Secure Online Image Trading Scheme Using DCT Coefficients and Moment Invariants Feature

Khairul Munadi[1,2], Mohd. Syaryadhi[1,2], Fitri Arnia[1,2], M. Fujiyoshi[3], and H. Kiya[3]
[1]Department of Electrical Engineering, Syiah Kuala University, Banda Aceh, Indonesia
[2]Master of Electrical Engineering Programme, Syiah Kuala University, Banda Aceh, Indonesia
Graduate School of System Design, Tokyo Metropolitan University, Tokyo, Japan

***Abstract*—In this paper, we introduce a scheme that enables secure image trading over the Internet. The involved parties in our image trading system are image provider, server provider, and commercial user. The proposed scheme facilitates secure storing and retrieval of original images for trading, but prevents access to unauthorized users and untrustworthy server provider. The original images are visually protected in Discrete Cosine Transform (DCT) domain, and stored at a server. Thumbnails of original images are generated and publicly accessible. A commercial user will browse these thumbnails which also serve as queries. Image matching between thumbnails and protected images is accomplished utilizing the DC component of DCT coefficients and moment invariant feature. Simulation results confirmed the effectiveness of the proposed method.**

I. INTRODUCTION

The advancement of Internet has trasformed traditional commercial transactions into online-based transactions, in which physical interaction between related parties is no longer necessary. Among online transactions, trading of multimedia content has been becoming more and more popular recently.

As multimedia contents, such as audio, image and video, are available in digital form, ones may be benefited by ease of manipulating, duplicating, publishing, and distributing them. However, those benefits would create problems when ones intend to perform illegally. Without proper arrangement, illegal content reproduction and dissemination tend to grow significantly due to the availability of the Internet. Hence, privacy protection of multimedia content is both important and a challenging research field [1-4].

Most of existing privacy protections focus on access control and secure data transmission [2], which ensure that unauthorized users have no access and the data can be securely exchanged. However, once stored at the server, the data is mostly being unprotected. This makes the user's private content vulnerable to untrustworthy server providers and unexpected intruders. Considering that an increasing amount of multimedia content will be stored at third-party server, it is both desirable and necessary to develop technologies that can better protect user's private content without sacrificing the usability and accessability of the information [2].

Motivated by the above concerns, we introduce a secure online image trading system. It is assumed that there are three parties involved in our proposed scheme: image provider, server provider, and commercial user. The scheme offers two features. It facilitates secure storing and retrieval of original images for trading. It also prevents access to unauthorized users, untrustworthy service providers, and intruders.

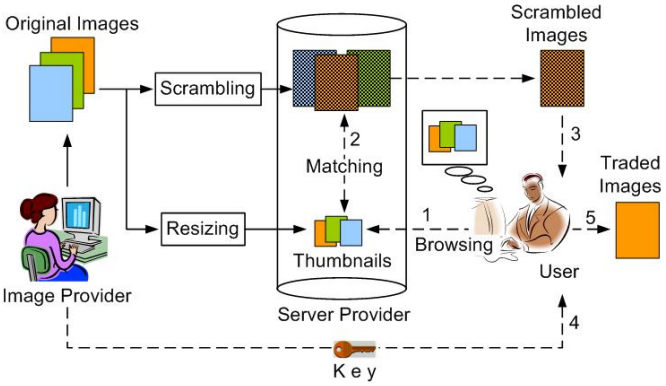

Figure 1. Proposed Scheme

II. PROPOSED SCHEME

Referring to Fig. 1, the proposed scheme is described in this section. Original images owned by image provider are first visually protected (scrambled) in Discrete Cosine Transform (DCT) domain. At the same time, thumbnails of original images are generated. Protected images are then stored at a third-party server. Thus, untrustworthy server provider has no access to the original images. Thumbnails can be stored at the same server and are publicly accessible. A commercial user will browse the thumbnail library and choose images of interest that also serve as queries (1). Image matching (2) between thumbnails and protected images is accomplished by comparing moment invariants of the thumbnails and of the DC component of protected images. After a matching process, the server will return the matched image to the commercial user (3). However, the matched image is kept visually protected unless the authorized commercial user receives a key from the image provider (4 and 5).

