International Journal of Computer Applications (0975 - 8887)
Volume 61 - No. 17, January 2013

An Efficient Multimedia DRM Technique using Secure Arithmetic Coding

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

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

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

ABSTRACT

The digital rights management (DRM) techniques are very important in the fields of multimedia security. The major areas of multimedia data security includes secrecy, ownership protection and traitor tracing. Even though, a number of encryption techniques were developed for multimedia encryption, most of them are vulnerable to several types of attacks. Hence, an encryption system having better security with minimal level of system complexity is an important requirement in multimedia security. In this paper, the cryptanalysis of two arithmetic coding based encryption techniques (randomized arithmetic coding(RAC) and chaotic binary arithmetic coding(CBAC))were proposed and proved that these schemes are vulnerable to known-plaintext attack. Then, a modified secure arithmetic coding based encryption system by providing block-wise shuffling of DCT matrix prior to the CBAC stage (block-shuffled CBAC)is proposed to improve the overall security of the system. In order to provide content protection after decryption for the proposed scheme, the joint fingerprinting and decryption (JFD) technique is provided at the receiver stage. Finally, this idea of image encryption has been extended to video (H.264 coding standard). Here, the work is based on a correlation preserving sorting algorithm whereby a comparable compression performance is obtained in addition to the high level of security. The proposed systems are tested against various types of attacks and it has been proved that these methods are able to withstand various types of attacks with good compression performance and minimal level of increase in system complexity.

Keywords:

Digital Rights Management, Chaotic-based Encryption, Secure Arithmetic Coding, Joint Fingerprinting and Decryption

1. INTRODUCTION

The rapid development of multimedia techniques enable more powerful processing and transmission of multimedia data in the recent years. Hence, the chances for unauthorized usage of multimedia data are increased tremendously. Protection of multimedia data from unauthorized access and illegal distribution are dominant research areas in the field of Digital Rights Management (DRM) system. Thus, better encryption, conditional access, copyright protection and traitor tracing are the major objectives of DRM system. Since, the size of the multimedia data is large and multimedia data is non i.i.d., the use of conventional encryption standards like DES, AES, RSA etc are not suitable for multimedia encryption [1],[2],[11]. Moreover, due to the introduction of delay, block based encryption techniques are less suited for real time applications. Generally, the encryption before the entropy coding/compression stage changes the statistical properties of the data resulting in reduced compression performance. Due to the limited bandwidth, it is not possible to make any compromise in the compression performance of the multimedia system. The encryption in the encoded bit-stream after compression may destroy the structure and syntax of coded bit-stream [8]. These structures enable the processing like, bandwidth adaptation, unequal error protection and random access in intermediate network links.

Thus, the most suitable domain for multimedia encryption is the entropy coding stage, where integration of encryption with entropy coding can be performed. Hence the joint encryption and compression of multimedia data is formulated in last decades. A number of methods were proposed to perform the encryption at the entropy coding stage. Depending on the different multimedia standards, the entropy coding stage may be either arithmetic coding or Huffman coding. The image and video coding standards like JPEG, MPEG-2, H.263 etc. rely on Huffman coding, whereas, comparatively newer compression standards like, JPEG2000 and H.264 use arithmetic coding as its entropy coding stage. The most well known approaches for joint compression and encryption are multiple Huffman tables (MHT)[17], arithmetic coding with key-based interval splitting (KSAC)[6],[15] and randomized arithmetic coding (RAC)[2].

Even though, these encryption methods provide better compression and less complexity of operation, most of them are vulnerable to several types of attacks. In [4], Jakimoski *et.al.* proved that the MHT based encryption system is vulnerable to known-plaintext attacks. In [21], the authors analysed the security of MHT based encryption scheme and suggested that multiple Huffman tables should be carefully selected to avoid the weak keys problem. Also, Zhou *et.al.* theoretically proved that same system is not secure against chosen-plaintext attack, known-plaintext attack and ciphertext only attack[22]. In [4], it is proved that KSAC method is also vulnerable to low complexity known- and/or chosen- plaintext attacks. In [20], it is proved that KSAC is less resistant against adaptive chosen-ciphertext attack. In [5], Katti *et.al.* proved the insecurity of RAC method over chosen-ciphertext attack and Jakimoski *et.al.* pointed out

