Research on Selective Encryption Algorithms of GIF Image Degradation Mode Based on GML

Ming Zhong1, a,Xu Ran2, b,Fang Cheng3, c, Jun Zhou4, d, XuDong Zhang5,e, ShunQin Li6,f

1,2,3NetWork Information Center,Chongqing Communication College,Chongqing,400035,China
4Basci Experiment Center,Chongqing Communication College,Chongqing,400035,China
5Equiment Office,Chongqing Communication College,Chongqing,400035,China
6Computer Basic Department ,Chongqing City Management College,Chongqing,401331,China
aemail:rfox@sina.com, bemail:361760350@qq.com, cemail:cf-cq@163.com, demail:453606051@qq.com, eemail:2245471608@qq.com,femail:weimilee@163.com

Abstract

GIF image is one of the most widely applied images on the Internet. This article puts forward selective encryption algorithms for degradation mode based on coding features of GIF image and presents encryption effect picture through experience and then analyzes its safety, enciphered data size, format compatibility and compression ratio.

Keywords: GIF format; degradation; format compatibility; safety;

1. Introduction

Multimedia information, such as digital image, audio and video is widely applied in Internet. To fully utilize the features of multimedia, selective encryption technology is widely employed [1]-[4]. Selective encryption is to select parts of data which is significant to human's sensing system for encryption so as to greatly reduce the calculated amount of encryption. Selective encryption at early stage was mainly based on the selective bit plane of uncompressed image. With wide application of compression technique, selective encryption technology based on compressed encoding becomes people's research emphasis [2][3].

There are two kinds of application modes for multimedia selective encryption technology: for degradation or confidentiality. Degradation is to degrade the definition of multimedia object, but will not reduce its main information. Confidentiality is to realize full protection over contents of multimedia so as to avoid interception of unauthorized users.

This article proposes selective encryption technology for degradation mode based on GIF encoding and this method can realize format compatibility of GIF encoding and has good performance in the aspects of security and compression ratio.

2. Brief introduction of format coding

GIF data generally includes two parts: color index list and encoding data flow. Encoding data flow adopts LZW compression algorithm with variable length. LZW algorithm can achieve the goal of reducing file size through compressing repeated parts of original data. A index list will be created dynamically in the course of encoding to store those character strings (or pixel string) which have appeared. If the encoding process involves the character strings which have appeared before, then this character string can be encoded by its index value, thus it is a kind of forward dependence encoding. GIF encoding also has some special rules on the basis of LZW compression algorithm.

3. Degradation of GIF format image

3.1 Basic degradation algorithm based on CML

We realize degradation by using the way of scrambling the original color index list. In original color index list for GIF encoding, each color of the image is designed with one index. Scrambling of this index list equals to substitute the same colors in original image with another color, but the shape of object in the image will not change, thus the degradation can be realized.

3.1.1 Chaotic coupled map lattices CML

Herein we adopt chaotic coupled map lattices CML[5] to produce scrambling table. Application of chaos in encryption is a relatively popular encryption method. CML employs the approach of coupling of two chaotic mappings which can perfectly solve the problem about degradation of dynamic attribute within limited precision. This article uses CML formed by two chaotic skew tent mappings to generate pseudorandom sequence. The definition of skew tent mapping is as follows:

$$g(x) = \begin{cases} x/b & 0 < x < b \\ (1-x)(1-b) & b \le x < 1 \end{cases}$$

(Formula 3.1)

Therein, *b* is a system parameter and *x* is a chaos state, $0 < b, x < 1$. Two skew tent mappings are coupled according to following rules:

$$\begin{cases} x_1(t) = \varepsilon \cdot g(x_1(t-1)) + (1-\varepsilon) g(x_2(t-1)) \\ x_2(t) = \varepsilon \cdot g(x_2(t-1)) + (1-\varepsilon) g(x_1(t-1)) \end{cases}$$

(Formula 3.2)

Therein, $x_1(t)$ and $x_2(t)$ are status values of two skew tent mappings, but ε is the coupling weight with a value very close to 1. Herein, the system parameter b and original state x_0 of these two skew tent mappings serve as the secret key to produce random sequences through multiple iterations, and then these random sequences can generate scrambling list. If a scrambling list within the range of [0, 2^n − 1] is required, 2^n random numbers can form a random sequence $P = [x_0, x_1, ..., x_{2^n-1}]$, and the random numbers in Sequence P will be sorted. m_i represents the position (counting from 0) of random number x_i after sorting and Table $T^{'} = [m_0, m_1, ..., m_{2^n-1}]$ is the produced scrambling table.

