International Journal of Multimedia and Ubiquitous Engineering
Vol.8, No.5 (2013), pp.105-118
http://dx.doi.org/10.14257/ijmue.2013.8.5.11

A New Framework for Encryption and Authentication of Multimedia Data

Sudhish N. George, R. Arun Raj and P. P. Deepthi

Department of Electronics & Communication Engineering
National Institute of Technology, Calicut, Kerala, India - 673601

sudhish@nitc.ac.in, arunraj.kolasseril@gmail.com, deepthi@nitc.ac.in

Abstract

The multiple Huffman table (MHT) based encryption technique for multimedia encryption gained much popularity, due to its simplicity, less complexity and good compression performance. At the same time, it is proved that the MHT based encryption system is vulnerable to several types of attacks. In this paper, the security issues of the MHT based encryption system are analyzed. On the basis of analysis, the paper proposes a modified version of MHT based encryption system, with minimal impact on its simplicity and compression performance. It is proposed to perform blockwise shuffling of the transformed image (in DCT domain) based on a chaotic map prior to the MHT stage, so that an attacker cannot retrieve the key because of the changes in the spatial arrangement caused by the blockwise shuffling in the transform domain. Moreover, to ensure copyright protection as well as traitor tracing, it is proposed to incorporate joint fingerprinting and decryption (JFD) technique at the receiver stage. The system is subjected to the known forms of attacks and it has been proved that the proposed system is able to resist the same with minimal level of increase in the system complexity.

Keywords: *Multimedia Encryption, Multiple Huffman Table, Joint Fingerprinting and Decryption, Data Compression*

1. Introduction

Over the past decades, there was a rapid development in the multimedia processing techniques. Moreover, due to the development of computer, internet and wireless technologies, the easiness of processing, storing and distributing the multimedia content gained immense attraction. To allow for wider availability of multimedia information and successful commercialization of many multimedia related services, assuring that multimedia information is used only by authorized users for authorized purposes has become essential [1]. Thus, encrypting the multimedia content is becoming a mandatory requirement to assure the usage of data only by authorized users. Moreover, once the data is decrypted, there may be the chances of illegal redistribution of multimedia data by the users/service providers. To avoid such malpractices, multimedia authentication techniques were developed [2]. In general, encryption and authentication techniques have great importance in the field of multimedia systems.

A large number of encryption techniques were proposed in the literature for encrypting the multimedia data, where large amount of data is to be processed. The conventional block based encryption standards like DES, AES, RSA etc are faithful, when small amount of data is used. Since, the multimedia processing deals with large chunks of data; it is becoming illogical to

ISSN: 1975-0080 IJMUE

use these conventional cryptographic techniques. Moreover, due to the non-iid nature of multimedia sources, the use of conventional cryptographic techniques (developed for iid sources) becomes inefficient. Since, most of the multimedia applications need real time operations, the block based encryption techniques are less suited because of the introduction of delay [7]. One of the main challenges faced by the multimedia communication system is the compression performance due to the limited bandwidth. It will not create any possibility to make any compromise in the overall compression performance while applying the encryption technique.

Some of the possible domains in which the encryption can be applied in multimedia systems are sample domain, quantized transform domain, together and after entropy coding domain [1]. Even though, some encryption techniques were proposed for compressing the encrypted data [4], generally the encryption before the entropy coding stage changes the statistical properties of the data resulting in the reduction of compression performance. If the encryption is provided after compression, it may destroy the structures and syntax of the coded bitstream. Thus, the most promising domain for performing the encryption is together with the entropy coding stage, so that the compression performance remains intact. The most popular entropy coding techniques are Huffman coding and arithmetic coding. The multimedia standards like JPEG, MPEG, mp3 etc. use Huffman coding, whereas JPEG 2000, H.264 etc. use arithmetic coding as its entropy coding stage. The well known entropy coding based encryption techniques are multiple Huffman table (MHT) [5], arithmetic coding with key based interval splitting (KSAC) [6] and randomized arithmetic coding (RAC) [7]. Since, arithmetic coding is very sensitive to errors and resynchronization capabilities [8], this paper focuses on the Huffman coding based encryption technique.