some drawbacks of the same in [17]. In [9], a chaotic binary arithmetic coder (CBAC) for video compression and encryption has been proposed and the authors analysed the security of the system and suggested some modification to the system to provide better security. Thus, it is concluded that even though, the proposed methods have less resource complexity and provides better compression performance, these methods are not secure against various types of attacks. Since, the newer multimedia compression standards like JPEG 2000 and H.264 are using arithmetic coding as its entropy coding stage[16], arithmetic coding based encryption techniques have been taken for the discussion.
Like encryption, the authentication is also a challenging field of research in DRM system. The authentication systems provide entity authentication, data authentication, non-repudiation and key authentication. Generally, watermarks are embedded in the original data for copyright protection. Depending on application different types of watermarks were proposed in literature. In order to protect the multimedia content after decryption from unauthorized dissemination by the service provider/end user, each end user/service provider copy should be uniquely identified by embedding unique ID (fingerprint) in each copy[7]. Since, the joint fingerprinting and decryption (JFD) technique provides lesser system complexity, better performance in real time applications and resistant against various types of collusion attacks, JFD scheme is the most suitable technique to provide data authentication[7]-[12]. Thus, a multimedia system with better security and robust fingerprints in each user's copy is a most promising system in the fields of DRM system.
Most of the image encryption techniques can be extended to video. The challenge behind video encryption lies in the spatial correlation of adjacent frames in a video. In order to achieve encryption without compromising compression, one has to consider this spatial correlation of frames. In [10], Soceck *et.al.* introduced a concept of correlation preserving video encryption algorithm based on sorting permutation, where the authors proposed to permute the current frame with a specific sorting permutation of a previous frame. Even though, their proposed methodology, encrypt the video content before the compression stage, the authors claim that their method provides comparable compression ratio.
The rest of this paper is organized as follows. Section 2 introduces the basic concepts of RAC, CBAC, JFD and digital video encryption based on correlation-preserving permutations. Cryptanalysis of CBAC/RAC schemes are explained in section 3. In section 4, a method for improving the security for RAC and CBAC is proposed with an additional feature of JFD. Taken into the consideration the advantages of the proposed system, the idea is extended into video by incorporating it into video encryption based on correlation preserving permutation, which is described in section 5. The paper concludes in section 6.

2. PRELIMINARIES

TThis section briefly explains the basic concepts of randomized arithmetic coding, chaotic binary arithmetic coding, joint source channel coding and joint fingerprinting and decryption.

2.1 Randomized Arithmetic Coding

The classical arithmetic coding shows very poor resynchronization capabilities. Hence, any decoding error in the AC system will not allow multimedia data to be decoded properly[2]. Thus, introduction of some decoding errors forcefully in the classical arithmetic coder causes difficulty in rendering the data without knowing the decoding key. The RAC based encryption rely on this principle, where swapping the intervals in the classical arithmetic coder is performed based on a random sequence. The algorithm for N binary symbols $(b_0, b_1, ..., b_{N-1})$ is given below[2]-[4].
For $i = 0 : N - 1$
Generate a random bit r_i using pseudorandom bit generator;
If $r_i = 1$, select the order [LPS, MPS] to encode b_i
else, select the order [MPS, LPS] to encode b_i
where, LPS and MPS represent the least probable symbol and most probable symbol respectively. The decoder should use the same random sequence to decode the data correctly.

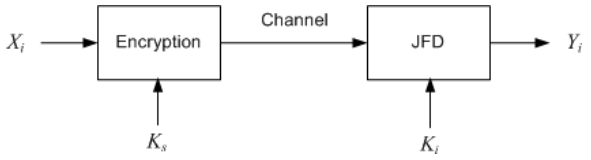


Fig. 1. Simplified block diagram of JFD

2.2 Chaotic Binary Arithmetic Coding

In [9], Pande *et.al.* presented binary arithmetic coding (BAC) in terms of skewed binary map and described seven other possible binary maps which give Shannon optimal performance. They proposed a randomization in the coding structure by chosing a binary map among these eight maps based on a chaotic key without affecting the coding efficiency. Generalizing, it is possible to write the set of encoding equations as,

$$x = \begin{cases} m_1 y + b_1, & \text{when, 0} \\ m_2 y + b_2, & \text{when, 1} \end{cases}$$

The decoding equations are given as,

$$y = \begin{cases} n_1 x + c_1, & \text{when, x} \leq k \\ n_2 x + c_2, & \text{when, x} > \text{k} \end{cases}$$

$$Decode \begin{cases} 0, & \text{when, x} \in [i_1, i_2] \\ 1, & \text{when, x} \in [i_3, i_4] \end{cases}$$

where, m, n, b and c values determine the slope of the binary map. The values of m_1, m_2, b_1, b_2, n_1, n_2, c_1, c_2, i_1, i_2, i_3 and i_4 for different binary maps are given in [9]. RAC can be considered as a special case of CBAC[9]. In that paper, the authors have done the cryptanalysis of the proposed system and suggested some modification to the system to improve the security of the overall system.

