Visual Security Assessment for Cipher-Images Based on Neighborhood Similarity

Ye Yao, Zhengquan Xu and Jing Sun
Liesmars, Wuhan University, Wuhan 430079,
Hubei, China
E-mail: xuzq@whu.edu.cn

Keywords: cipher-images, visual security, objective assessment, neighborhood similarity

Received: September 7, 2008

In the recent decades, many practical algorithms have been put forward for images and videos encryption. However, there is no objective security assessment algorithm or calculation index has been proposed at present. According to the differences of pixel value and neighborhood distribution between cipher-images and original images, we present a visual security assessment algorithm based on neighborhood similarity. The experiment result shows that the scheme can provide an objective assessment which is match up to subjective assessment, and is also suitable for the security assessment of cipher-images produced by other selective encryption algorithms.

Povzetek: Analizirana je ocena varnosti kodiranja slik.

1 Introduction

With the rapid development of information and network technology, the acquisition and transmission of visual media have been developed at a higher speed than ever. The visual media has been extensively applied to many key departments and fields which are closely related to people's livelihood as well as national security. As a result, the security of visual media (images & videos) is becoming more and more important. In the recent decades, many practical algorithms have been put forward for images and videos encryption[1].

Compressed bitstreams of images and videos become to be cipher-bitstreams when they are encrypted by selective encryption algorithms [1] that can maintain bitstream format compatibility. If cipher-bitstreams are directly inputted to standard decoder and are decoded without decryption, the images we get are called ***cipher-images***.

Compared with the original images (in Fig.1(a)), the pixel value and neighborhood distribution of the cipher-images (in Fig.1(c)) all have been changed. However, for the same original image, different encryption algorithms produce different cipher-images (in Fig. 1(d~f)), which have different changing degrees of pixel value and neighborhood distribution, and then make the ***unrecognizable degree*** much different. The higher the unrecognizable degree of the cipher-images is, the less visual information the attacker will get, which can make the attack more difficult, and the security level of the relevant encryption algorithm should be higher. Therefore, when evaluating and comparing the encryption algorithms of visual media, we need to consider the unrecognizable degree of cipher-image, namely ***visual security***.

Visual security of cipher-images has attracted a lot of attention. However, no researcher put forward systematic research results in visual security assessment means on cipher-images, and no objective assessment algorithm has been proposed. Current researchers of visual media generally give the cipher-images decoded from the cipher-bitstreams at first, and then make a subjective assessment for the unrecognizable degree of the cipher-images. Subjective assessment for the visual security of the cipher-images can be influenced by measurement

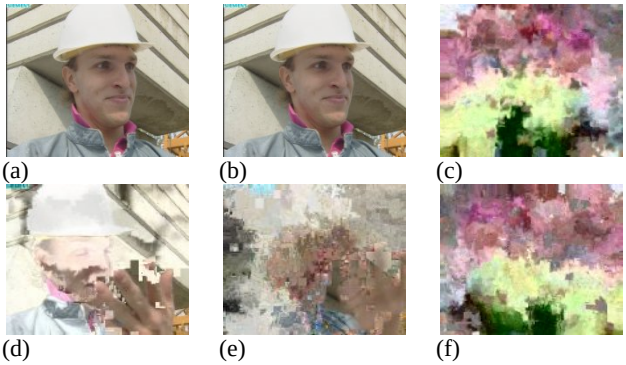


Figure 1: Original images and cipher images. (a) is the original image, (b) is the reconstruction image, (c) is the cipher-image, (d~f) are cipher-images of the image produced by different encryption algorithms.

[1] Supported by the National Basic Research Program of China (Grant No. 2006CB303104) and the National Natural Science Foundation of China (Grant No.40871200/D010702)

environment and subjective sensation. What's more, because of low speed and high cost, it is not very feasible in practical application.

According to the differences of pixel value and neighborhood distribution between cipher-images and original images, we present a visual security assessment algorithm based on neighborhood similarity. This assessment algorithm can assess how much the video information in cipher-videos is distorted, shuffled, and unrecognized, and provide objective assessment compliant with subjective assessment.