In MHT based encryption system, multiple statistical models are alternately used in a secret manner to encode the input symbols [5]. In the literature, it is proved that the MHT based encryption system is vulnerable to known plaintext attack [9-10] and ciphertext only attack [11]. Thus, the MHT based encryption system alone is unable to provide complete level of end to end security and making modifications to Huffman coding must be done with extreme care without affecting its compression performance and simplicity. Thus, the aim of the proposed system is to give some modification to the MHT based system without creating much overhead in the resource complexity and maintaining a comparable compression performance as that of the normal Huffman coding system.

Since, the security of the decrypted data is completely lost, it is required to apply suitable authentication technique to provide entity authentication, data authentication, non-repudiation and key authentication. In order to protect the multimedia content after decryption from unauthorized dissemination by the service provider/end user (traitor tracing), each service provider/end user should be uniquely identified by embedding unique ID for each copy [2]. The joint fingerprinting and decryption (JFD) technique can fulfill this requirement. Since, the JFD technique provides lesser system complexity, better real time system performance and is resistant against various types of collusion attacks [12-14], it is the most promising technique for multimedia authentication.

The aim of this work is to develop a system which provides high level of encryption and data authentication with very less impact in the compression performance and resource complexity. The rest of the paper is organized as follows. Section 2 introduces the basic principles of multiple Huffman table based encryption and joint fingerprinting and decryption techniques and analyses the security issues of the MHT based encryption system. Section 3 proposes the modified method of MHT based encryption system which is capable of negating the drawbacks of MHT system and includes JFD for content authentication. Results and its discussions are given Section 4. The paper concludes in Section 5.

2. Basic Principles

The first part of this section explains the fundamental principles of MHT based encryption system and its cryptanalysis. It is found that the MHT based encryption system is vulnerable to several forms of attacks. The second part gives an overview about the JFD technique to provide multimedia authentication.

2.1 Multiple Huffman Table based encryption

Huffman coding is the simplest and fastest entropy coding technique, which provides high efficiency. Thus, providing encryption in the Huffman coding stage without affecting its simplicity and speed of operation is a challenging task. In [5], Wu *et al.*, proposed a multiple Huffman table (MHT) based encryption system to provide compression and encryption simultaneously. In MHT system, an adaptive entropy coder based on multiple Huffman tables is used. The selection of particular Huffman tables and the order in which they are selected are kept secret as the key of the encryption algorithm. The basic algorithm for MHT based encryption can be summarized in three steps as listed below.

1. Choose m different Huffman coding tables numbered from 0 to $m-1$.
2. Generate a random vector $P = (p_0, p_1..., p_{n-1})$, where each p_i is a k-bit integer varying from 0 to $(m - 1)$ and k is equals to $\lceil \log_2 m \rceil$.
3. For the i^{th} symbol in the original data stream, use $p_{i \bmod n}$ table to encode it.

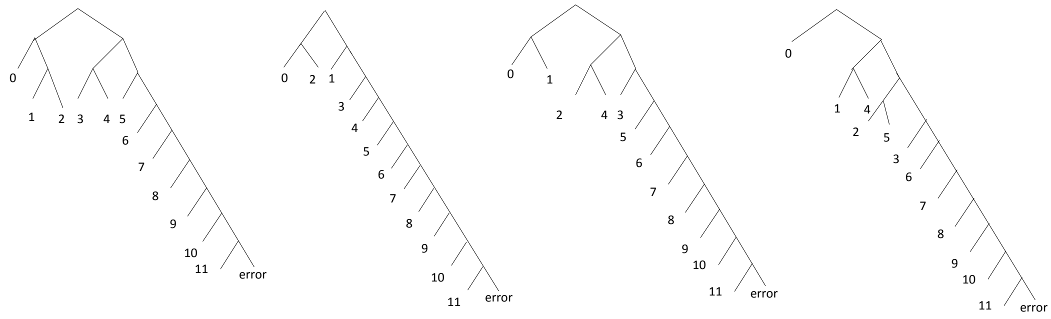

Figure 1. Basic Huffman trees used in MHT scheme

The typical values for m and n are 8 and 128 respectively. The problem of limited key space can be avoided by using m statistical models instead of one. Since, the memory requirements to store these statistical models is linearly increased with the value m, m should be kept as a small value. In order to avoid such a scenario, in [5] itself, Wu *et al.*, suggested to select only four Huffman coding tables, instead of training thousands of Huffman tables. Based on these four Huffman tables, it is possible to obtain thousands of Huffman tables by using the technique, known as Huffman tree mutation. The mutation operation can be implemented by using a key. To do this, if the i^{th} bit of the key is 1, the labels of two branches of the i^{th} node in the Huffman tree are exchanged, otherwise kept unchanged. Thus, the number of possible values of an n-bit code of a symbol increases to 2^n [5, 10]. Since, there is no additional computation overhead for this algorithm compared with the standard Huffman coding, MHT based system is computationally fast [9]. The basic Huffman trees are given in Figure 1.