2.3 Joint Fingerprinting and Decryption

In [7], Kundur *et.al.* proposed a method for joint fingerprinting and decryption of video. The basic idea is to partially decrypt the multimedia ciphertext and the un-decrypted ciphertext imitates multimedia fingerprint embedding. In JFD, the encryption is done using a global key K_s, whereas a unique key K_i is disributed to each user to decrypt the data. 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 give the information carried by the fingerprint. It can be mathematically represented as, $H(f_i) = H(K_s/K_i)$, where $H(f_i)$ is the entropy of the fingerprint for user i. The block diagram for JFD architecture is shown in Fig. 1.
From the multimedia data (image or video), initially, the perceptually relevant components X are extracted. It is then selectively encrypted with a global key K_s. Then, the resultant encrypted multimedia content Y is given to the user through any distribution channel. In the receiver section, for each receiver, unique keys K_i are provided. The receivers do not have the knowledge

about the global key K_s. Generally, the correlation between decryption and encryption keys derives the fingerprint. 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, the coding techniques used to generate fingerprint should make it resistant to collusion attacks. The popular coding techniques are orthogonal fingerprinting and coded fingerprinting using BIBD techniques[13],[14],[18],[19].

2.4 Video Encryption based on Sorting Permutation

In [10], Socek *et.al.* proposed a method to encrypt the digital video based on correlation preserving permutations. This method is based on the concept that when a sorting permutation of the previous frame acts on the current frame, it produces an "almost sorted" frame. Moreover, the sorted as well as almost sorted frames provide good compression performance, even more compression than the original source frames in some situations. From the initial frame, it is possible to calculate the initial permutation and the next frames can be converted into almost sorted frames. In the receiver side, if the initial frame is received safely, it is possible to recover sorting permutation and it can be used to recover original frames from the almost sorted frames.
Fig. 2 represents the simplified block diagram of this system. Here I_i represents the frames of the input video where i varies from 1 to m. σ represents the index matrix for sorting. S represents secure channel whereas R represents the normal insecure channel.

3. PROPOSED METHOD: CRYPTANALYSIS OF CBAC/RAC

This section proposes to analyse the security aspects of RAC/CBAC. Brute force attack and known-plaintext attack (KPA)have been performed on CBAC to validate the effectiveness of this method. All types of cryptanalysis performed on CBAC apply to RAC since RAC can be considered as a special case of CBAC. Moreover, the known-plaintext attack on CBAC with key update is performed.

3.1 Known-Plaintext Attack

Since each pixel is encrypted with the same key pattern, it becomes logical to use the known-plaintext attack. It is assumed that one plain pixel and the corresponding cipher pixel is known. For a key of length 24 bits, there will be 8 numbers (grouping by 3). For these 8 numbers, 8! = 40,320 combinations are possible. Among these 40,320 combinations, there will be some other key combination that can give the same output. Even in the worse case situation only 40320 combinations needed to be checked. Thus, CBAC alone proves to be highly vulnerable to known-plaintext attack. Vulnerability of CBAC towards KPA indicates the susceptibility of RAC towards attack as RAC is a special case of CBAC. The decrypted lena image using KPA is shown in Fig.3.

3.2 Known-Plaintext Attack on CBAC with key update

In [9], Pande *et.al.* proposed a modified method of CBAC. In this modified scheme, the authors suggested to update the key of the CBAC encoder for every iteration by xoring the output bits with the key as shown in Fig. 4. From the inspection itself, it is possible to conclude that this modified method is also vulnerable to some sort of cryptanalysis. It can be mathematically expressed as follows.

Fig. 3. Known-plaintext attack on CBAC image

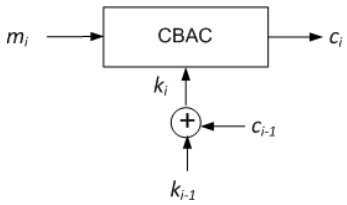


Fig. 4. CBAC with key update

(a) (b)

Fig. 5. (a) Input image (b) Output Image after KPA on CBAC image with key update

(1) Initially assume that input message bit m_i and corresponding ciphertext c_i are known (according the fundamental principle of KPA).
(2) Find key k_{i-1} using m_i and c_i by applying the techniques of KPA.
(3) Since $k_i = k_{i-1} \oplus c_i$, deduce k_i from k_{i-1} and c_i.

Since the key is obtained, all the remaining procedures of KPA are same. It is just a matter of performing this xor operation in a loop. Fig. 5 represents the results of cryptanalysis of CBAC with key update.