2 Background

2.1 Selective encryption algorithms

Visual media have large volume of data with complicated syntax. General data encryption algorithm can not provide direct encryption to protect visual media data. The initial algorithms of visual media encryption protect images by means of shuffling and scramble. As the development of visual media codec technology for images and videos, visual media encryption algorithms have been widely studied since late 1990s, and many achievements have been reported. Among these algorithms, selective encryption algorithms [1,2,3] have attracted more and more attention.

The Selective Encryption Processes with Visual Security Assessment is shown in Fig.2. Selective encryption algorithm encrypts the bits in the compressed bitstreams that are the most critical to image reconstruction. By reducing the amount of data that need to be encrypted, selective video encryption provides a perfect solution to lightweight video encryption. Furthermore, some selective video encryption algorithms generate the encrypted bitstreams that are still compliant with standard syntax

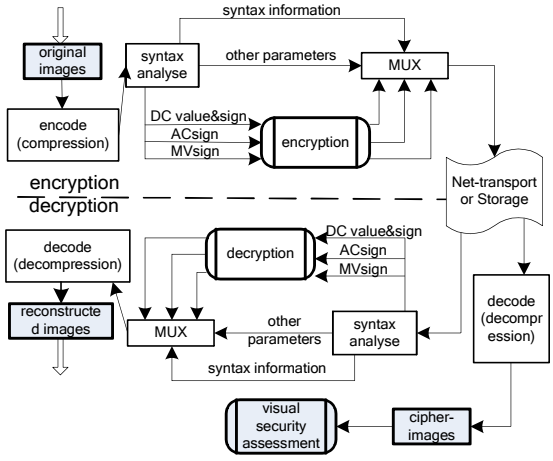


Figure 2: Selective Encryption Processes with Visual Security Assessment.

format. The critical bits of bitstreams do not contain syntax information, such as markers and headers, so the cryptographic bitstreams can keep full bit-level compliance to standard syntax. It is very important to keep bitstreams compliance after encryption for many applications. A standard player will work properly (does not crash) when it decodes these compliant bitstreams of cipher-videos.

Typical selective encryption algorithms [4,5,6,7,8,9,10] include encrypting DCT Coefficients, motion vector, and sign bits of those, and so on. For different kinds of key data encrypted, these cipher-images have different visual security. For example, images without encryption of the motion vectors can be clearly recognized the motion information of people or objects in videos; images without encryption of DC coefficient of low frequency component can be recognized the approximate luminance information; images without encryption of AC coefficient of high frequency component can be recognized the outline information.

2.2 Visual security assessment methods

Visual security assessment is a necessary part of the performance analysis on the image and video encryption algorithms. Security analysis of the encryption algorithm is commonly needed for evaluating and comparing the performance of encryption algorithms. Performance analysis based on cryptanalysis can prove the complexity for the attacker deciphering the encryption algorithm in theory, but can not provide the visual security degree of the cipher-images. In order to develop an objective assessment algorithm on visual security degree of visual media, current security assessments methods of image and video encryption were deep studied and divided into three kinds: assessment based on cryptographic analysis, assessment based on subjective evaluation, and assessment based on video quality assessment.

Assessment based on cryptographic analysis quantitatively analyzes the possibility of deciphering the cipher visual media through the use of cryptanalysis theory. Reference [11] gives the possibilities of ciphertext-only attack, known-plaintext attack and chosen-plaintext attack during the security analysis of encryption algorithms. It also quantitatively gives the compute complexity of ciphertext-only attack through the use of exhaustive method. Reference [12] presents two quantitative cryptanalytic findings on the performance of ciphers against plaintext attacks based on a general model of permutation-only multimedia ciphers. In different perspectives, other references [13,14] also use the cryptanalysis to analyze the possibility and complexity for the attacker to decipher the encryption algorithms successfully. These types of assessments, which process security analysis of encryption algorithms by means of cryptanalysis, are extensively adopted by the most of performance analysis of visual media encryption algorithms.