3.1.2 Basic degradation algorithm

It is assumed that T represents original color index table; I represents original image; $I^{'}$ represents encoding data flow; function L represents LZW encoding operation. Then encoding process of GIF can be:

$$I^{'} = L(T, I)$$

(Formula 3.3)

Function $C_{K1}(T)$ can be adopted to produce scrambling table to scramble T, and therein K1 represents the secret key for generation of scrambling table, so the degradation algorithm can be:

$$I^{'} = L(C_{K1}(T), I)$$

(Formula 3.4)

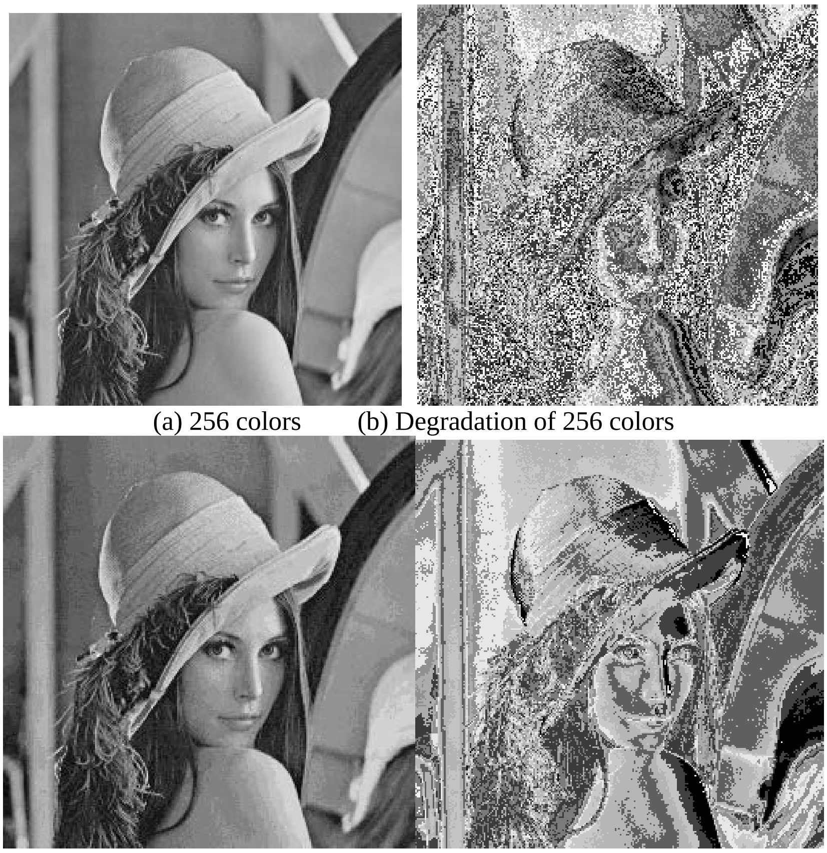
During decoding, the original color index table is scrambled by using same secret key and scrambling method and this index table is used to carry out LZW decoding. We employ function L^{-1} to represent decoding operation of LZW algorithm, and then decoding process can be described by formula as follows:

$$I = L^{-1}(C_{K1}(T), I^{'})$$

(Formula 3.5)

Attention: scrambled index table $C_{K1}(T)$ is still used for decoding.

Four pictures in Picture I are result comparison after we use above mentioned algorithm to degrade 256 colors Lena picture (a) and 64 color Lena Picture (c). Picture (b) is the degradation result of 256 color Lena Picture and we can see rough picture contour. Picture (d) is the degradation result of 64 color Lean Picture and we find that the picture contour is clearer.



(a) 256 colors (b) Degradation of 256 colors

(c) 64 colors (d) Degradation of 64 colors

(Picture I: basic degradation algorithm encryption for Lena Picture)

We can find out that this basic degradation algorithm can perfectly realize image degradation only under the circumstance of simple scrambling, but result in bad image quality for images with rich colors.

3.2 Adoption of degradation algorithm with subset scrambling to control image visibility

The result of experiment in Section 3.1 shows that the way of scrambling the whole original index table can realize degradation, but the image quality is relatively bad for those images with rich colors and is not applicable for previewing. Thus, we adopt index table with subset scrambling to realize control of visibility of degraded image.

Subset scrambling is to divide the index table into N continuous subsets $\{ T_1, T_2, ..., T_N \}$, and then scramble these subsets respectively, i.e.

$$T^{'} = C_{K1}(T_1, T_2, ..., T_N) = \{C_{K1_1}(T_1), C_{K1_2}(T_2), ..., C_{K1_n}(T_N)\}$$

(Formula 3.6)

Therein, $K1_1, K1_2, ..., K1_n$ are different sub-keys produced by the secret key $K1$.