2.2. Cryptanalysis of MHT scheme

In [10], it is proved that the MHT based encryption scheme is vulnerable to known plaintext attack. They have considered two key possibilities; long-term keys and pre-message keys. In long-term keys, one key is used to encrypt a large number of messages, whereas, for pre-message keys a new key is generated for each new message. Jakimoski *et al.*, proved that in both cases, MHT system is vulnerable to known plaintext attack [10]. Zhou *et.al.* theoretically proved that MHT based encryption is not secure under chosen-plaintext attack, known-plaintext attack and ciphertext-only attack [11]. They claimed that with only 10 known plaintext–ciphertext pairs for long-term key encryption scheme or one ciphertext and its corresponding plaintexts consisting of 10 blocks of symbols for per-message key encryption scheme, an attacker can recover the key with known-plaintext attack. With several thousands of ciphertexts, it is possible to recover the key with ciphertext-only attack [11].

2.3. Joint Fingerprinting and Decryption

In [12], Kundur *et al.*, proposed a method for joint fingerprinting and decryption for video data. The basic idea is to partially decrypt the multimedia ciphertext and the un-decrypted ciphertext imitates multimedia fingerprint embedding. In JFD, the encryption key K_s is a group key. But, each user has a single key K_i, which is unique for that user. This gives the provision of embedding a unique fingerprint for each user to get distinct copies for different users. The relative entropy between the encryption and decryption keys gives the information carried by the fingerprint. It can be mathematically represented as,

$$H(f_i) = H(K_g/K_i)$$

where, $H(f_i)$ is the entropy of the fingerprint for user i. The block diagram for JFD architecture is shown in Figure 2.

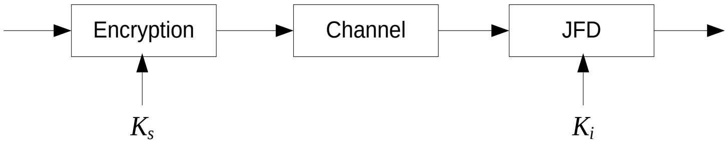

Figure 2. Simplified block diagram of JFD

The receivers do not have the knowledge about the key *Ks*. Generally, the correlation between decryption and encryption keys derives the fingerprint. The fingerprint is from the multimedia data (image or video). Initially, the perceptually relevant components X are extracted. It is then selectively encrypted with global key *Ks*. Then, the resultant encrypted multimedia content Y is given to the user through distribution channel. In the receiver section, for each receiver, unique keys K_i are provided. The fingerprint is embedded in the decrypted data using appropriate embedding techniques without affecting the perceptual quality of the image/video. The main problem with the JFD is the collusion attack. This is nothing but, the attempt of the user or a group of users to destroy the fingerprint embedded in the decrypted data. Therefore, proper coding techniques can be used to generate fingerprint such that it is resistant against collusion attacks. The most popular coding techniques are orthogonal fingerprinting and coded fingerprinting using BIBD techniques [12-14].

3. Modified multiple Huffman table based encryption technique

From the literature, it is clear that even though the MHT based encryption system provides good compression performance and simple design, it is vulnerable to many forms of attacks. Moreover, the system is not capable of providing any authenticity, once it is decrypted. Hence it is necessary to develop a modified version of MHT based encryption system, which can provide better security before decryption and authenticity after decryption without adversely affecting its compression performance and simplicity. From Section 2.2, it is clear that the MHT based encryption system alone is not capable of providing complete level of security before and after decryption. Thus, it is better to provide some less complicated encryption stages before the MHT stage, so that the system can withstand known plaintext attack. In known plaintext attack, some pairs of plaintexts and corresponding ciphertexts are available with the attacker and hence the attacker has the maximum information about the data. Thus, if the system is able to withstand known plaintext attack, it can be concluded that the system is highly secure.