Assessment based on subjective evaluation process security analysis to the encryption algorithm

subjectively through judging the unrecognizable degree of the cipher-images which decoded from the cipher-bitstreams directly. After introducing the encryption algorithm, reference [15] directly presents six cipher-images of three video test sequences to prove that encryption algorithm can distort the visual information of images, and that cipher-images are unrecognizable to meet the need of visual security. Similarly, reference [16] presents more graphics of cipher-images, and analyzed the unrecognizable degree of the cipher-images subjectively, then compared the visual security of cipher-images getting from different encryption methods. Subjective assessment for the visual security of the cipher-images can be influenced by the measuring environment and subjective sensation. What's more, because of low speed and high cost, it is not very feasible for security analysis only based on the subjective assessment in practical application. Cryptanalysis is needed for security assessment. The subjective assessments are combined with the cryptanalysis, which have already been extensively applied in visual media security evaluation, especially in security evaluation of image encryption algorithm.

Assessment based on video quality assessment theory is a kind of objective security evaluation method, but for which there are few studies or applications so far. There are many video quality assessment methods currently, among which the method based on peak signal noise ratio (PSNR) is widely applied for easy implement and low computational complexity. At present, a few papers of visual media encryption analyze the cipher-images' unrecognizable degree with PSNR value when evaluating the encryption algorithm. Reference [17] presents cipher-images for subjective assessment, and analyze the security degree of the cipher-images according to the cipher-images' PSNR value at the same time. The reference points out that the lower the PSNR value is, the more different between the cipher-images and the original images there will be, and the lower the intelligibility degree of the cipher-image is, so the better the security level is. Reference [18] gives the cipher-images and the change curve of PSNR value, and analyze the recognizable degree of the cipher-images getting from different kinds of encryption algorithms.

Security level evaluation of cipher-images is different from video quality assessment of video codec because they have different research objects and goals. Video quality assessment is a method to measure the distorted degree of loss compression in video codec. It only reflects the accumulation value of error between original image and reconstruction image, which is adopted to assess images that have little difference after compressed and reconstructed. The aim of visual security assessment is to assess how much video information in cipher-videos is distorted, shuffled, and unrecognized. That is to say, visual security assessment has an emphasis on the evaluation of the unidentifiable degree of cipher-images. Cipher-images have many changes not only in pixel value but also in spatial distribution. Therefore, visual security assessment is different from video quality assessment, and the traditional video quality assessment algorithms are not appropriate to evaluate the security level of cipher-videos, and thus it needs to present new objective assessment methods.

3 The proposed assessment scheme

Video image consists of many structured pixels, and there're different levels of brightness value and chromatic value among the pixels. The neighboring pixels present spatial continuous distribution of brightness and chroma. Human visual system could comprehend the continuous distribution of brightness and chroma, and get content information in the images. We consider the continuous characteristic of brightness and chroma in images, and name it as ***neighborhood similarity***.

In Fig.1, the values of pixels in parts of the original image (a) are very close to each other, such as the hat, the wall in background, the face, the clothes, etc. Pixels in these areas have a strong neighborhood similarity. However, when the image is encrypted, the regular spatial distribution of the pixels in these areas is distorted, which results in the decrease of the neighborhood similarity between the neighboring pixels, and the whole image (c) becomes unrecognizable. This paper proposes the definition of neighborhood similarity according to the similarity of the neighborhood distribution of pixels in images. The characteristic that the neighborhood similarity of video images will decrease when the video images are encrypted can provide a way to assess the visual security of cipher-images objectively.

3.1 Definition of neighborhood similarity

***Definition A*:** Let (i, j) and $(i+\alpha, j+\beta)$ denote two pixel in one image with distance as (α, β), and their pixel values are $g_{i,j}$ and $g_{i+\alpha,j+\beta}$. Let the positive constant m denote the difference of the pixel value (Only consider the brightness of pixel value.). Let

$$g(i,j,\alpha,\beta)=\begin{cases}1 & \left|g_{i,j}-g_{i+\alpha,j+\beta}\right|\le m\\ 0 & \left|g_{i,j}-g_{i+\alpha,j+\beta}\right|>m\end{cases} \quad (1)$$

, then the two pixels are ***Similar*** if $g(i,j,\alpha,\beta)=1$; otherwise the two pixel are ***not Similar*.**

***Definition B*:** to calculate whether the points of the $(2d+1)^2$ number on $[-d,+d]$ are similar to the center point (i, j), and to accumulate and normalize the results, then obtain

$$f(i,j) = \sum_{\alpha,\beta\in[-d,+d]} g(i,j,\alpha,\beta) \Big/ (2d+1)^2 \quad (2)$$

. We call $f(i,j)$ the ***Neighborhood Similarity*** of the pixel point (i,j) on the rectangle with radius d.

