International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.12 (2016), pp.181-190
http://dx.doi.org/10.14257/ijmue.2016.11.12.17

A Study on Hybrid Encryption Technique for Digital Contents of Copyrights

Hwan-Seok Yang

Dept. of Information Security Engineering, Joongbu University
Goyang-si, Gyeonggi-do, Korea
yanghs@joongbu.ac.kr

Abstract

The environment using multimedia information such as image, audio, and video is widely applied through the rapid development of the IT environment. The digital content industry applying this has been developed in a variety of forms. However, copyright is subjected to a serious threat as digital content is distributed in quantity with the spread of the Internet. Also, business model of companies is threatened largely by the variety of attacks such as illegal copy and transformation of digital content. In this paper, we propose a hybrid encryption in order to prevent copyright information damage by malicious attacks. The encryption process in two steps is performed in order to enhance hiding copyright in the proposed technique. The block encryption process is performs to prevent exposure and transformation of encrypted information after encryption performs using ARIA algorithm for copyright information. The encrypted copyright information like this improved robustness to several of attacks. The performance of the proposed technique is confirmed by experiments.

Keywords*: Digital Contents; Hybrid Encryption; Copyrights; Steganography*

1. Introduction

Recently, application field of multimedia information is growing rapidly by the wide spread of wireless computing devices and the rapid development of network technology. Especially, entertainment-oriental digital content markets such as music, image, and broadcasting are growing rapidly. Digital content can be applied and distributed through information communication network such as the internet, digital broadcasting such as DTV, and a storage media such as DVD. However, digital content has vulnerabilities that can be replicated easily, reproduced by a forgery, and leak easily data by network eavesdropping. In order to prepare for this vulnerability, many studies have been conducted on the techniques that can fundamentally prevent the illegal content through technical means such as watermarking, DRM (Digital Rights Management), and steganography for digital content. (1-2) However, the strong cryptography for copyright information is required because many damages by a variety of attacks are caused nowadays.

In this paper, we propose hybrid cryptography to protect the copyright of digital content safely and prevent illegal distribution. Two-step encryption process is performed in order to protect the copyright information safely. In the first step, 7-copyright information is encrypted using ARIA encryption algorithm. The encryption key used for the encryption in the process is inputted from the user. In the second step, the process that mixes and hides randomly the information is performed after the encrypted copyright information is blocked to two-dimensional array. By doing so, it can improve further the security by having the complexity than existing blocked encryption algorithm. The proposed technique was comparative experimented with Chord technique and the excellent performance was confirmed.

ISSN: 1975-0080 IJMUE

This paper is organized as follows. Chapter 2 explains the techniques for copyright protection. The hybrid encryption technique for improve the safety of the proposed copyright information is described in chapter 3. The performance evaluation of the proposed technique is performed through experiments in chapter 4. Finally, chapter 5 concludes.

2. Related Works

Digital content security technology enhances security such as Digital Rights Management (DRM), Data Leak Prevention(DLP) in fear of the technology leakage. The technique protecting the copyright for the digital content is classified into two types. One is the technique blocking fundamentally the access of unauthorized user using access control by encryption technology. The other one is the technique tracking or monitoring distribution channels after the identification information to the digital content is inserted or database that extracts the feature information which can identify individual digital content is built.

2.1 Digital Content Protection Technology

Protection technology to prevent illegal outflow by controlling in order that only authorized users can access to digital content is CPRM, CAS, DRM, *etc.* CPRM(Content Protection for Recordable Media) is a copy protection technology that prevents copying content to other storage medium by encrypting digital content to a specified storage medium or device information. (3) CAS(Conditional Access System) has been used as copyright protection technology in the satellite digital broadcasting, *etc.* It provides encryption function of broadcasting content and a function which can watch the broadcast content after only the contractor releases the password. DRM(Digital Rights Management) is a technology for solving the existing drawback that relies on only encrypted. (4) If the digital content is copied to other computer, the hidden private key in the computer or unique ID is changed and a certification process must be again undergone because of the method using by transforming the unique ID of the user's computer or the method using this that embed the user's private key in the computer.

The content protection technology using the hiding data has been utilized for a variety of purposes such as proof of ownership and copyright protection. It is insufficient to provide sufficient means to verify the content's integrity because encryption is guaranteed only protection on the content deployment process although it also is a method for digital content protection and one decoded content cannot be protected anymore. (5) However, hiding technology can be good way to protect content even after distributed because hiding technology can satisfy the requirements of a variety of information insert, toughness, and confidentiality. The data hiding technology is classified into steganography and digital watermarking according to the relevance of the inserted message and the original content. The inserted confidential information in the data hiding methods by steganography is no relevance of the origin content and is a means of transformation of only confidential information. However, digital watermarking is that message to be inserted and origin content has a close association. The metadata for origin content or information for the integrity verification becomes the contents of the watermark.