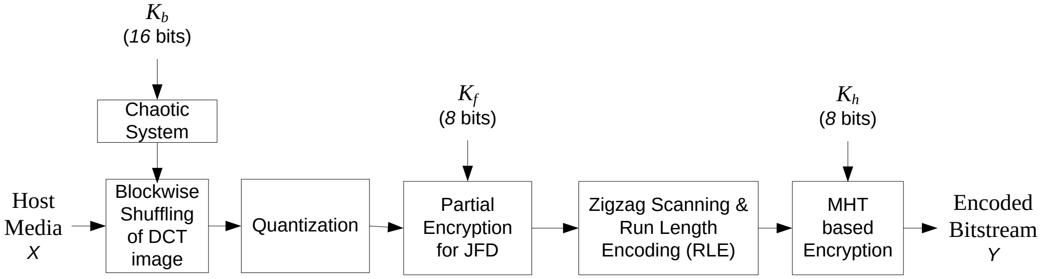

Figure 3. Proposed encryption system

In the proposed system, various stages of JPEG standard are considered for experiments. Providing encryption in the spatial domain reduces the compression performance since it destroys the spatial correlation. Hence it is better to provide the encryption in the transform domain so that the compression performance can be maintained. It is proposed to perform blockwise shuffling of the transformed image (after applying the DCT) based on a chaotic map. To provide authenticity after decryption, it is better to implement the JFD technique in the decryption stage. Since, the JFD method is based on the partial decryption technique, it is required to include a partial encryption stage in the encoding section. Thus, to maintain data security before and after the decryption, it is necessary to incorporate two encryption stages before the MHT stage. The proposed encryption system is shown in Figure 3.

3.1. Blockwise shuffling of transformed image

In order to increase the security of the system, blockwise shuffling algorithm is incorporated in the transformed image. It can be performed before or after the quantization stage. Incorporating a shuffling algorithm in the spatial domain can result in an immense reduction in the compression ratio. Since, in most of the multimedia applications, the larger compression is a mandatory requirement, it is not possible to implement the shuffling algorithm in the spatial domain. Hence performing the shuffling operation in the transform domain, without affecting the compression ratio is favorable. Thus, block-wise shuffling of DCT matrix is performed so that compression remains intact. Shuffling is performed based on a chaotic map.

Assume that the size of the plain-image is $M \times N$. Select an initial condition *x(0)* of a one-dimensional chaotic system as the secret key of the encryption system defined by the following logistic map [15-16].

$$x(n) = \mu x(n-1)(1 - x(n-1))$$

The shuffling operation can be summarized as follows.

1. Select an $M \times N$ image, divide it into blocks of 8×8 and apply DCT.
2. Run the chaotic system

   for $i = 1 : (MN/8)$

   $$x(i) = \mu x(i-1)(1 - x(i-1))$$

3. Group the chaotic sequence into 8-bits to form pseudo random array of MN/64 integers.
4. Shuffle the blocks of image based on the pseudo random array.

The block shuffling operation can be implemented before or after the quantization stage. Since the blocks of the transformed image are shuffled with respect to the different states of chaotic map, the correlation properties of the images are not lost and effective compression performance is not reduced. Moreover, shuffling operation inside a block is not effective, because of the statistical properties of the coefficients, where an attacker can easily find the correct order of coefficients. Hence, the most promising domain for performing the shuffling operation is the blockwise shuffling of the block transformed domain, so that the compression performance remains unchanged.

3.2. Partial encryption for JFD

In Section 2.3, it is mentioned that the joint fingerprinting and decryption technique is based on the principle of partial decryption. Hence it is required to provide a partial encryption in the encoder stage. In the proposed system, the partial encryption is incorporated after the quantization stage in the JPEG coding standard. An 8-bit key can be used to implement the partial encryption. It can be implemented as follows,

$$x_{pi} = x_{di} + k_f$$

where, x_{di} represents the selected coefficients for partial encryption, k_f represents the encryption key and x_{pi} represents the partially encrypted coefficients.

3.3. Multiple Huffman table based encryption

In Section 2.2, it is explained that even though, the MHT based encryption system can provide encryption and compression simultaneously, it is vulnerable to several forms of attacks. But, when the MHT system is supported with a prior encryption stage, it is difficult for an attacker to find out the correct key easily. The MHT based encryption system can be implemented as described in Section 2.1. The four basic Huffman trees and their mutated versions are used to implement MHT based encryption system. An 8-bit key can serve this operation. Thus, together with the block shuffling stage the MHT based encryption system can provide highly secure system with negligible increase in the system complexity.

