AN IMAGE IDENTIFICATION SCHEME OF ENCRYPTED JPEG IMAGES FOR PRIVACY PRESERVING PHOTO SHARING SERVICES

Kenta Iida, Hitoshi Kiya (Tokyo Metropolitan University, Japan)

Summary

◆The proposed scheme aims to **identify encrypted JPEG images** generated from the same original image, even if encrypted JPEG images are **recompressed and re-encrypted by different keys**.

◆Image encryption is carried out **by extending a block-scrambling method** for Encryption-then-Compression (EtC) systems, and feature vector is designed for the identification of images encrypted by the extended method.

Background

◆Photo sharing via various services such as SNS has greatly increased.

- It is not guaranteed that the service provider (third party) is trusted.
- Third party manipulates uploaded JPEG images.(ex. recompression and editing header).

⇒Privacy-preserving photo sharing needs to satisfy requirements:

1) Protection of visual information
2) Tolerance for recompression after encryption
3) Identification of encrypted images

Our goal:
All requirements are satisfied

◆Almost methods do not satisfy requirement 2).

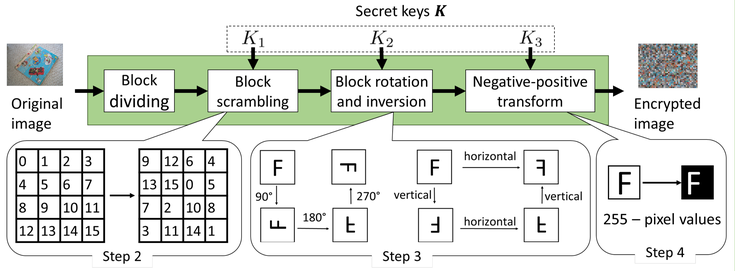
⇔EtC systems[1] satisfy requirements 1) and 2), although requirement 3) is not considered.

⇒Proposed scheme aims to identify JPEG images encrypted by a block-scrambling method, which is used in EtC system and robustness against ciphertext-only attack [1].

Block-scrambling-based image encryption

◆An image is divided into M 8x8 blocks.

◆ Step 3 does not change sum of pixel values in a block.

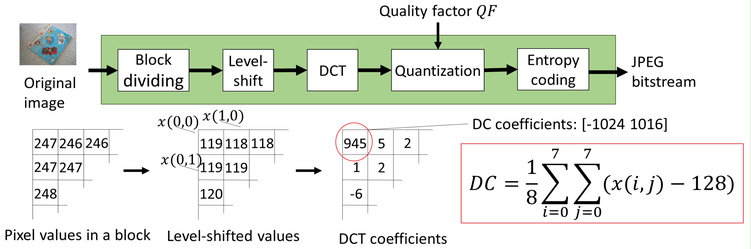


JPEG compression

◆An image is divided into M 8x8 blocks.

◆Pixel values are shifted from [0 255] to [-128 127].

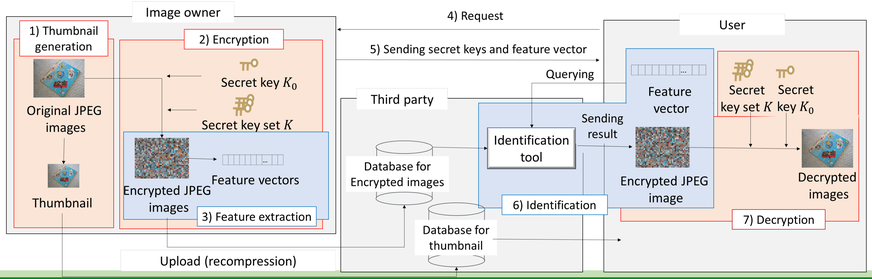
◆DC coefficients are calculated from sum of pixel values in the block.



Scenario

◆Image owner shares images to user via third party in an encrypted form.

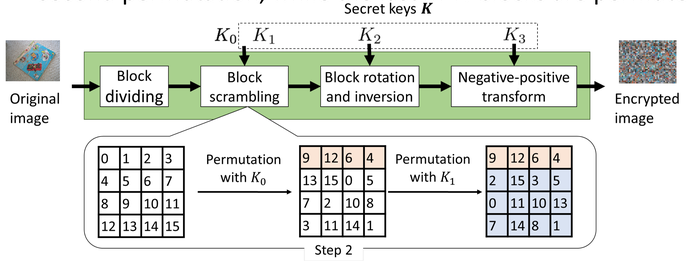
◆Assumption: thumbnails are not tied with the corresponding encrypted ones.