Steganography transmits the confidential information by hiding to any of the cover image. This technology makes other people not to recognize the presence or absence of hided confidential information by changing pixel value of cover image. (6-7) In other words, it utilizes a method hiding another file in the file. It is a method transmitting by hiding important data and the third person knows as to transmit general data not important data. It is more secure than encryption because the fact that data transmitting to the third people is a confidential data can be hided. The biggest drawback of steganography is that

is easy to be caught because of capacity by putting the file in the file. The other drawback is that can extort the file using this tools because hiding file mostly is not encrypted when the file is hided using this technology. In other to overcome, the file should be transmitted by reducing the capacity of the file as much as possible.

The digital watermarking technology has invisibility, security, robustness, and insertion space. The invisibility means that watermark should not be visible after video, audio, picture, *etc.* compared to the original image when watermark is inserted to video, audio, picture, *etc.* In other words, the watermark entering content should not be known when watermarked video is seen or heard. The digital watermark has the important characteristics related to the content protection on the internet. The security means that should not determine whether watermark is inserted or not after the content that watermark is inserted is looked. (8) The security and invisibility has similar characteristics. The watermark included in the digital content has a characteristics that the watermark should be detected after this signal processing because it is strong to a general compression, filtering, rotation, transfer, enlargement, reduction, brightness change, color change, noise added, and filter processing. That these characteristics are important is because restoring is a goal that data compression technology removes most of unnecessary or redundant information of image and audio, compresses, and restores this as close to the origin picture. (9)

Insertion space means the space to insert the watermark. That is, this is that should put enough copyright information and it is required to the technology inserting enough copyright information to minimal space by streamlining insertion space. Figure 1 shows the process of the watermarking.

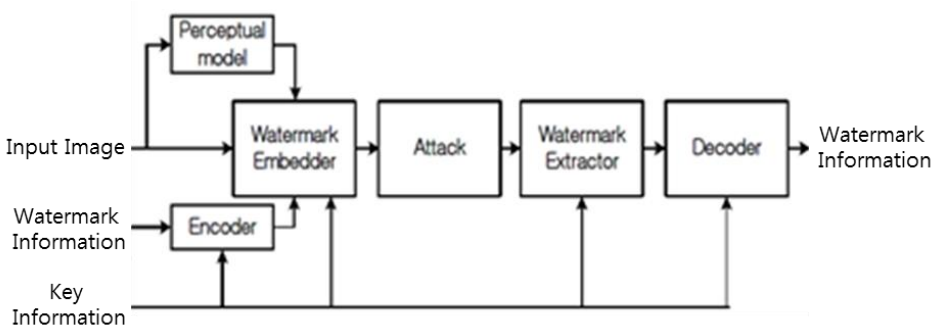

Figure 1. The Process of the Watermarking

3. The Proposed Hybrid Cryptography

The hybrid cryptography of the copyright is described in order to block the illegal distribution of digital content by protecting the copyright of the digital content.

3.1. The Structure of the Proposed Technique

The structure of cryptography proposed in this paper is composed of a two-step encryption process in order to have the robustness to various attacks. First, the first step is the step of encrypting by using the ARIA encryption algorithm and the copyright of digital content. In this step, the encryption is performed by using 7 copyright and the encryption key used for encryption is inputted from the user. The encrypted copyright information like this is divided, mixed randomly, and hided after the encrypted copyright information is blocked to two-dimensional array using a block encryption in the second step. The hided for copyright information is enhanced without causing a large change in digital content through this process.

