be-decrypted video file and obtaining a ciphertext storage area in accordance with the header data,

reading the ciphertext in accordance with the ciphertext storage area,

decrypting the ciphertext using the decryption key to obtain an plaintext, the decrypted ciphertext having a first length greater than a second length, and

obtaining the decrypted video file in accordance with the decrypted ciphertext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext.

9. The method of claim 9, wherein obtaining the decrypted video file in accordance with the plaintext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext comprises:

obtaining a to-be-decrypted video file storage area,

starting from a start point of the to-be-decrypted video file storage area, obtaining a storage area having a first length as a plaintext storage area,

maintaining the remaining data in the to-be-decrypted video file, overwriting the plaintext storage area with plaintext to obtain the decrypted video file.

10. The method of claim 9, wherein the to-be-decrypted video file comprises a preview-required video file, the method comprising:

reading the plaintext of the first length and the remaining data, and making a streaming video from the plaintext and the remaining data to be provided to a streaming media to be played.

11. The method of claim 9, wherein determining the pre-encryption storage location of to-be-decrypted video file and moving the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file comprise:

obtaining inode information associated with the to-be-decrypted video file,

obtaining an established correspondence between inode information associated with a to-be-encrypted video file and inode information associated with an encrypted video file,

obtaining, from the established correspondence, pre-encryption inode information corresponding to the inode information associated with the to-be-encrypted video file, the pre-encryption inode information comprising the to-be-encrypted video file and a pre-encryption storage path,

moving the decrypted video file to a storage location indicated by the pre-encryption storage path by changing the inode information associated with the to-be-decrypted video file to the pre-encryption inode information.

12. A video file encryption device, comprising:

a first obtaining module that obtains a to-be-encrypted video file and an encryption key,

an encryption module that encrypts the to-be-encrypted video file using the encryption key to obtain an encrypted video file,

a second obtaining module that obtains scanned non-hidden partitions of a mobile terminal and an extended memory of the mobile terminal for storing user data, and

a first moving module that determines a partition storing the to-be-encrypted video file among the non-hidden partitions and moves the encrypted video file to a folder in the partition storing the to-be-encrypted video file,

wherein the first moving module comprises:

a first obtaining sub-module that obtains inode information associated with the to-be-encrypted video file, the inode information comprising a storage path, the inode information corresponding to video data in the video file;

an allocation sub-module that allocates, in accordance with the storage path associated with the to-be-encrypted video file, one of the partitions for storing the to-be-encrypted video file;

a calculating sub-module that calculates, in accordance with the folder of the partition storing the to-be-encrypted video file, a storage path associated with the encrypted video file so that the storage path associated with the encrypted video file points to the folder in the partition for storing the to-be-encrypted video file, obtaining inode information associated with the encrypted video file; and

a first changing sub-module that changes the inode information associated with the to-be-encrypted video file to the inode information associated with the encrypted video file to move the encrypted video file to the folder of the partition for storing the to-be-encrypted video file.

13. The device of claim 14, comprising:

a scanning module that scans the non-hidden partitions of the mobile terminal and the extended memory of the mobile terminal, and

creates a folder in each of the scanned partitions.

14. A video file decryption device, comprising:

a third obtaining module that obtains a to-be-decrypted video file and a decryption key,

a decryption module that decrypts the to-be-decrypted video file using the decryption key to obtain a decrypted video file, and

a second moving module that determines a pre-encryption storage location of to-be-decrypted video file and moves the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file,

the decryption module comprises:

a second read sub-module that reads header data having a second length and stored in a header of the to-be-decrypted video file, obtaining a storage area of ciphertext in accordance with the header data,

a third read sub-module that reads the ciphertext in accordance with the storage area of the ciphertext,

a decryption module that decrypts the ciphertext using the decryption key to obtain an plaintext, the plaintext having a first length greater than a second length, and

an overwriting sub-module that obtains the decrypted video file in accordance with the plaintext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext.

15. A non-transitory computer-readable medium of a device, the medium storing a program which, when executed by a processor, performs the steps of:

obtaining a to-be-encrypted video file and an encryption key,

encrypting the video file using the encryption key to obtain an encrypted video file,

obtaining scanned non-hidden partitions of a mobile terminal and an extended memory of the mobile terminal for storing user data,

determining a partition storing the to-be-encrypted video file among the non-hidden partitions, and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file,

wherein, to perform the step of the determining a partition storing the to-be-encrypted video file among the non-hidden partitions and moving the encrypted video file to a folder in the partition storing the to-be-encrypted video file, the program performs the steps of:

obtaining inode information associated with the to-be-encrypted video file, the inode information comprising a storage path, the inode information corresponding to video data in the video file,

allocating, in accordance with the storage path associated with the to-be-encrypted video file, one of the partitions for storing the to-be-encrypted video file,

calculating, in accordance with the folder of the partition for storing the to-be-encrypted video file, a storage path associated with the encrypted video file so that the storage path associated with the encrypted video file points to the folder in the partition for storing the to-be-encrypted video file, obtaining inode information associated with the encrypted video file, and

moving the encrypted video file to the folder of the partition for storing the to-be-encrypted video file by changing the inode information associated with the to-be-encrypted video file to the inode information associated with the encrypted video file.

16. A non-transitory computer-readable medium of a device, the medium storing a program which, when executed by a processor, performs the steps of:

obtaining a to-be-decrypted video file and a decryption key,

decrypting the to-be-decrypted video file using the decryption key to obtain a decrypted video file, and

determining a pre-encryption storage location of the to-be-decrypted video file and moving the decrypted video file to the pre-encryption storage location of the to-be-decrypted video file,

wherein, to perform the step of decrypting the to-be-decrypted video file using the decryption key to obtain the decrypted video file, the program performs the step of:

reading header data having a second length and stored in a header of the to-be-decrypted video file and obtaining a ciphertext storage area in accordance with the header data,

reading the ciphertext in accordance with the ciphertext storage area,

decrypting the ciphertext using the decryption key to obtain an plaintext, the decrypted ciphertext having a first length greater than a second length, and

obtaining the decrypted video file in accordance with the decrypted ciphertext and remaining data in the to-be-decrypted video file other than the header data and the ciphertext.

17. A mobile terminal, comprising the video file encryption device of any one of

claims 14 or 15 and the video file decryption device of claim 16.