Joint Image Compression and Encryption Based on Alternating Transforms with Quality Control

Peiya Li [#1], Kwok-Tung Lo [*2]

[#] *Department of Electronic and Information Engineering*
The Hong Kong Polytechnic University
Hung Hom, Kowloon, Hong Kong, China
[1] yolanda.peiya@connect.polyu.hk

[*] *Department of Electronic and Information Engineering*
The Hong Kong Polytechnic University
Hung Hom, Kowloon, Hong Kong, China
[2] kwok.tung.lo@polyu.edu.hk

***Abstract*—In this paper, we propose a novel joint image compression and encryption technique where an annoying image can still be recovered even without the encryption key. Our work is based on JPEG standard. By embedding encryption algorithm at the transformation stage, we realize image encryption and compression together with controllable image quality. Instead of using the 8×8 discrete cosine transform (DCT) alone for transformation, we develop new orthogonal transforms by introducing sign-flips into the butterflies of DCT's flow-graph structure, and then employ them alternatively in JPEG's transformation stage according to a secret key. By carefully selecting the butterflies for sign-flipping, we can control the visual quality of the encrypted images. Finally, a detailed security analysis of our proposed encryption algorithm is presented to show its resistance to various attacks, such as cryptographic attack, replacement attack and statistical model-based attack.**

***Index Terms*—Image encryption, orthogonal transforms, security analysis, JPEG standard, quality control.**

I. Introduction

Thanks to the rapid development of multimedia technologies in recent years, many powerful and interesting new applications have been developed for people to share their images in their mobile smart devices through social network platforms such as Facebook and Instagram. In typical use of images,the owners may want to store them for future use or distribute them to the specific people through the Internet which is particularly vulnerable to eavesdropping and intercepting. Therefore, there exists a great demand on secure image storage and transmission. Encryption is one of the common ways to ensure image security.

Unlike text data encryption, image encryption has its unique properties, like large size, real-time processing requirement, thus traditional encryption algorithms, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [1], are not very suitable for image encryption. Considering the fact that compression is a must-do step for most images we see on the Internet, the focus of image security research shifted to integrating image compression process with encryption, for the purpose of reducing encryption and decryption time in image communication and processing. The most popular method for this encryption direction is partial encryption.

In [2], Tang proposed a method to realize partial image encryption by encrypting the DC coefficients with DES and randomly permuting the AC coefficients rather than the standard zigzag scanning order. But this scheme will introduce about 40% loss in the compression efficiency, because the new permutation disrupts the probability distribution of run-lengths, and renders the performance of Huffman tables less than optimal [3]. Later, Shi and Bhargava [4] modified this algorithm to encrypt the sign bit of every DCT coefficient in JPEG, but even without the encryption key, useful image information can be recovered by assigning all DC coefficients to 128 and all AC coefficients to positive [5]. For partial encryption performed after entropy coding, [5] pointed out that it is difficult to distinguish which bits are most important for intelligibility.

In this work, we propose a new joint image compression and encryption method with controllable encryption parameters. The proposed method can achieve a sufficiently high level of security while maintain the good compression performance of JPEG, and it is format compliant to JPEG standard. Using the strategy made in [6] and [7] for perceptual video encryption, we carry out encryption at the transformation stage of JPEG through alternately employing different new orthogonal transforms, generated by sign-flipping strategy, for the 1^{st} and 2^{nd} dimension transformation, according to a predefined security key. Moreover, quality control of the encrypted images is achieved by carefully selecting some of the butterflies at different stages to change while fixing the others. Security analysis of our encryption algorithm is also provided to confirm its persistence to different types of attacks, such as cryptographic attack, replacement attack, and statistical model based attack.

In the rest of the paper, Section II introduces the generation

of new transforms and the performance of our proposed encryption algorithm. Section III describes the way to realize quality control of encrypted images. Section IV shows security analysis results of our encryption scheme. Section V gives a conclusion and presents future research directions.

II. Joint Image Compression and Encryption Based on Alternating Transforms

A. Generation of New Orthogonal Transforms from the Flow-graph of Order-8 DCT

In JPEG, 8×8 DCT is used for transformation, because DCT has proved to be the best transform in terms of the compression ability when the correlation among inter-pixels is strong - which is actually true in most natural pictures. We try to generate new sets of unitary transforms through modifying the flow graph of the 8-point 1-D DCT as shown in Fig. 1. Considering the encryption performance, the coding efficiency of these new generated transforms should be exactly the same to what can be achieved by DCT or just falls slightly. In [6] and [7], they have derived efficient alternative transforms from the flow-graph of DCT by introducing sign-flipping strategy at the same stage, which is equivalent to an extra rotation angle of π. Adopting this method, we can generate many different orthogonal transforms through embedding sign-flips in different butterflies at different stages in Fig. 1.