3.2. The Copyright Encryption

In this paper, ARIA(Academy, Research, Institute, Agency) encryption algorithm is used for encryption of the copyright information about the digital content. ARIA algorithm uses a block of 128-bit size and a key of 128, 192, and 256-bit size. It is a block encryption algorithm having ISPN(Involutional SPN) structure of 12, 14, 16 round according to a key size. The substitution layer in even-numbered and odd-numbered rounds is different in each round function of ARIA. In addition, it is the structure that the inverse of the substitution layer of the even-numbered round becomes to the substitution of the odd-numbered round. Bits of the encryption key give a number that starts from zero and ends to a smaller number than the key length. The given number of bits i is the bit index and is one range among $0 \le i \le 128$, $0 \le i \le 196$, and $0 \le i \le 256$ according to the block and key lengths. This ARIA is designed to be resistant to all known attacks to the block cryptography. The round function of ARIA encryption algorithm consists of round key addition(AddRoundKey), substitution layer(SubstLayer), and diffusion layer(DiffLayer). Round function uses a different type of substitution layer by odd-numbered round and even-numbered round. The diffusion layer in the final round is replaced to round key addition in the final round. In the first AddRoundKey, 128-bit round key is performed XOR operation with round input 128-bit by bit. Second, substitution layer is composed of the two kinds of 8-bit input and output S-box and has to satisfy the properties that the maximum differential/linear probability is 2^{-6}, algebraic order is 7, and no fixed point and half-fixed point. The form for the affine transform to function x^{-1} on the finite $GF(2^8)$ satisfying these properties has been widely used. x^{-1} has the same characteristics with x^{-2^n}, $n = 0, \ldots, 7$ and S-box is created by doing an affine transform of x^{-1} and x^{2^n}. That is, S-box S_1, S_2 is the same as equation (1), (2).

$$S_1(x) = B x^{-1} \oplus b \quad (1)$$

$$S_2(x) = C x^{-1} \oplus c \quad (2)$$

Here, B, C is a nonsingular matrix, and b, c is 8×1 matrix. In ARIA, S_1, S_2 and the reverse substitution S_1^{-1}, S_2^{-1} is used. Third, diffusion layer is the main part distinguished with other block cryptography and uses involutions binary matrix. The spreading function outputs 16 bytes of result performing the matrix products for the 16 bytes. The diffusion layer considers the most importantly safety and efficient implementation possibilities in various application environments.

The key expansion of ARIA is divided into two parts initialization process and the round key generation process. In the key initialization process, four 128-bit values is created from cryptography key using 3 round Feistel cryptography as shown in Figure 2.

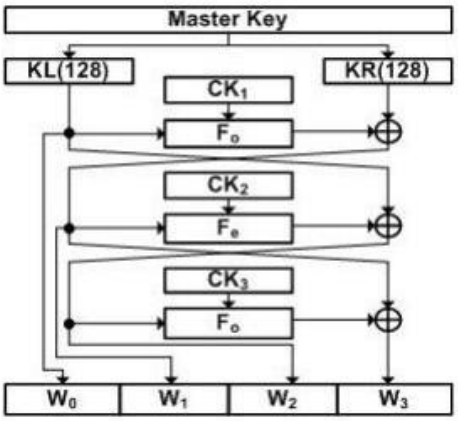

Figure 2. The Process of Key Initialization

The hiding order of copyright information is as follows. First, seven copyright information such as name, date of birth, email address, *etc.* and the data such as insert time of the copyright information is ' #' as a separator. And a string of series is made. Second, the encrypted copyright information is gotten by ARIA encryption algorithm that this string is a plain text and inputted password is a key.

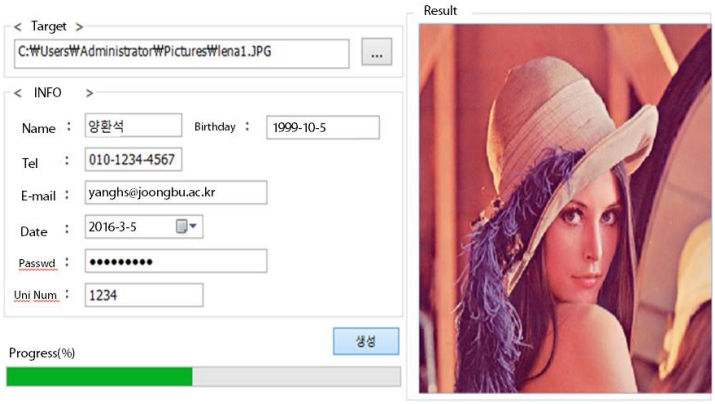

Figure 3. Encryption Copyright Information Using ARIA

3.3. Encrypted Copyright Block Encryption

This step is the process that encrypted copyright information is done to block encryption in order to improve the robustness of the various attacks for encrypted copyright information using ARIA algorithm. First, encrypted copyright information to ARIA algorithm is divided into 1/N after it is configured in a two-dimensional array. That is, it is improved security with more complexity because encryption information is interlinked to up, down, left, and right and blocked than DES or AES that data regularly in one-dimensional array is blocked to 64bit or 128bit and applied encryption algorithm. Figure 4 shows the block encryption of the encrypted copyright information.