***Definition C*:** For an image with width M and height N, let the positive constant m denotes the difference of the pixel values, then count the similarity degree of each pixel respectively, and accumulate and normalize the results, get

$$count_m = \sum_{i,j\in[M,N]} f(i,j) \Big/ (M*N) \quad (3)$$

. We call $count_m$ m-level ***Neighborhood Similarity Degree*** of this image.

3.2 Rectangular radius d and pixel value difference m

According to the definition of neighborhood similarity, the value of neighborhood similarity relate to not only spatial distribution states of image's pixel but also the value of d and m. Different value of d and m can lead to different precision.

As to rectangular radius d, big value can get good precision of neighborhood similarity, and result in good description of visual security in theory. However, the computational complexity of neighborhood similarity will increase obviously, when rectangular radius d is numerically larger. For visual security assessment of visual media encryption, we propose that the rectangular radius d have value of 3 or 4, because many video coding algorithms adopt DCT transform with size of 8x8, and such size rectangular radius d represent the pixel boundary of images during video codec. In this paper, rectangular radius d is fixed to 3.

Different images have different spatial distribution of pixels, and different quantity of information. Such difference also exists in different region of the same image. For example, in the original image (a) of Fig.1, the pixel values in the hat region change slightly and in the background wall change more, but in the person face change the most. Therefore, it can assign pixel value difference m to different value to satisfy different precision requirement. Through analysis of some video test sequence, three ranks of pixel value difference m are designed.

1) High precision: High precision value of m represents the similarity of the image area in which the change of pixel value is smooth. For example, in the original image (a) of Fig.1, the hat region pixel value changes slightly, so we can set m a smaller value to get a higher precision. Selecting the pixel point (171, 45), and setting rectangular radius d as 3, can get $(2d+1)^2$ pixel points for which where their pixel values are shown in Fig.3(a).

Analyzing the pixel values, it can be seen that the value of pixel point (171, 45) is 236, and the value of most pixel points around (171, 45) are 235 or 236 with a difference span which does not exceed 2. Due to the discussion above, assigning pixel value difference m to 2 will assure us a higher precision.

2) Medium precision: Medium precision value of m represents the similarity of most image regions. For example, in the original image (a) of Fig.1, the pixel value of the eyes (shown in Fig.3(d)), the nose and the background wall are closely similar to neighbor pixel on a changing trend, so we can set a medium value to get a medium precision. Selecting the pixel point (151,146), and setting rectangular radius d as 3, can get $(2d+1)^2$ pixel points for which their pixel values are shown in Fig.3 (b).

Analyzing the pixel values, we can see that the value of pixel point (151,146) is 64. The values of the pixel points around (151,146) distribute in a wider span. The pixels in left eye of foreman distribute in the range of [61,71], so the pixel value difference m can be set to 5. Due to the discussion above, assigning pixel value difference m to 5 will assure us a medium precision.

236	236	236	236	236	236	235
236	236	236	237	236	236	235
236	235	235	236	235	235	236
236	235	236	236	235	236	237
235	235	236	236	235	237	235
236	236	236	237	236	236	235
235	236	236	234	235	235	235

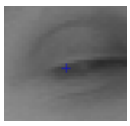
(a) High precision (m=2)

103	105	106	106	101	96	85
99	94	87	77	72	68	66
75	64	63	63	61	63	65
70	68	66	64	63	63	65
77	73	74	71	70	71	74
87	82	79	79	84	84	85
98	96	97	98	98	99	98

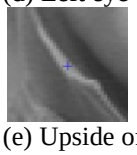
(b) Medium precision (m=5)

159	152	128	89	79	80	76
153	157	146	119	86	78	76
130	158	155	142	116	85	77
108	146	160	151	140	110	87
89	120	156	156	144	136	110
86	96	129	154	154	146	135
83	85	105	134	156	160	155

(c) Low precision (m=10)



(d) Left eye of foreman



(e) Upside of right collapsible

Figure 3: Neighborhood Characteristic of image.