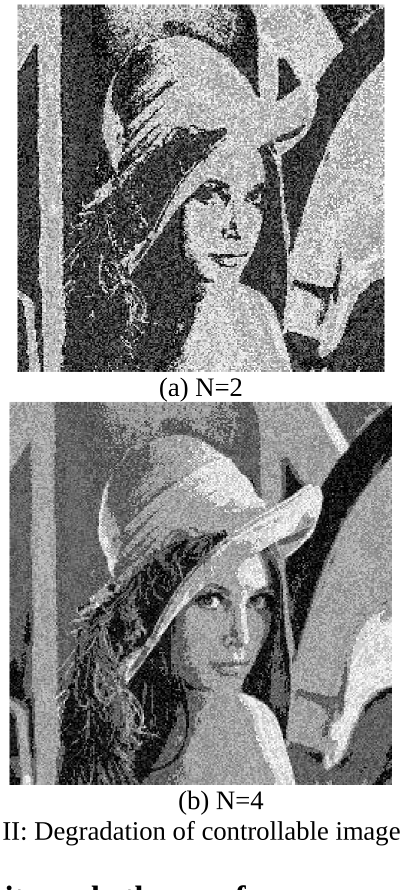
Then the degradation algorithm for subset scrambling can be described by formula as follows:

$$I' = L\left(C_{K1}\left(T_1, T_2, ..., T_N\right), I\right)$$

(Formula 3.7)

With the degradation algorithm for subset scrambling, pixel value of image only vary within the subset range and the image quality can be controlled by adjusting number of subsets. More divided subsets will result in narrower variation range of pixel values and the quality of degraded image will be higher.

Picture II is the effect picture after dividing color index table into different subsets and then using degradation algorithm for subset scrambling to encrypt. In Picture (a), N=2 and in Picture (b), N=4. We can find out that (b) contains more details than (a).



(a) N=2

(b) N=4

(Picture II: Degradation of controllable image quality)

Analysis on security and other performances

For the above mentioned encryption algorithm, we respectively conduct security analysis.

Degradation algorithm: security of degradation algorithm depends on the security of produced scrambling table. In the event of ciphertext-only attack, scrambling space for original color index table of 256 color images is 256!. The attack is unworthy for common commercial application. In the event of known-plain text attack, color index table *T'* can be obtained by comparing pixel value of know-plain text image with pixel values of corresponding points in ciphertext image. It is unsafe to select plain text to attack this algorithm. Therefore, we can use the way of one-time pad to strengthen the security and use different secret keys $K1$ to produce scrambling tables.

According to the above analysis, we think that for common commercial application, the algorithm has sufficient security, but for the application requiring higher security level, we can encrypt more code streams to improve the security.

In other aspects, the algorithm also has good performance:

Encrypted data size: the algorithm only selects minor data to encrypt and computation complexity is reduced. For a 256×256 image, the encrypted data size only accounts for about 1% of compressed data size.

Format compatibility: degradation algorithm is to scramble the original index table and will not impact encoding and decoding process of LZW so as to realize format compatibility;

Compression ratio: degradation algorithm will not impact encoding process of LZW, so it will not result in change of compression ration. Meanwhile, the encryption algorithm assures same length of plain text and ciphertext and will not lead to additional bits.

Table I is performance contract of various encryption algorithms. N1 represents color number used in original color index table and N2 represents frequency of occurrence of Clear Code in the course of encoding.

Performance Algorithm	Security	Format compatibility	Encrypted data size (byte)	Compression ratio	Image visibility after encryption
Basic degradation algorithm	High degradation degree	Format compatibility	N1	Not change	Visible picture contour
Controllable degradation algorithm	Controllable degradation degree	Format compatibility	N1	Not change	Controllable visibility

(Table I: performance contrast of encryption algorithm)

Conclusion

GIF image is one of the most widely applied images on the Internet currently. This article put forwards selective encryption algorithms for degradation mode based on coding features of GIF image. We adopt the way of subset scrambling to realize controllability of image degradation and guarantee format compatibility and unchanged compression ratio.

Reference

[1] C. Wu, C. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems", IEEE transaction on multimedia, 2005 Vol. 7(5), pp.828-839

[2]H. Cheng ,X. Li. “Partial encryption of compressed images and videos”. IEEE Transactions on Signal Processing,2000,48(8):2439–2451

[3]Changgui Shi, Bharat Bhargava.“An efficient MPEG video encryption algorithm.” Pro-ceedings of the 17th IEEE Symposium on Reliable Distributed System. IEEE Computer Soci-ety,1998a:381-386

[4] Grangetto, M.; Magli, E.“Multimedia Selective Encryption by Means of Randomized Arithmetic Coding”Multimedia,IEEE Transactions on Volume 8,Issue 5,2006:905-917

[5]Fridrich,J.“Symmetric ciphers based on two-dimensional chaotic maps.” I.J.Bifur.Chaos,
1998,8,(6):1259-1264