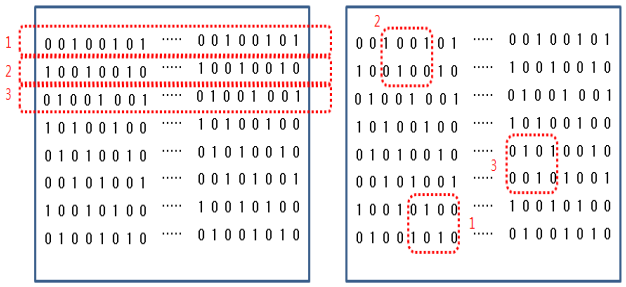

Figure 4. Block Encryption of the Encrypted Copyright Information

The permutation process that the information is mixed randomly is processed after blocking the encrypted copyright information described above. The robustness of the copyright attack is ensured and the copyright information is protected more safely through this process. Figure 5 shows the appearance of hiding information using blocked encryption.

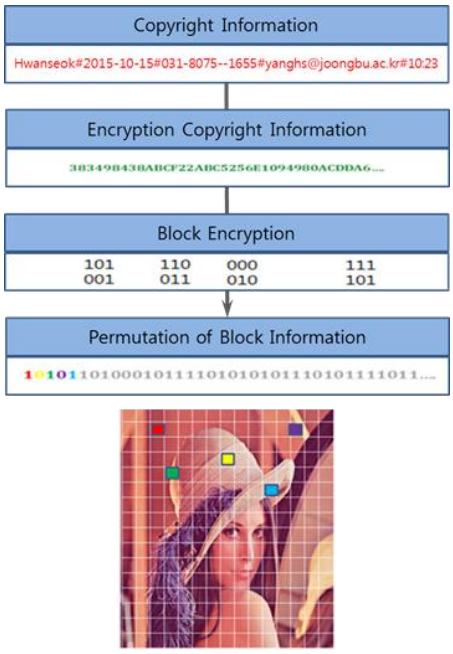

Figure 5. Information Hiding Using Block Encryption

4. Performance Analysis

4.1. Experimental Environment

In this chapter, the performance of cryptography was measured to protect the copyright information proposed in this paper. 4 24bit color images of 512×512 size of USC-SIPI(University of Southern California-Signal & Image Processing Institute) image database were used.

(Sailboat) (Lena) (Tree) (House)

Figure 6. The Experimental Images

7-copyright information was used in the experiment. Image degradation exposed visually was evaluated by inserting copyright information to the image through block cryptography after this copyright information was encrypted. PSNR(Peak Signal to Noise Rate) value was calculated and compared in order to evaluate quantitatively the quality of image inserting copyright information of the proposed encryption technique. PSNR(dB) was calculated by the Equations (3) and (4) based on the quality of the origin image. The robustness of geometry attack and vertex attack was measured.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}[I(i,j)-K(i,j)]^2 \quad (3)$$

$$PSNR = 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \quad (4)$$

4.2. Performance Analysis

Figure 7 shows the quantitative analysis result by PSNR numerical calculation. As shown in Figure 7, numeric value did not appear high in the result that inserted copyright information encrypted by the proposed cryptography. In other words, we can confirm it is difficult to acknowledge this from the attacker because it is difficult to check inserted status of the copyright information when it compared visually with the original image.

Insert Level	Sailboat	Lena	Tree	House
0	48.60	47.31	47.94	48.10
1	44.30	42.80	43.20	44.60
2	39.90	40.60	38.70	42.10
3	36.50	37.50	35.80	38.20
4	35.42	36.46	34.20	36.60

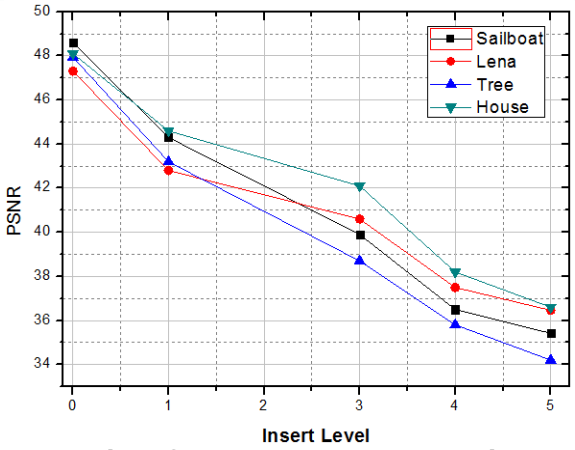

Figure 7. The Results of PSNR Measurement about Four Images

Figure 8 shows experimental result measuring detection rate of copyright information after copyright information instigates geometry attack and vertex attack to the inserted image in order to measure the robustness on the attack of the proposed cryptography. Detection rate of the copyright information after geometry attack was higher more than 93% in all four images. It showed a high detection rate of 85% or more for addition/detection attack of object. Detection rate will be lower if addition/detection attack of object is increased. The detection rate appears similarly for an attack to cut when 70% of the total data is left. However, the robustness of proposed technique was confirmed for the vertex attack that loss of direct data occurs.