3.4. Joint Fingerprinting and Decryption

As discussed in Section 3.2, partial encryption is provided in the encoding stage to incorporate JFD in the decoding stage. This is done by adding the selected coefficients with the partial encryption key k_f. The partially encrypted received coefficients can be represented as,

$$r_{pi} = r_{di} + k_f$$

where, r_{pi} and r_{di} are received partially encrypted coefficients and corresponding original coefficients respectively. To implement JFD, it is necessary to provide unique keys for each user. The partial decryption key k_j for the j^{th} user can be obtained as,

$$k_j = \alpha \times id_j - k_f$$

where, id_j represents the unique id assigned to user j and 'α' is the perception coefficient. 'α' is selected in such a way that the reconstructed images remain perceptually unaltered. The coefficients after embedding the fingerprint can be expressed as,

$$\begin{aligned} r_{fi} &= r_{pi} + k_i \\ &= r_{pi} + \alpha \times id_i - k_f \\ &= r_{di} + k_f + \alpha \times id_i - k_f \\ &= r_{di} + \alpha \times id_i \end{aligned}$$

Thus, the selected coefficients of each user's copy are modified with the unique id assigned to each user ensuring that the fingerprint embedding does not create any perceptual difference. To make the proposed system a collusion resistant scheme, any robust watermarking scheme can be incorporated.

4. Results & Discussions

This section deals with the results obtained from the proposed system. It includes the compression analysis, perceptual quality analysis after embedding the fingerprint and cryptanalysis. A comparison analysis with standard JPEG coding system was performed and it was proved that the proposed system provides a comparable compression performance as that of the standard JPEG coding. The perception coefficient 'α' was selected in such a way that the fingerprinted image does not create any visual disturbance. The security of the proposed system is measured in terms of various types of attacks and it was proved that the system can withstand the same.

4.1. Compression Analysis

The standard quantization matrix is selected to provide a compression level of 50. Proper scaling of the quantization matrix gives a compression level in the range of 0 to *100*. The PSNR value reduces as the value of compression level goes from 0 to 100.

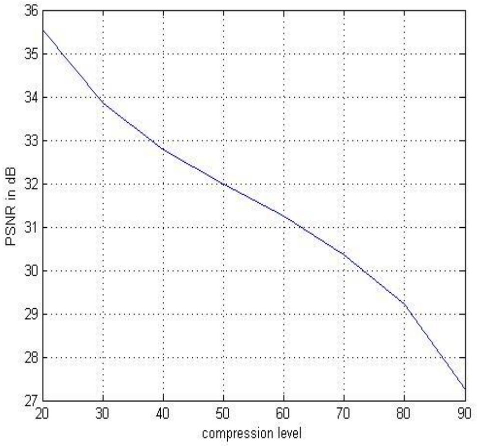

Figure 5. PSNR – Compression level characteristics

The PSNR can be calculated as,

$$PSNR = 10\log_{10}\left(\frac{MAX_I}{MSE}\right)$$

where, MAX_I represents the maximum pixel value of an image. MSE for an $M \times N$ image can be calculated as, $MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - K(i,j)\right)$

where, $I(i, j)$ and $K(i, j)$ correspond to original and reconstructed pixels respectively. Figure 5 shows the compression performance of standard Lena image of size 256×256. The comparison of compression performance against several standard test images like Lena, Mandril, Cameraman etc. of different sizes are performed. The percentage increase in the compression of the proposed system with respect to standard JPEG is listed in Table 1. From the table, it is clear that on an average the proposed system can provide a comparable compression performance as that of the JPEG coding standard.

Table. 1 Comparison of compression performance of the proposed system

Test Image	Number of bits after encoding		Percentage increase in compression for proposed system with JPEG
	Standard JPEG	Modified MHT Scheme	
Lena (256×256)	79789	81989	-0.25
Mandril (512×512)	326560	325617	0.29
Cameraman (512×512)	307895	310062	-0.70

4.2. Fingerprinting

In the proposed system, the data can be partially decrypted even without the use of the partial decryption key k_j for each user. Figure 6 shows the partially decrypted Lena images. Figure 6(a) & (b) shows the partially decrypted images corresponding to images where partial encryption of the DCT coefficient values 100 to 150 and 100 to 200 respectively are performed. Since, the partial encryption is provided in the DCT domain, the partially decrypted image has its effect throughout the image as shown in Figure 6.