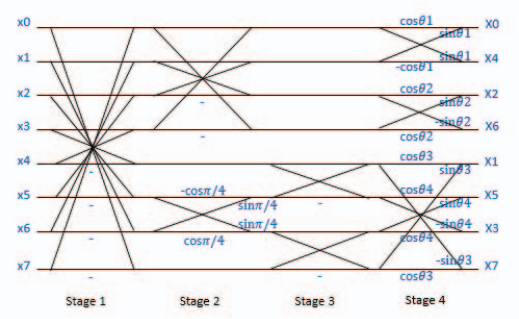

Fig. 1. Flow graph of 8-point (1-D) DCT ($\theta_1 = \pi/4$, $\theta_2 = 3\pi/8$, $\theta_3 = 7\pi/16$, $\theta_4 = 3\pi/16$)

In our work, we do not do sign-flips for the butterflies in Stage-1 and Stage-2, because this will cause big changes in the transform coefficients, which will eventually affect the overall coding efficiency. We only do sign-flips at Stage-3 and Stage-4. Choosing whether to do sign-flips for the two butterflies at Stage-3 or not, we can obtain two different sets of new transforms. The first transform set, called *TS1*, has 16 different transforms which are generated by introducing sign-flips into the four butterflies in Stage-4. The second transform set, called *TS2*, has 64 different transforms that are generated by introducing butterflies into the four butterflies in Stage-4 and the two butterflies in Stage-3.

B. Joint Image Compression and Encryption Using New Transforms Sets

Our joint image compression and encryption scheme can be divided into two parts: 1) random (secret) key generation, and 2) alternating transforms according to the secret key. For the key generation, we use the RC4 algorithm, which turns to be the most commonly-used random key generator [8]. The encryption algorithm can be stated as follows:

Encryption Algorithm

Step 1: Initialize the RC4 key generator by a random 128-bit key;
Step 2: For an input image 8×8 block, do
  Step 2.1: Get 52 bits from the random generator;
  Step 2.2: The first 4 bits are used to select one transform from *TS1* for *all* rows in the 1^{st} dimension;
  Step 2.3: The following 48 bits are used to select one transform from *TS2* for *each* column in the 2^{nd} dimension;
Step 3: Repeat *Step2* until we finish the whole image.

For the decryption algorithm, we just follow JPEG's decoding process by using the corresponding encryption transform sets. In our algorithm, we use the two transform sets together and implement the 1^{st} and 2^{nd} dimension transformation separately, which will change the transformed coefficients in both signs and magnitudes, thus cryptanalyzing images through some sign-flips on the DCT transformed coefficients of the same data block is not feasible. The encryption and compression performance of our encryption algorithm based on the test image 'Lena.tiff' are shown in Fig. 2 and 3 respectively. Performance comparison between our encryption algorithm and the *Algorithm-3* in [6] is also provided. We can observe a large PSNR value drop from Fig. 2 when the encryption key is unknown and only IDCT is used for decryption, which means a good protection ability of our encryption algorithm. For the compression performance shown in Fig. 3, only a small value drop is observed when compared with JPEG standard, and a better compression ability can be seen when compared with the reference's algorithm. Hence, we can conclude that our method can achieve a high level of security without sacrificing too much on the compression ability of the JPEG scheme.

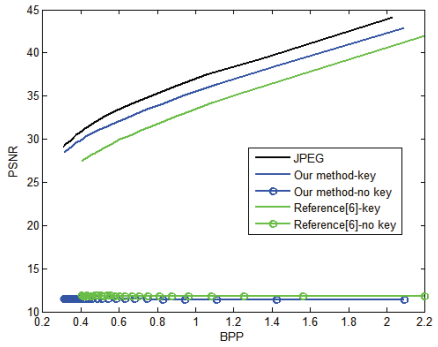

Fig. 2. R-D (rate-distortion) performance for Lena

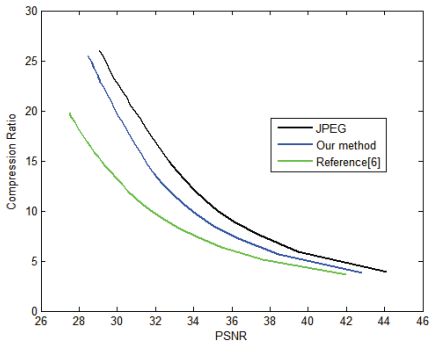

Fig. 3. Compression ratio comparisons for Lena

III. Quality Control of Our Joint Image Compression and Encryption Algorithm

For partial image encryption, an encrypted image with poor visual quality can be obtained without the encryption key. However, for different applications, the visual quality requirement of the encrypted images may be different, thus it is necessary to allow the service provider a chance to control how bad the encrypted image quality will be.