Attack Types		Detection Rate(%)			
		Sailboat	Lena	Tree	House
Geometry Attacks	Rotation 1°	98.7%	98.2%	98.2%	98.4%
	Rotation 15°	97.2%	97.4%	95.6%	96.4%
	Rotation 30°	96.9%	97.1%	96.2%	95.9%
	Scaling 0.7	97.8%	98.1%	97.4%	96.9%
	Scaling 2	98.6%	98.4%	97.9%	97.4%
Vertex Attacks	Add 10 Object	97.6%	95.9%	96.8%	95.3%
	Add 40 Object	96.2%	94.6%	94.1%	93.4%
	Del 10 Object	94.2%	93.9%	93.4%	94.2%
	Del 40 Object	92.6%	92.1%	91.2%	92.9%

Figure 8. Copyright Detection Rates for the Attacks

5. Conclusion

The use of multimedia information has been increased rapidly and the digital content industry is being developed in various forms due to the wide spread of the internet and the wireless terminal. The damage caused by illegal acts and attacks for digital contents is increasing day by day in this IT environment and the preparation for this is required.

In this paper, we proposed the hybrid encryption technique to hide securely the copyright information in digital content. The proposed technique is largely made up of a two steps encryption process for safe protection of the copyright information. The first step is to perform a cryptographic process for 7-copyright information using ARIA encryption algorithm. This encrypted copyright information like this is hided using block cryptography of the two-dimensional structure. In particular, the security performance of the blocked information is further improved by increasing the complexity through information hiding courses mixing at random. The hided copyright information in this way cannot be recognized by attacker. It is not possible to determine the information accurately even if found. In this way, the ability that can block the illegal deal in a digital content was provided. In addition, we confirmed proposed encryption technique is robust against geometric and vertex attacks through experiments.

Acknowledgement

This paper was supported by Joongbu University Research & Development Fund, in 2016.

References

[1] S. Goel, A. Rana and M. Kaur, "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems www.ijcdsonline.com, vol. 3, no. 1, **(2013)**.
[2] D. Mistry, "Comparison of Digital Watermarking Methods", (IJCSE) International Journal on Computer Science and Engineering, vol. 2, no. 9, **(2010)**, pp. 2805-2909.
[3] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, vol. 1, no. 2, **(2013)**.
[4] Y. Yusof and O. O. Khalifa, "Digital Watermarking for Digital Images Using Wavelet Transformation", appear in proceeding of the IEEE, **(2007)**, pp. 665-669.
[5] C. S. Chan and C. C. Chang, "An efficient image authentication method based on Hamming code", The Journal of the Pattern Recognition Society, **(2007)**, pp. 681-690.
[6] Z. J. Lee, S. W. Lin, S. F. Su, and C. Y. Lin, "A hybrid watermarking technique applied to digital images", Applied Soft Computing, **(2008)**, pp. 798-808.
[7] I. Usman and S. Khan, "BCH coding and intelligent watermark embedding: employing both frequency and strength selection", Applied Soft Computing, **(2010)**, pp. 332-343.

[8] X. Zheng and J. Jin, "Research for the application and safety of MD5 algorithm in password authentication", Paper presented at Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on, Sichuan, **(2012)**, pp. 2216-2219.
[9] F.-H. Hsu, M.-H. Wu and S.-J. Wang, "Dual-watermarking by QR-code applications in image processing", Paper presented at Computing (UIC/ATC). 2012 9th International Conference on, **(2012)**, pp. 638-643.

Authors

Hwan-Seok Yang, he is holding Assistant Professor Position in Information Security at Joongbu University. In 2007-2010, he worked as a Research Professor in Dept. of Cyber Investigation Police at Howon University. He received the Ph. D. degree in Computer Science and Statistics from the University of Chosun in 2005. He conducts research in the general areas of security analysis of computer system and mobile networks.