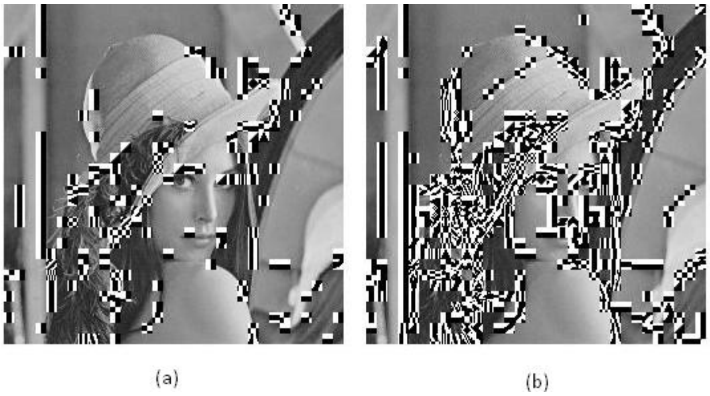

Figure 6. PSNR – Partially decrypted images

If the key for partial encryption k_f is a 32-bit key with IEEE representation instead of 8-bit key, the overall key size can be increased. Figure 7 shows the graph between PSNR and perception coefficient (α). As the value of 'α' increases, PSNR decreases and hence partially decrypted image reveals only lesser information. Hence the peak signal to noise ratio decreases as observed from the graph. As explained, the DCT coefficients are modified at the transmitter for JFD, which requires a key. Here a brief analysis is provided to explain JFD.

Key at transmitter (for JFD): 100001.1000111101011100

User No: 89

Key for user (for JFD): 111100.0100001010001111

Figure 8 shows the original and fingerprinted images and corresponding histograms for a user id of 89 and perception coefficient of 0.3. Since, the fingerprint embedding is performed in the transform domain, the fingerprint is distributed throughout the image. In order to make the proposed system collusion resistant, any anti-collusion codes in the fingerprint embedding stage can be chosen.

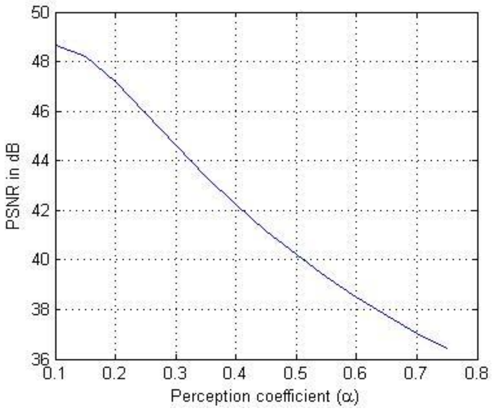

Figure 7. Perception coefficient versus PSNR

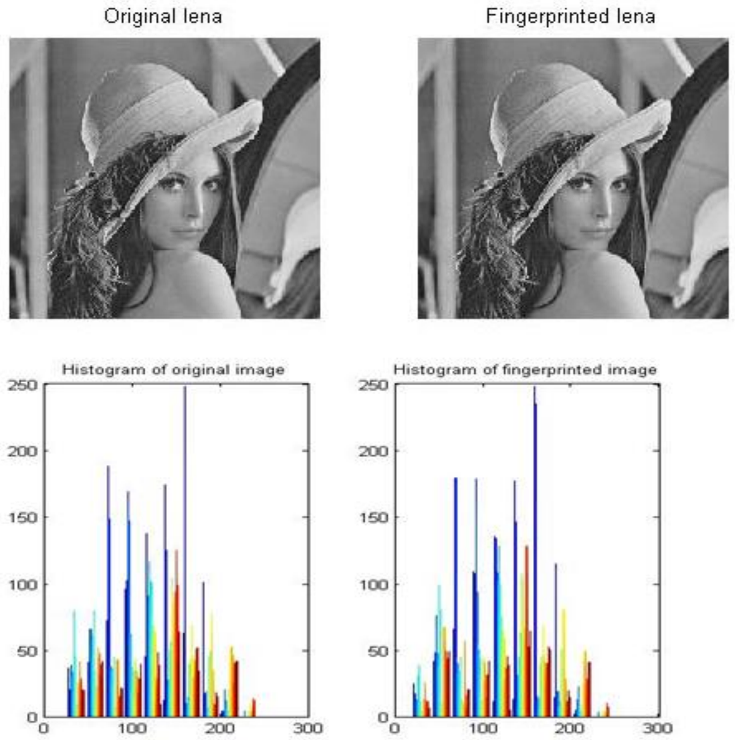

Figure 8. Original and Fingerprinted Images

4.3. Cryptanalysis

In [11], it is proved that the MHT based encryption system is vulnerable to known plaintext attack, and ciphertext only attack. But, due to the presence of blockwise shuffling of DCT image as an additional encryption stage prior to the MHT stage, the proposed system is capable of resisting against these types of attacks. This is based on the fact that the block shuffling of the DCT image destroys the correspondence between the plaintexts and ciphertexts.