3) Low precision: Low precision value of m represents the similarity of the image area in which the change of pixel value is large. As the areas at the top of the right collapsible shown in Fig. 3(e), the pixel points distribute in a strip. The changes of pixel value within that area are in a wider span, and there are big differences with the pixel points outside these areas. Selecting the pixel point (141,247), and setting rectangular radius d as 3, can get $(2d+1)^2$ pixel points for which their pixel values are shown in Fig.3 (c).

Analyzing the pixel values, it can be seen that the value of pixel point (141,247) is 151. The changes of

pixel value in that area are in a wider span, but the pixel points distribute at the edge of the collar distribute in one strip. The pixel values distribute between [140,160], so the pixel value difference m can be set to 10. Due to the discussion above, assigning pixel value difference m to 10 will assure us a low precision. It is necessary to set pixel value difference m to a bigger value in order to describe neighborhood similarity of complex images.

For different images, we should select pixel value difference m according to different precision demand. High precision pixel value difference m (m=2) is suitable for simple images, which have less quantity of information. Low precision pixel value difference m (m=10) is suitable for complex images, which have more quantity of information. But for many pictures, some regions are smooth and their structures are simple, other regions have much more texture information. We can adopt weighted neighborhood similarity to describe such images, and adjust weighted factor to meet different demand of visual security assessment for different kinds of images.

***Definition D*:** For an image, suppose three level neighborhood similarity are $count_{m=2}$, $count_{m=5}$, $count_{m=10}$ respectively, and the weighted factor is $a+b+c=1$. We define

$$count = a*count_{m=2} + b*count_{m=5} + c*count_{m=10} \quad (4)$$

, then we call $count$ ***Weighted Neighborhood Similarity Degree*** of this image.

3.3 The calculation and comparison of neighborhood similarity degree

For an image or a video frame with width M and height N, its Neighborhood Similarity calculation process is as follows:

1) Choose appropriate rectangular radius d, and pixel value difference m based on 3.2 section's analysis.

2) According to ***Definition B,*** calculate $f(i,j)$ the Neighborhood Similarity of each pixel point (i,j) on the rectangle with radius d by Eq.2.

3) According to ***Definition C,*** accumulate $f(i,j)$ of each pixel (i,j) on the rectangle with radius d, and then get Neighborhood Similarity Degree of the image or the video frame by Eq.3.

For different cipher-images by using different encryption algorithms, we can obtain their objective assessment results on visual security by comparing their Neighborhood Similarity Degree. The larger the Neighborhood Similarity Degree of the image is, the smaller the distorted degree. And the higher the recognizable degree is, the lower the visual security of the corresponding encryption algorithm.

For video sequences, we calculate the Neighborhood Similarity Degree of each frame, and get the curses of Neighborhood Similarity Degree by using different encryption algorithms. Because of different encryption algorithms to be used, different curves of the neighborhood similarity can be obtained, and the smaller the Neighborhood Similarity Degree of the image is, the higher the visual security of the used encryption algorithm. Through observation and comparison of changes in the curves, we can determine the visual security degree of the encryption algorithms.

4 Experiment and results

In this section, through the analysis of different cipher video sequences, three examples are provided for the real applicability of the proposed assessment scheme.

4.1 Visual security assessment for key data encryption

We take the cipher-images of MPEG4 as an example in this paper, and introduce objective assessments of visual security based on neighborhood similarity. The cipher-images of MPEG4 are generated by the selective encryption algorithms which can keep the format compatibility of the bitstreams. There are already many research results [1,3,19,20] on selective encryption algorithm for the MPEG4 compressed bitstreams. Among these results, the proposed key data that can be selectively encrypted includes: DC coefficient sign, DC value, AC coefficient sign, and motor vector sign. Separately encrypting the four types of key data, we can get cipher-images in different recognizable degree. Using the method based on neighborhood similarity we proposed in this paper, we can obtain objective assessment of visual security to these four types of cipher-images.