4. PROPOSED SYSTEM: BLOCK-SHUFFLED SECURE ARITHMETIC CODING SCHEME FOR IMAGE ENCRYPTION

As proven from the cryptanalysis, CBAC/RAC is susceptible to known-plaintext attack. Hence it became necessary to device a method that could combine all the advantages of CBAC/RAC and negate the vulnerability of the same against all forms of attack. In the proposed system, block shuffling of DCT matrix prior to the entropy coding stage is performed to improve the security. This section discusses the details of the proposed system.

4.1 Transmitter Stage

The main purpose of the block shuffling of DCT matrix stage is to make the system stable against all attacks. Known-plaintext attack can be easily avoided by inserting a shuffling algorithm

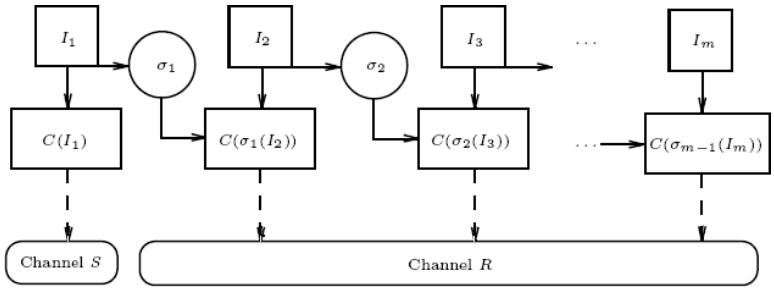


Fig. 2. Simplified block diagram of video encryption based on correlation preserving permutation[10]

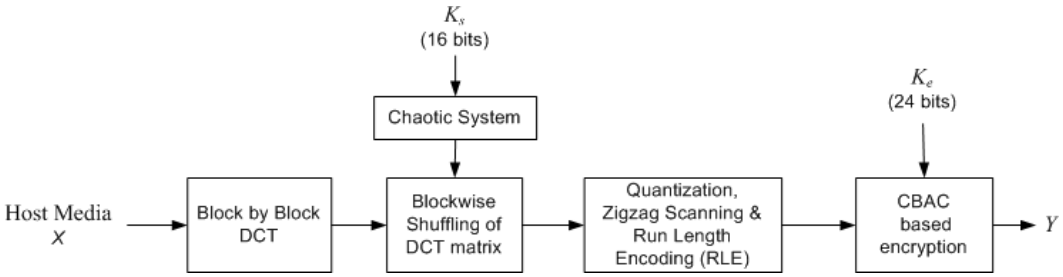


Fig. 6. Transmitter Stage

anywhere prior to entropy coding. The insertion of shuffling algorithm in the spatial domain reduces the compression rate as any change in spatial domain can affect the spatial redundancy of the data. Hence a block-wise shuffling at the DCT domain is provided. Since shuffling is performed block-wise the effect on reduction in compression is negligible. The transmitter stage of the proposed system is shown in Fig. 6.

4.1.1 Chaotic key based block shuffling of DCT matrix. Like standard JPEG compression, the image is divided into 8×8 blocks, followed by block by block DCT. The block-wise shuffling is performed with the help of a chaotic system. 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 [3],[23].

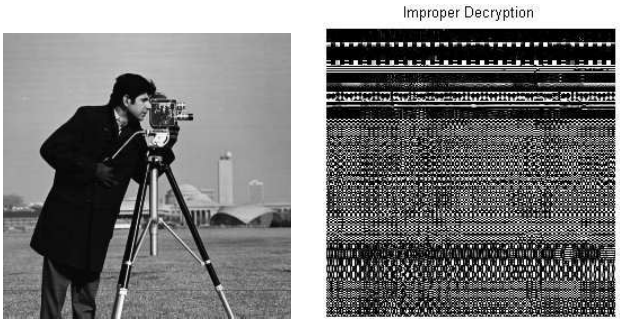
$$x(n+1) = \mu x(n)(1 - x(n)) \quad (1)$$

It has been experimentally proved that the system behaves chaotically if the value of $\mu > 3.5699$. This chaotic system is run to make a chaotic sequence $x(i)$ for i varying from 0 to $(MN/8) - 1$. It is then grouped into 8 bits to form an integer so that a pseudo random array of $MN/64$ integers is formed. By avoiding the repeating elements, it is possible to form an array of length 256. This array can be taken as an index to shuffle the columns of input DCT matrix. This system is a well encrypted system providing good compression by suitably selecting the quantization matrix. The key (K_s) size is chosen as 16-bit.