4.3.1. Known plaintext attack: In known-plaintext attack (KPA), the attacker has samples of both the plaintext and its ciphertext and is at liberty to make use of them to reveal further secret information such as secret keys and code books. Since the spatial relationship between the plaintext and the corresponding ciphertext are lost due to block shuffling stage, for an attacker the direct mapping of known plaintext and ciphertext is possible. Hence the known plaintext attack is irrelevant here. The output obtained after applying the known plaintext attack is shown in Figure 9.

4.3.2. Ciphertext-only attack: Cipher text-only attack (COA) or known cipher text attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. The attack is completely successful if the corresponding plaintexts can be deduced or even better the key. The ciphertext only attack can be considered as the special case of known plaintext attack. This is because of the fact that the attacker has maximum information about the ciphertext-plaintext. Thus, a system, which is capable of resisting known plaintext attack can withstand against ciphertext only attack.

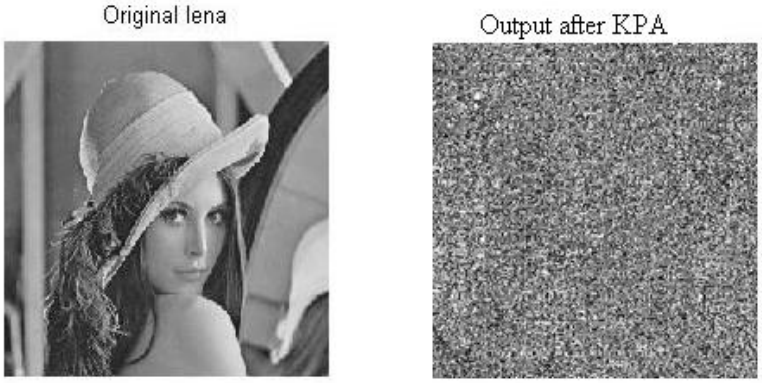

Figure 9. Output obtained after KPA

4.3.3. Brute force attack: Brute force attack is an exhaustive key search strategy whereby, the attacker tries out all the possible key combinations. In general for an n-bit encryption key, the brute force attacker will be able to deduce the key in $2^{(n-1)}$ operations. For analysis, we considered standard Lena image of size 512×512, which was divided into the blocks of size 8×8. The chaotic system is run to make a pseudorandom 8-bit integer array of size 4096. By using these 4096 random integers, it is possible to shuffle 4096 blocks of the image. A 16-bit key for the chaotic map serves this operation. It has been proved that the system behaves chaotically if the value of $\mu > 3.5699$. Also, an 8-bit key is used in the partial encryption stage for JFD. Thus the total key size is $(16 + 8+8) = 32$. On an average $2^{32}/2 = 2^{31}$ operations are required to find out the correct key. In image processing applications, this much of operations account for very large number. Thus, it is proved that the proposed system can withstand brute force attack.

5. Conclusion

In this paper, the security issues of MHT based multimedia encryption technique is analyzed and is found that it is vulnerable to several forms of attacks. To improve the security, block shuffling of the transformed data is performed based on a chaotic map prior to the MHT stage. The block shuffling of transformed data alters the relationship between plaintexts and corresponding ciphertexts. Since the block shuffling is performed in the transform domain, the compression performance of the proposed system is not affected and provides a comparable compression performance as that of the MHT based system. Moreover, the chaotic map based block shuffling ensures simple structure and low implementation cost with marginal increase in the system complexity. To ensure the data security after decryption, joint fingerprinting and decryption scheme is provided with the modified version of MHT based encryption system, so that the proposed system can prevent the illegal redistribution of data, maintaining the copyright protection. The proposed system is tested against various types of attacks and found that is resistant against the same. Further enhancement in the security of the proposed system can be obtained by increasing the key size by providing higher bit representation for the chaotic map and the partial encryption key. Moreover, usage of good anti-collusion codes will create collusion resistant fingerprints.

References

[1] Y. Mao and M. Wu, "A joint signal processing and cryptographic approach to multimedia encryption", IEEE Trans. Image Processing, vol. 15, no. 7, **(2006)**.