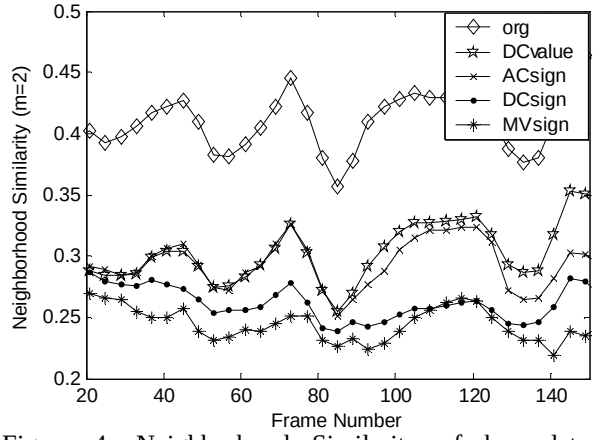


Figure 4: Neighborhood Similarity of key data encryption.

The neighborhood similarity curves of the cipher-images generated by separately encrypting the four types of key data are shown as Fig.4. The topside line (org) of the curve represents the neighborhood similarity of the original image. The lower the value of the neighborhood similarity degree is, the more the image's pixel distribution is distorted, and the better

the visual security level will be. According to the curves of the Fig.4, the cipher-images generated by encrypting MV sign have the best visual security, while the DC value encrypted has the lightest impact. Motion vectors include all the motion information of the video sequence, the motion information after encryption makes the reconstruction of the cipher-images refer to the wrong macro blocks, which has the greatest influence on the recognizable degree of the cipher-images. Based on the above analysis, it can be seen that the cipher-images generated from MV sign encrypted bitstreams have the best visual security. The objective assessments are consistent with the subjective evaluation, and also with the theoretical analysis.

4.2 Visual security assessment for multi-level encryption

By the combine encryption of the four key data, we can realize multi-level encryption to meet the needs of different security and the application of different processing capability. The multi-level encryption algorithm proposed in reference [3], and VEA algorithm, MVEA algorithm and RVEA algorithm proposed in reference [19] all can realize the multi-level encryption. This paper applied the algorithm proposed in reference [19] to encrypt MPEG4 compressed bitstreams. The combination put forward in this reference is as follows: the first level, encrypt AC sign; the second levle, add the encryption of DC value and DC sign; the third level, add MV sign encryption. Different level of encryption leads to different recognizable degree of the cipher-images. By calculating the neighborhood similarity degree, we can get objective assessment of visual security to different security level of cipher-images.

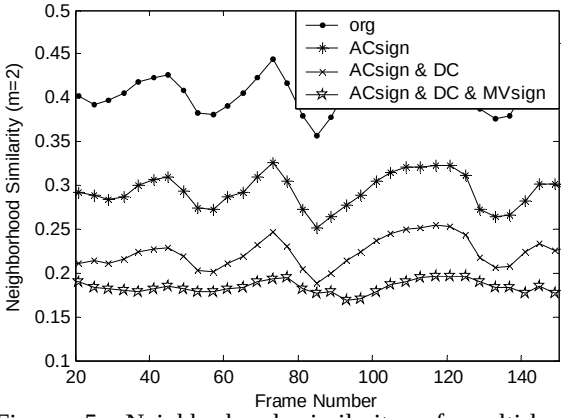


Figure 5: Neighborhood similarity of multi-level encryption.

The neighborhood similarity curves of the cipher-images generated from multi-level encryption of foreman video sequence are shown as Fig.5. We can infer from the curves that with the increase of the key data encrypted, the neighborhood similarity of the cipher-images gradually drops. The cipher-images of the third level encryption that encrypted all the key data have the lowest neighborhood similarity, which reflects the best visual security. However, the original image (org) has no change on the distribution of the pixels, so it has the highest neighborhood similarity. The objective assessments are consistent with the subjective evaluation, and also with the theoretical analysis in theory.

4.3 Visual security assessment for several cipher videos

Encrypting several video test sequences respectively with multi-level selective encryption algorithm, we can get cipher video sequences of different security level. Separately calculating the neighborhood similarity of every frame of the cipher video sequences, and then computing the mean of all the frames' neighborhood similarity, we can get the mean neighborhood similarity of each cipher video sequences. By comparison of the mean neighborhood similarity of the three security level of cipher video sequences, we get the objective visual security assessment result of the multi-level encrypted video sequences.