In our encryption scheme, for the two transforms sets, *TS1* and *TS2*, we both introduce sign-flips into the four angles at Stage-4. To achieve image quality control, we can select some of the four angles to change while keeping the others unchanged. Table I has listed the different PSNR performances of various selections of θ_i for encryption. Three images are used for testing. All images used in our experiment are taken from the USC-SIPI image database available on the website "http://sipi.usc.edu/database". We assume that the standard IDCT is used for decryption when the encryption key is unknown.

TABLE I
PSNR Performance of Various Selction of θ_i for Encryption

Image / Angle change	Lena	Resolution chart	Chemical plant
None (a)	33.7991	29.9812	30.6216
Stage-3 (b)	22.6201	14.3639	20.4480
Stage-3 & θ_1	11.6110	5.0427	11.8321
Stage-3 & θ_2	21.7588	11.6614	18.8295
Stage-3 & θ_3	19.9004	12.1566	19.0178
Stage-3 & θ_4	22.9596	13.8221	20.2598
Stage-3 & $\theta_1\theta_2$	11.3679	4.8466	11.7172
Stage-3 & $\theta_1\theta_3$	11.3574	4.9567	11.7888
Stage-3 & $\theta_2\theta_3$ (c)	19.1724	10.7887	17.9032
Stage-3 & $\theta_1\theta_4$	11.4121	4.8865	11.8132
Stage-3 & $\theta_2\theta_4$	21.1732	11.5342	18.6535
Stage-3 & $\theta_3\theta_4$	19.8652	11.6732	18.8287
Stage-3 & $\theta_1\theta_2\theta_3$	11.4745	4.8665	12.1119
Stage-3 & $\theta_1\theta_2\theta_4$	11.4880	4.8523	12.1052
Stage-3 & $\theta_2\theta_3\theta_4$	18.6295	10.3300	17.9818
Stage-3 & $\theta_1\theta_3\theta_4$	11.4535	4.8536	12.0761
Stage-3 & $\theta_1\theta_2\theta_3\theta_4$ (d)	11.5409	4.8483	11.9608

From Table I, it is clearly that among four angles, θ_1 has the biggest influence on the PSNR value, as it controls the DC component of each 8×8 block. In Fig. 4, we present the visual results of the four representative selections in Table I of Lena image. Although these cases all have a PSNR drop, the visual qualities of them are quite different. Image in Case (b) are visually much more pleasant than image in Case (c) and Case (d). Thus, we can choose whether to change θ_1 or not to obtain high or low encryption ability, and change other three angles to make some fine adjustment on the quality of images.

Fig. 4. Encrypted Lena image with different angles change (left-lop: Case (a) in Table I; right-top: Case (b) in Table I; left-bottom: Case (c) in Table I; right-bottom: Case (d) in Table I)

IV. Security Analysis

A. Key Space and Encryption Space

In typical cryptographic attacking methods, ciphertext-only attack is the most realistic and basic one in which attackers can only obtain the encrypted data. One of the common methods for ciphertext-only attack is to try all possible keys in the brute-force manner. In our algorithm, we apply the RC4 key generator with a 128-bit key, thus obtain a 2^{128} key space, which is not feasible for attackers to guess. However, instead of guessing the key we use, attackers can guess the transforms we use for encryption. In our algorithm, a total of 52 sign-flips have been embedded in the various stages of the order-8 DCT flow-graph: 4 in the 1^{st} dimension and 6 for each column in the 2^{nd} dimension (4+6×8=52). If we define the *encryption space* to denote how many sign-flips can be embedded, then the encryption space of each 8×8 block for our algorithm is 2^{52}. Since there will be 1024 blocks with 8×8 size in a 256×256 image, it is not feasible to try all transforms for all blocks.

B. Security against Replacement Attack

Replacement attacks are used to break multimedia encryption algorithms that try to recover the plain media by replacing the encrypted parameter with the unencrypted ones or some others [9]. We recover different encrypted images by assigning all dc coefficients to 128 and all ac coefficients to positive, and the performance is judged by the PSNR value and SSIM

TABLE II
PSNR OF DIFFERENT DECRYPTED IMAGES BY THE DIRECT REPLACEMENT ATTACK

File name	File description	PSNR	SSIM
4.2.04	Girl (Lena)	13.9444	0.0046
5.1.12	Clock	12.4885	-0.0067
5.1.13	Resolution chart	8.6664	0.3121
5.1.14	Chemical plant	14.4466	-0.0006
5.2.08	Couple	14.3298	-0.0272
5.2.09	Aerial	14.6786	0.0086
5.2.10	Stream and bridge	12.6616	0.0013

[10] value shown in Table II. It is clearly that both values of various decrypted image are very low, which means that the direct replacement attack is not feasible.