4.1.2 Joint encryption using CBAC scheme. The entropy coding stage used in the proposed system is the CBAC encoding as explained in [9]. For each symbol input, we are using all the 8 combinations as specified in [9]. Each combination can be represented using 3 bits. Hence the key (K_s) used for this section is having a size of 24 bits.Thus, this stage can provide encryption and compression simultaneously.

4.2 Receiver Stage

The decryption at the receiver end is exactly the reverse operation that was performed at the transmitter. The block diagram of receiver section is shown in Fig. 7. The 24-bit K_e is used to decrypt the multimedia data in the entropy decoding stage. Since,



(a) (b)

Fig. 8. (a) Input Image (b)Improper Decryption (without decrypting the block shuffling stage)

three more decryption stages are present in the system; the receiver cannot retrieve the data from this simple decryption stage. The shuffled DCT matrix is converted back into its original form with the 16-bit key K_s. After inverse DCT, joint fingerprinting and decryption has been implemented. The reconstructed image without decrypting the block shuffling stage is shown in Fig. 8

4.2.1 JFD for image authentication. In order to restrict the illegal usage of the multimedia data after decryption, it is proposed to include joint fingerprinting and decryption in the decoding/decryption stage. To implement joint fingerprinting and decryption, one of the disadvantages of the CBAC/RAC encryption system (attack point of view) is used. As explained earlier, CBAC/RAC system has multiple key facility for decrypting. Thus, it is possible to distribute the same multimedia data to multiple users with unique key. During decryption this key gets embedded at the output image by any of the suitable watermark embedding technique.

4.3 Results and Discussions

This section discusses results after implementing the proposed system. This includes compression analysis where the perceptual quality of the image is compared at different compression levels. This section also deals with the authentication part where

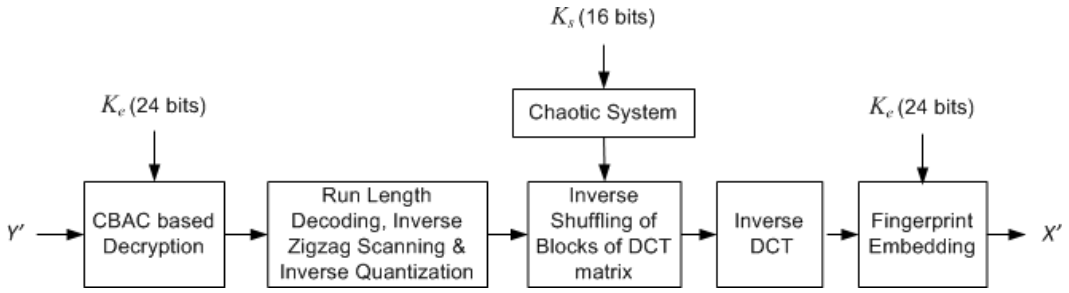


Fig. 7. Receiver Stage

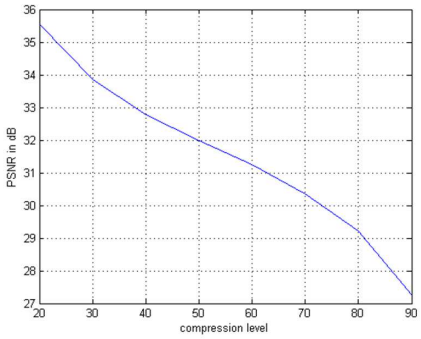


Fig. 10. Compression Level versus PSNR

the input image and the fingerprinted image in terms of the perceptual quality are compared.

4.3.1 Compression analysis. The main cause of compression during the JPEG coding depends on the quantisation stage. The standard quantisation matrix is chosen to provide a compression level of 50. Suitable scaling of the quantisation matrix allows the compression level to vary from 0 to 100. Compression level 0 corresponds to zero compression in the sense that the quantisation matrix that is chosen to quantise is a unit matrix. Fig. 9(a) shows the output image at a compression level of 20. Fig. 9(b) depicts the output image at compression level 50 and Fig. 9(c) shows the one at a compression level of 90.
It becomes obvious that the peak signal to noise ratio (PSNR) of the output decreases as compression level goes from 0 to 100. In addition to perceptual measure it is necessary to validate this statement with some mathematical measures. The PSNR can be calculated as,

$$PSNR = 10log_{10}\left(MAX_I^2/MSE\right) \tag{2}$$

where, MAX_I is the maximum possible pixel value of the image. The MSE can be calculated as,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I\left(i,j\right) - K\left(i,j\right)\right)^2 \tag{3}$$

for an $M \times N$ image, where $I(i,j)$ and $K(i,j)$ represent the original and reconstructed image pixels respectively. The PSNR was plotted against the compression level as shown in figure 10. From the graph it is clear that as compression level increases PSNR decreases.