[2] S.-W. Sun, C. -S. Lu and P. -C. Chang, "AACS-compatible multimedia joint encryption and fingerprinting: Security issues and some solutions", J. Signal Processing: Image Communication, vol. 23, **(2008)**.

[3] R. Bose and S. Pathak, "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system", IEEE Trans. Circuits and Systems, vol. 53, no. 4, **(2006)**.

[4] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramchandran, "On compressing encrypted data", IEEE Trans. Signal Processing, vol. 52, no. 10, **(2004)**.

[5] C.-P. Wu and J. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems", IEEE Trans. Multimedia, vol. 7, no. 5, **(2005)**.

[6] J. Wen, H. Kim and J. D. Villasenor, "Binary arithmetic coding with key-based interval splitting", IEEE Signal Processing Letters, vol. 13, **(2006)**.

[7] M. Grangetto, E. Magli and G. Olmo, "Multimedia Selective Encryption by Means of Randomized Arithmetic Coding", IEEE Trans. Multimedia, vol. 8, no. 5, **(2006)**.

[8] P. W. Moo and X. Wu, "Resynchronization properties of arithmetic coding", in Proc. IEEE Int. Conf. Image Processing, **(1999)**.

[9] J. Zhou, Z. Liang, Y. Chen and O. C. Au, "Security analysis of multimedia encryption schemes based on multiple Huffman table", IEEE Signal Processing Letters, vol. 14, no. 3, **(2007)**.

[10] G. Jakimoski and K. P. Subhalakshmi, "Cryptanalysis of Some Multimedia Encryption Schemes", IEEE Trans. Multimedia, vol. 10, no. 3, **(2008)**.

[11] Q. Zhou, K. -w. Wong, X. Liao and Y. Hu, "On the security of multiple Huffman table based encryption", J. Vis. Commn. Image R., vol. 22, no. 1, **(2011)**.

[12] D. Kundur and K. Karthik, "Video Fingerprinting and Encryption Principles for Digital Rights Management", Proc. IEEE, vol. 92, no. 6, **(2004)**.

[13] M. Wu, W. Trappe, Z. J. Wang and K. J. R. Liu, "Collusion- Resistant Fingerprinting for Multimedia", IEEE Signal Proc. Mag., **(2003)**.

[14] H .V. Zhao and K. J. R. Liu, "Fingerprint Multicast in Secure Video Fingerprinting", IEEE Trans. Image Processing, vol. 15, no. 1, **(2006)**.

[15] J. -C. Yen and J. -I. Guo, "A new chaotic key-based design for image encryption and decryption", Proc. IEEE Int. Conf. Circuits and Systems, Processing, vol. 4, **(2000)**, pp. 49-52.

[16] H. -C. Chen and J. -C. Yen, "A new cryptography system and its VLSI realization", Journal of Systems Architecture, vol. 49, **(2003)**, pp. 355-367.

Authors

Sudhish N George received B.Tech degree in Electronics & Communication Engineering from MA College of Engineering, Kothamangalam (MG University, India) in 2004 and M.Tech degree from College of Engineering, Thiruvananthapuram in 2007. Currently, he is working as Assistant Professor in the department of Electronics & Communication Engineering, National Institute of Technology, Calicut , India from 2010 onwards. He is pursuing his PhD in Multimedia Security. His current interests include Signal Processing and Cryptography.

Arun Raj R received B.Tech degree in Electronics & Communication Engineering from Rajeev Gandhi Institute of Technology, Kottayam (MG University, India) in 2010 and M.Tech degree from National Institute of Technology, Calicut in 2012. He is currently working as Associate Engineer at Renesas Mobile Corporation, Bagalore, India. His current interests signal processing and wireless communication.

Deepthi P P received B.Tech degree in Electronics & Communication Engineering from NSS College of Engineering, Palakkad (Calicut University) in 1991, M.Tech degree from Indian Institute of Science, Bangalore in 1997 and PhD from National Instiute of Technolgy, Calicut in 2009 in the field of secure communication. She has been working as faculty in institutions under IHRD, Thiruvanthapuram, Kerala, India from 1992 to 2001. She is working as faculty in the department of Electronics & Communication Engineering, National Institute of Technology, Calicut from 2001 onwards. Currently she is working as Associate Professor. Her current interests include Cryptography, Signal Processing with Security Applications, Information Theory and Coding Theory.