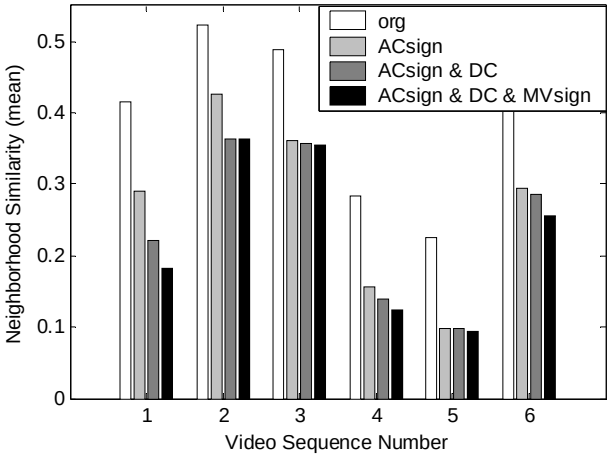


Figure 6: Neighborhood similarity of several cipher videos.

Using bar charts, the mean values of neighborhood similarity for the six multi-level encrypted video sequences are shown as Fig.6. The six video sequences are: foreman, mother&daughter, news, tempete, mobile, hallmoniter. Inferred from the bar charts, with the key data encrypted adding, the neighborhood similarity of each cipher video sequence gradually decreased. The height of the bars basically reflects relative value of neighborhood similarity. Except for sequence 2, 3 and 5, the distinction degrees of the visual security assessment is better for the other video sequences. There is no significant difference between the neighborhood similarity of the third level and that of the second level of video sequence 2 (mother&daughter), that's because the motion information of this video sequence is comparatively less, and the third level cipher-bitstreams have no significant difference from the second level after adding the MV sign encryption. Distinction degrees of

video sequence 3 and 5 are not ideal, which shows the objective algorithm proposed in this paper needs to improve.

5 Performance analysis

In this section, we give performance analysis of the proposed assessment scheme, such as computational complexity, time complexity and applicability, and so on. On applicability analysis, different evaluation results were analyzed in detail in Section 4. As can be seen from the analysis, the changes of neighborhood similarity of cipher video sequences in the curve can be a very good reflection of the changes of visual security.

On the computational complexity and time complexity, we also did experiment and analysis. For the CIF (352 * 288) size of the video sequences, the calculation time of the neighborhood similarity for each frame is not more than one second. Furthermore, from Fig. 2, we can see that the proposed assessment of visual security is independent of the process of video codec, and it also independent of encryption and decryption. Visual security assessment scheme can be made an independent module. For cipher video sequences by using different encryption algorithms, we can obtain objective evaluation results by off-line analysis. As a result, computational complexity and time complexity will not affect the application of the proposed objective visual security assessment scheme. And the research on visual security should be focused on the applicability of assessment algorithms.

6 Conclusions and future work

Visual security is a very important target of security assessment in the field of video encryption, which has direct relation to the attacker's comprehension degree of the cipher-images. The more information the attacker gets from the cipher-images, the faster the unauthorized decryption will be. Security analysis of video encryption now mostly put emphasis on the security analysis of the encryption algorithm, but not on the visual security assessment method. Till now, an applicable objective security assessment algorithm or calculation index has not been proposed. Therefore, it need to present new objective security assessment method. On one hand, based on the analysis of encrypting different key data, it can guide us to design good combinations of key data encryption, and then design selective encryption algorithms of high visual security. On the other hand, it can be applied to evaluation the visual security of the encryption algorithms and provide some references on performance analysis. It can be believed that the study will be very significant to further research on video encryption.

We present an objective method based on neighborhood similarity to carry out visual security assessment in this paper. It takes cipher-images as the research object, which is independent of video encryption algorithms. Therefore, it can be made an independent module based on off-line analysis, and its computational complexity and time complexity will not affect its application. The detail analysis in Section 4 verifies that our proposed assessment method is efficient to evaluation the visual security of the encryption algorithms. Our next step is focused on the research of the availability of evaluation, especially on the extension of its applicability.

Visual security assessment is a brand-new research topic. After we present the objective assessment method based on neighborhood similarity, all the relevant research will begin soon. The method proposed in this paper will probably be further optimized and improved, and new objective assessment algorithms would be developed based on the characteristic of cipher-images.

References

[1] Wen Jiangtao, Severa Michael, Zeng Wenjun, Luttrell Maximilian, etc. A format compliant configurable encryption framework for access control of Video. IEEE Tran. Circuits & Systems for Video Technology, 2002, Vol. 12, 545-557.