4.3.2 Fingerprinting. One of the prime requirements in fingerprinting is that the fingerprinted image should be perceptually similar to the original image. In the proposed system, the 24-bit for the decryption of the entropy coding stage is embedded as the fingerprint in the reconstructed image. Fig. 11 shows the input image and the fingerprinted image. Even after embedding

Fig. 11. Input Image and the Fingerprinted Image

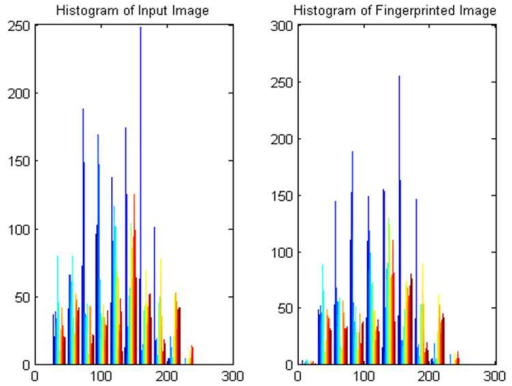


Fig. 12. Histograms of the Input image and the Fingerprinted image

the fingerprint image remains perceptually same. Histograms of the two images are shown in Fig. 12 which clearly show that the fingerprint has been embedded.

4.3.3 Cryptanalysis. Among, all types attacks, if an encryption system can overcome known-plaintext attack, then that encryption scheme is considered to be secure against other types of attack. This is because of the fact that in known-plaintext attack, the attacker has access to maximum amount of information. The proposed system was subjected to brute force attack and known-plaintext attack.

Brute Force attack

Brute force attack is that type of attack done where all the possible combinations of the key are tried out to find out the correct match. An important point to note regarding CBAC/RAC from an attacker point of view is the multiple key decrypting facility. The ciphertext can be decrypted using different sets of keys. Two maps from the eight possible maps give the correct reconstruction for a single bit. For N bit message, the total key space is 2^{3N} and out of these 2^{3N} combinations 2^N choices can correctly de-

(a) (b) (c)

Fig. 9. (a) Output Image at a compression level of 20 (b) Output Image at a compression level of 50 (c)Output Image at a compression level of 90

crypt the data. Hence, an attacker needs to try out less number of keys. The below mentioned analysis on Brute force attack has been done.

(1) For an n-bit representation of images, the key used is having $n \times 3 = 3n$ bit length and the total key space is 2^{3n}.
(2) Out of these 2^{3n} combinations, 2^n are correct decryption keys.
(3) If the value of n is 8, 2^8 combinations out of 2^{24} combinations will give the correct key. Thus the probability of getting the correct key is 2^{-16}.

Hence, the probability of finding out the correct key is higher and the computational complexity of the attacker to track the correct decryption key is much lower.
Thus, with the entropy coding based encryption alone, the system is prone to brute force attack. But, the proposed system consists of block shuffling of DCT matrix prior to the entropy coding stage. Thus, the size of the key space is going to increase. Since, the proposed system has a 40 bit key (24+16), it requires $2^{40}/2 = 2^{39}$ operations on an average to find out the key. The brute force attack on individual encryption stages will not create any reduction in the complexity of brute force attack in this scenario. Hence, it is proved that the proposed system is stable against brute force attack.

Known-Plaintext Attack (KPA)

As proved in section 3.1, CBAC stage alone is vulnerable to known-plaintext attack. Even in the worse case scenario, only 8! = 40,320 operations (for 24-bit key) are to be checked to find out the correct key. But in the proposed method, block-wise shuffling of DCT matrix is provided before CBAC based encoding. Each of these stages alone in an encryption system is vulnerable to KPA. But, when both of these stages are combined in a system, for the known message input and corresponding ciphertext, it is not possible to obtain the correct decryption key. The block shuffling algorithm incorporated at the DCT domain is responsible for the failure of KPA since it alters the spatial arrangement of available plaintext and the ciphertext. Hence, the proposed system is resistant to known plaintext attack.

5. PROPOSED SYSTEM: MODIFIED VIDEO ENCRYPTION BASED ON CORRELATION PRESERVING PERMUTATION

The main drawback of correlation preserving video permutation proposed by Socek *et.al.*[10] is the unpredictable spatial correlation of frames in a video. Moreover, the author's haven't mentioned about the secure channel through which the initial frame has to be transmitted. To overcome the first drawback, it is proposed to compute the correlation coefficient between successive frames and if this parameter is greater than a specified threshold then go with the earlier case, else transmit the next frame through a secure channel. For experiments, the H.264 video standard is considered[16]. The first frame as well as the frames having a correlation coefficient less than the threshold are encrypted using block-shuffled secure arithmetic coding and transmitted. If the correlation coefficient is greater than the threshold value, the almost sorted frames are encoded using the video coding standard(here it is H.264). The correlation coefficient that is used for experiments is the average intensity of the frame. The flowchart of the proposed system is shown in Fig. 13. The analysis of the proposed system is given in the coming subsections.