Proposed Scheme

■Two-layer image encryption

◆The positions of the first N blocks are **not changed** in the second permutation, while the last *M-N* blocks are permuted.



■Identification of encrypted image

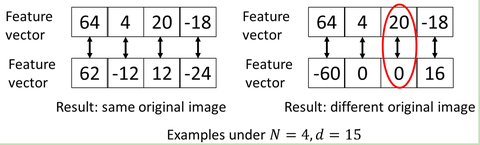
◆Feature vector: absolute values of DC coefficients of the first N blocks in Y

- Having robustness against recompression[2]
- Not changed by block rotation and inversion
- Not greatly changed by negative-positive transform

$$DC_{np} = \frac{1}{8}\sum_{i=0}^{7}\sum_{j=0}^{7}((255 - x(i,j)) - 128) = \frac{1}{8}\sum_{i=0}^{7}\sum_{j=0}^{7}(-x(i,j)) + 127) = -DC + 8$$

DC_{np}: DC coefficients when negative-positive transform is appied

◆If the difference between the values at the same position is larger than d, it is judged that two images do not have the same original image.



Simulation

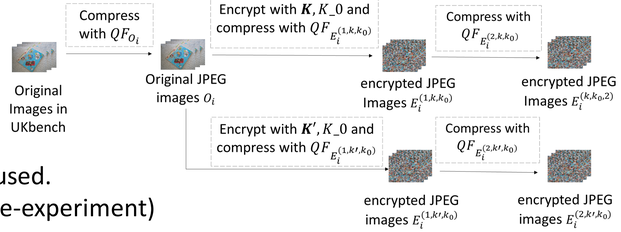
■Condition

◆Dataset: 500 images in UKbench (size 640x480)

◆500x2000 identification processes between $E_i^{(1,k,k_0)}$ and $E_i^{(2,k,k_0)}$ and 500x2000 identification processes between $E_i^{(1,k,k_0)}$ and $E_i^{(2,k',k_0)}$ are performed under each condition.

◆$d = 150$ and $N = 480$ are used. (these are determined in pre-experiment)

Condition	QF_{O_i}=	$QF_{E_i^{(1,k,k_0)}} = QF_{E_i^{(1,k',k_0)}} =$	$QF_{E_i^{(2,k,k_0)}} = QF_{E_i^{(2,k',k_0)}} =$
(1)	95	95	85,80,75,70
(2)	85	85	
(3)	75	75	



■Results

◆Only the proposed scheme achieved **perfect identification performance**, even if K_1, K_2 and K_3 are different.

Scheme	Condition	$\boldsymbol{k} = \boldsymbol{k}'$		$\boldsymbol{k} \neq \boldsymbol{k}'$	
		Precision[%]	Recall[%]	Precision[%]	Recall[%]
Proposed (d=150)	(1)	100	100	100	100
	(2)	100	100	100	100
	(3)	100	100	100	100
DC sign	(1)	100	100	0	0
	(2)	100	100	0	0
	(3)	100	100	0	0
Sparse coding	(1)	99.95	100	3.45	3.45
	(2)	100	100	3.25	3.25
	(3)	100	100	3.6	3.6
Quaternion	(1)	100	100	0.09	0.15
	(2)	100	100	0.33	0.55
	(3)	100	100	0.06	0.1
ITQ	(1)	100	100	0.31	0.5
	(2)	100	100	0.24	0.4
	(3)	100	100	0.56	0.95

Conclusion

◆Two-layer block scrambling is performed in the encoding process.

◆Feature vector designed to have robustness against the encryption and recompression is extracted from DC coefficients.

◆The use of them allow us to identify encrypted JPEG images, even if these images are **recompressed and re-encrypted by different keys**.

References

[1]K. Kurihara et al., "An encryption-then-compression system for jpeg/motion jpeg standard," IEICE Trans. Fundamentals., 2015.

[2]K. Iida et al., "Robust Image Identification for Double-Compressed and Resized JPEG Images," in Proc. APSIPA ASC, 2018.

[3]Y. Li et al., "Robust image hashing based on low-rank and sparse decomposition," in Proc. IEEE ICASSP, 2016.

[4]Y.Li et al., "Robust image hashing based on selective quaternion invariance," IEEE Signal Processing Letters,2015.

[5]Y.Gong et al.,"Iterative quantization: A procrustean approach to learning binary codes for large-scale image retrieval," IEEE Trans.PAMI, 2013.