[2] Howard Cheng and Xiaobo Li. Partial Encryption of Compressed Images and Videos. IEEE Transactions on Signal Processing, v 48, n 8, Aug, 2000, 2439-2451.

[3] Yuan chun, Zhong yuzhuo, Yang Shiqiang. Composite Chaotic Pseudo-Random Sequence Encryption Algorithm for Compressed Video. Tsinghua Science and Technology. 2004, Vol.9, No.2, 234-241.

[4] Iskender Agi and Li Gong. An empirical study of secure MPEG video transmission. Proceedings of the Internet Society Symposium on Network and Distributed Systems Security. San Diego, CA, 1996. 137-144.

[5] Tang Lei. Methods for encrypting and decrypting MPEG video data efficiently. Proceedings of the Fourth ACM International Multimedia Conference (ACM Multimedia 96'). Boston, MA, 1996. 219-230.

[6] Ali Saman Tosum and Wuchi Feng. Efficient multilayer coding and encryption of MPEG video streams. IEEE International Conference on Multimedia and Expo. New York, 2000. 119-122.

[7] Lintian Qiao and Klara Nahrstedt. Is MPEG encryption by using random list instead of zigzag order secure. IEEE International Symposium on Consumer Electronics. Singapore, 1997, 226-229.

[8] Shi C G, Bhargava B. A fast MPEG video encryption algorithm. Proceedings of the 6th ACM International Multimedia Conference. Bristol, 1998, 81-88.

[9] Changgui Shi, Shengyih Wang, Bharat Bhargava. MPEG video encryption in realtime using secret key cryptography. Proceedings of

the International Conference of Parallel and Distributed Processing Techniques and Applications (PDPTA99'). Las Vegas, Nevada, 1999, 2822-2828.

[10] JuiCheng Yen, Juning Guo. A new MPEG encryption system and its VLSI architecture. IEEE Workshop on Signal Processing Systems. Taipei, 1999. 430-437.

[11] Shiguo Lian, Zhongxuan Liu, Zhen Ren, Zhiquan Wang. Selective Video Encryption Based on Advanced Video Coding. PCM 2005, Part II, LNCS 3768, 281-290.

[12] Shujun Li, Chengqing Li, Guanrong Chen, Nikolaos G. Bourbakis, Kwok-Tung Lo. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing: Image Communication, 2008, vol. 23, no. 3, 212-223.

[13] Yuan Li, Liwei Liang, Zhaopin SU, Jianguo Jiang. A New Video Encryption Algorithm for H.264. ICICS 2005, 1121-1124.

[14] Yuanzhi Zou, Tiejun Huang, Wen Gao, Longshe Huo. H.264 Video Encryption Scheme Adaptive to DRM. IEEE Transactions on Consumer Electronics, Vol.52, No.4, NOVEMBER 2006, 1289-1297.

[15] Jinhaeng Ahn, Hiuk Jae Shim, Byeungwoo Jeon, Inchoon Choi. Digital Video Scrambling Method Using Intra Prediction Mode. PCM 2004, LNCS 3333, 386-393.

[16] Sang Gu Kwon, Woong Il Choi, Byeungwoo Jeon. Digital Video Scrambling Using Motion Vector and Slice Relocation. ICIAR 2005, LNCS 3656, 207-214.

[17] Shiguo Lian, Zhongxuan Liu, Zhen Ren, Haila Wang. Secure Advanced Video Coding Based on Selective Encryption Algorithms. IEEE Transactions on Consumer Electronics, Vol.52, No.2, MAY 2006, 621-629.

[18] Thomas Stutz, Andreas Uhl. On Efficient Transparent JPEG2000 Encryption. MM&Sec'07, September 20-21, 2007, Dallas, Texas, USA.

[19] Bharat Bhargava, Changgui Shi, Sheng-Yih Wang. MPEG Video Encryption Algorithms. Multimedia Tools and Applications, 2004, Vol.24, No.1, 57-79.

[20] Wenjun Zeng, Shawmin Lei. Efficient Frequency Domain Selective Scrambling of Digital Video. IEEE Transactions on Multimedia, 2003, Vol.5, No.1, 118-129.