Table 1. Compression analysis of proposed encryption system versus H.264 encoding

Input Video	Raw video	Sorted video
Suzie	237 KB	231 KB
Coastguard	1200 KB	1027 KB
Cat	108 KB	102 KB

5.1 Compression Analysis

H.264 encoding is performed on the sorted video. Table 5.1 compares raw video compression with that of sorted video compression for various standard videos. The various standard videos chosen for the experiments were of different nature with reference to the rate at which frames vary. It can be clearly seen that the sorted video coding provides better compression than the original video coding with some sort of increase in resource complexity.

5.2 Cryptanalysis

During the implementation of the above method a very interesting fact was noticed. Consider a video 'X' having a sorting matrix 'A' and sorted matrix 'M'. Consider another video 'Y' having a sorting matrix 'B' and sorted matrix 'N'. Intuitively, if 'X' and 'Y' are correlated sorting 'M' based on 'B' should yield 'X' but experimentally it yielded 'Y'. This concludes the fact that sorting order has higher significance. The attacker might have an idea of what type of video is being transmitted. It can be checked by using another video of same type to yield the sorting matrix proves to be valiant in this case. Thus, it can be concluded that the correlation preserving video permutation is highly secure. Fig. 14 (a) and Fig. 14 (b) show the single frames of two similar input videos for performing cryptanalysis. Figure 14 (c) depicts the output frame obtained after performing the cryptanalysis, which proves the real security of the proposed system.

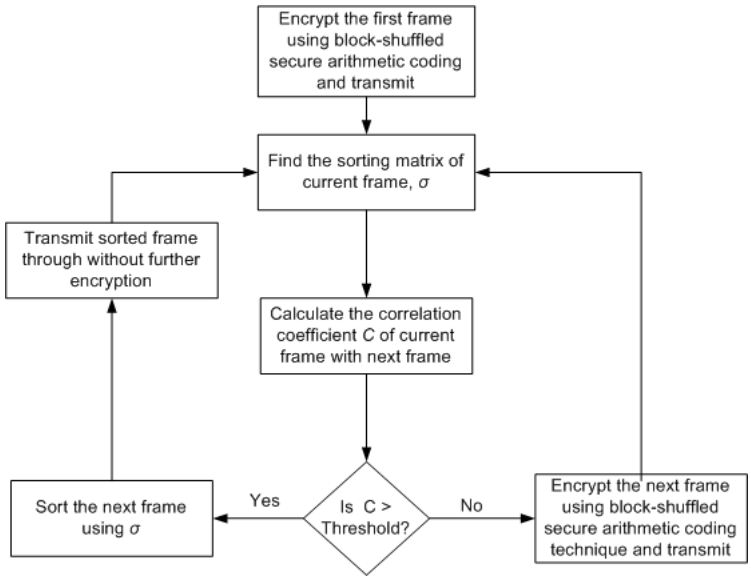


Fig. 13. Flowchart of modified video encryption based on correlation preserving permutation

(a) (b) (c)

Fig. 14. (a) Input frame - 1 of X (b) Input frame - 2 of Y (c)Output frame obtained with sorted matrix of X and sorting matrix of Y

6. CONCLUSION

Since arithmetic coding has been gaining immense attraction recently due to its inclusion in several multimedia standards, analysis of existing arithmetic coding based encryption techniques like RAC, CBAC etc were carried out. From the experiments it can be concluded that that these methods were prone to attacks though they provide good compression. Hence a new system that could prove to provide good compression as well as high security has been proposed. In the proposed system, the block-shuffling of DCT matrix prior to the joint encryption stage in the entropy coding stage is provided. Authentication was another key aspect that has been dealt with. The concept of joint fingerprinting and decoding to validate the truthfulness of the data in the proposed method has been incorporated. From the experimental results, it can be concluded that the proposed method is stable against various types of attacks, give better compression and perceptually similar images after JFD. This idea is extended into video, where the correlation preserving permutation based video encryption is taken into account. It is modified by calculating the correlation coefficient between successive frames. Then, based on the value of correlation coefficient, the frames are encrypted using block-shuffled secure arithmetic scheme or "almost sorted" frames are encoded using standard video coding technique. The above mentioned scheme is also experimentally verified to be stable against various types of attacks and to be capable of providing very good compression performance with minimal increase in resource complexity.