C. Security against Statistical Model-based Attack

Statistical model-based attack aims to recover the cipher image's intelligibility under the condition of knowing only cipher images. In this attack, the degradation of the cipher image is reduced by using a statistical model [9]. Attackers try to decrypt the cipher image by studying the relationship between plain image and cipher image without knowing the encryption key. Generally, histograms and correlation diagrams of the original image and the encrypted image are two ways to indicate the degree of relationship [11], [12].

Fig. 5 and Fig. 6 show histograms and correlation charts of the original "Aerial.tiff" image and the encrypted image. It can be seen that histogram of the encrypted image have little statistical similarity to histogram of the original image. And for the correlation diagram drawing, we initially identify the neighbourhood of diagonal pixels from the original image and the encrypted image. Then 1000 pairs of two adjacent pixels are randomly selected to plot the correlation diagram based on the value of each pixel and its diagonal neighbours. We can observe that the linear property of our encrypted image, which reflects the correlation degree between pixels, shows less than that of the plain image.

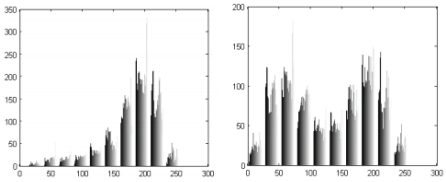

Fig. 5. Histogram chart: left: Aerial image, right: encrypted Aerial image

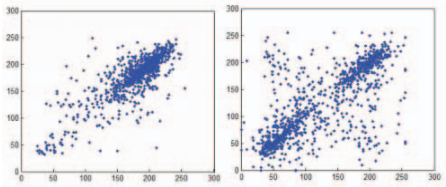

Fig. 6. Correlation chart with neighbourhood of diagonal: left: Aerial image, right: encrypted Aerial image

V. CONCLUSIONS

In this paper, a new joint image compression and encryption scheme is proposed to realize image encryption in the transformation stage of JPEG. We want to emphasize that our proposed encryption scheme does not aim at confidentiality, because people can still see some annoying image information even without the secret key.

In our encryption scheme, different orthogonal transforms, generated by the sign-flipping strategy, are alternatively applied in JPEG's transformation stage according to a predefined secret key. Experimental results have shown that our proposed algorithm can provide a sufficient level of protection without scarifying JPEG's compression ability too much. Additionally, visual quality control of the encrypted images is achieved by carefully selecting the butterflies for sign-flipping. Security analysis of our encryption algorithm against various attacks has also confirmed its effectiveness.

In our next work, we will first try to combine our encryption scheme with other encryption methods which are realized after JPEG's transformation stage, to increase the security level. Then, developing and applying integer transforms, like ICT, for encryption will also be considered in order to reduce the computational cost.

REFERENCES

[1] D. R. Stinson, *Cryptography: theory and practice*. CRC press, 2005.

[2] L. Tang, "Methods for encrypting and decrypting mpeg video data efficiently," in *Proceedings of the fourth ACM international conference on Multimedia*. ACM, 1997, pp. 219–229.

[3] L. Qiao, K. Nahrstedt, and M.-C. Tam, "Is mpeg encryption by using random list instead of zigzag order secure?" in *Consumer Electronics, 1997. ISCE'97., Proceedings of 1997 IEEE International Symposium on*. IEEE, 1997, pp. 226–229.

[4] C. Shi and B. Bhargava, "A fast mpeg video encryption algorithm," in *Proceedings of the sixth ACM international conference on Multimedia*. ACM, 1998, pp. 81–88.

[5] C.-P. Wu and C.-C. J. Kuo, "Fast encryption methods for audiovisual data confidentiality," in *Information Technologies 2000*. International Society for Optics and Photonics, 2001, pp. 284–295.

[6] S.-K. A. Yeung, S. Zhu, and B. Zeng, "Perceptual video encryption using multiple 8× 8 transforms in h. 264 and mpeg-4," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 2011, pp. 2436–2439.

[7] ——, "Design of new unitary transforms for perceptual video encryption," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 21, no. 9, pp. 1341–1345, 2011.

[8] K. Kaukonen and R. Thayer, "A stream cipher encryption algorithm arcfour," 1999.

[9] S. Lian, *Multimedia content encryption: techniques and applications*. CRC press, 2008.

[10] Z. Wang and A. C. Bovik, "A universal image quality index," *Signal Processing Letters, IEEE*, vol. 9, no. 3, pp. 81–84, 2002.

[11] W. Li and N. Yu, "A robust chaos-based image encryption scheme," in *Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on*. IEEE, 2009, pp. 1034–1037.

[12] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.