7. REFERENCES

[1] PUB FIPS. 197: advanced encryption standard. *National Inst. of Standards & Tech*, 2001.

[2] M. Grangetto, E. Magli, and G. Olmo. Multimedia selective encryption by means of randomized arithmetic coding. *Multimedia, IEEE Transactions on*, 8(5):905–917, 2006.

[3] J.I. Guo et al. A new chaotic key-based design for image encryption and decryption. In *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, volume 4, pages 49–52. IEEE, 2000.

[4] G. Jakimoski and KP Subbalakshmi. Cryptanalysis of some multimedia encryption schemes. *Multimedia, IEEE Transactions on*, 10(3):330–338, 2008.

[5] R.S. Katti, S.K. Srinivasan, and A. Vosoughi. On the security of randomized arithmetic codes against ciphertext-only attacks. *Information Forensics and Security, IEEE Transactions on*, 6(1):19–27, 2011.

[6] H. Kim, J. Wen, and J.D. Villasenor. Secure arithmetic coding. *Signal Processing, IEEE Transactions on*, 55(5):2263–2272, 2007.

[7] D. Kundur and K. Karthik. Video fingerprinting and encryption principles for digital rights management. *Proceedings of the IEEE*, 92(6):918–932, 2004.

[8] Y. Mao and M. Wu. A joint signal processing and cryptographic approach to multimedia encryption. *Image Processing, IEEE Transactions on*, 15(7):2061–2075, 2006.

[9] A. Pande, J. Zambreno, and P. Mohapatra. Joint video compression and encryption using arithmetic coding and chaos. In *Internet Multimedia Services Architecture and Application (IMSAA), 2010 IEEE 4th International Conference on*, pages 1–6. IEEE, 2010.

[10] D. Socek, S. Magliveras, O. Marques, H. Kalva, B. Furht, et al. Digital video encryption algorithms based on

correlation-preserving permutations. *EURASIP Journal on Information Security*, 2007.

[11] D.E. Standard. Fips pub 46-2. *National Bureau of Standards*, 1993.

[12] S.W. Sun, C.S. Lu, and P.C. Chang. Aacs-compatible multimedia joint encryption and fingerprinting: Security issues and some solutions. *Signal Processing: Image Communication*, 23(3):179–193, 2008.

[13] W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu. Anti-collusion fingerprinting for multimedia. *Signal Processing, IEEE Transactions on*, 51(4):1069–1087, 2003.

[14] Z.J. Wang, M. Wu, H.V. Zhao, W. Trappe, and K.J.R. Liu. Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation. *Image Processing, IEEE Transactions on*, 14(6):804–821, 2005.

[15] J. Wen, H. Kim, and J.D. Villasenor. Binary arithmetic coding with key-based interval splitting. *Signal Processing Letters, IEEE*, 13(2):69–72, 2006.

[16] T. Wiegand, G.J. Sullivan, G. Bjontegaard, and A. Luthra. Overview of the h. 264/avc video coding standard. *Circuits and Systems for Video Technology, IEEE Transactions on*, 13(7):560–576, 2003.

[17] C.P. Wu and C.C.J. Kuo. Design of integrated multimedia compression and encryption systems. *Multimedia, IEEE Transactions on*, 7(5):828–839, 2005.

[18] M. Wu, W. Trappe, Z.J. Wang, and K.J.R. Liu. Collusion-resistant fingerprinting for multimedia. *Signal Processing Magazine, IEEE*, 21(2):15–27, 2004.

[19] H.V. Zhao and K.J.R. Liu. Fingerprint multicast in secure video streaming. *Image Processing, IEEE Transactions on*, 15(1):12–29, 2006.

[20] J. Zhou, O.C. Au, and P.H.W. Wong. Adaptive chosen-ciphertext attack on secure arithmetic coding. *Signal Processing, IEEE Transactions on*, 57(5):1825–1838, 2009.

[21] J. Zhou, Z. Liang, Y. Chen, and O.C. Au. Security analysis of multimedia encryption schemes based on multiple huffman table. *Signal Processing Letters, IEEE*, 14(3):201–204, 2007.

[22] Q. Zhou, K. Wong, X. Liao, and Y. Hu. On the security of multiple huffman table based encryption. *Journal of Visual Communication and Image Representation*, 22(1):85–92, 2011.

[23] Z. Zhu, W. Zhang, K. Wong, and H. Yu. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, 181(6):1171–1186, 2011.