A. Scrambling for Visual Protection

Visual protection of original images proceeds as follows:

1. Original images are partitioned into 8x8 blocks.
2. The DCT coefficients of each block are calculated.
3. Both the DC and AC components of DCT blocks are scrambled with separate keys.
4. Inverse DCT is applied to the scrambled DCT blocks resulting visually protected images.

B. Thumbnails Generation

Original images are downscaled to produce thumbnails with any sizes. The size is flexible depending on the required dimension of display devices.

978-1-4673-6199-6/13/$31.00 ©2013 IEEE

(a) (b)

Figure 2. Original Image (a) and Visually Protected Image (b).

C. Image Matching

We exploit the seven moments proposed by Hu [5] for matching purposes. Image matching, between thumbnails and visually protected images, is done by calculating the moment distance, *d*, between thumbnails and DC component of protected images. The distance is defined as:

$$d(a,b) = \sum_{j=1}^{7} \left| M_j^a - M_j^b \right| \quad (1)$$

where, *a* and *b* are the thumbnail and the DC image respectively, *M* is Hu's moments as described in [5], [6]. The matching process proceeds as follows:

1. The moments of thumbnail image are calculated.
2. Protected images are partitioned into 8x8 blocks and DCT coefficients of each block are calculated.
3. DC components from each block of protected images are extracted. Since the scrambling key is known, DC images can be generated.
4. The moments of DC images are calculated.
5. The moment distances between query and DC images are calculated using Eq. 1. Minimum value of *d* means image matching.

III. SIMULATION RESULTS

Simulations have been carried out to confirm the effectiveness of the proposed scheme. We assumed 10 grayscale images, 512x512 pixel, as original images being traded. Example of original and protected images are shown in Fig. 2. The thumbnails were generated by rescaling the orignal images by a factor of 0.25, resulting 128x128 pixel images. The DCT is applied to the original images, and block based scrambled of DCT coefficients was carried out to produce visually protected images. The size of the DC images, which are generated from protected images, was 64x64 pixel. Those protected images and thumbnails were assumed to be stored at the same third-party server.

Simulation results are presented in Table 1. There were a total of 100 matching runs. As can be seen, the proposed moment distance performed satisfactorily in retrieving the target images. All queries returned the exact images.

IV. CONCLUSIONS

We have presented an online secure image trading scheme. The traded images are visually protected in DCT domain, and stored at a service provider's server. Thumbnails of original images are publicly accessible and serve as queries. Image matching between the thumbnails and protected images is done by comparing moment invariants of the thumbnails and of the DC component of protected images. The proposed moment distance was able to differentiate the target images among other protected images in the database.

ACKNOWLEDGMENT

The work reported in this paper is the result of research projects partially funded by Directorate General of Higher Education (DGHE) of the Republic of Indonesia, under *International Research Collaboration and Scientific Publication* Scheme.

REFERENCES

[1] W. Lu, A. L. Varna, A. Swaminatahan, and M. Wu, "Secure image retrieval through feature protection," *Proc. IEEE ICASSP,* pp. 1533-1536, 2009.

[2] W. Lu, A. L. Varna, A. Swaminatahan, and M. Wu, "Security analysis for privacy preserving search of multimedia," *Proc. IEEE ICIP,* pp. 2093-2096, Hongkong, 2010.

[3] H. Kiya and I. Ito, "Image matching between scrambled images for secure data management," *Proc. 16th EUSIPCO,* Lausanne, Switzerland, August 25-29, 2008.

[4] M. Okada, Y. Okabe and T. Uehara, "Security analysis on privacy-secure image trading framework using blind watermarking," *Proc. IEEE Ninth Annual Int. Symp. on Applications and the Internet*, pp. 243 – 246, 2009.

[5] H. Ming-Kuei, "Visual pattern recognition by moment invariants," *Information Theory, IRE Transactions,* vol. 8, pp. 179-187, 1962.

[6] Z. Huang and J. Leng, "Analysis of Hu's moment invariants on image scaling and rotation," *Proc. IEEE ICCET, Chengdu, China,* pp. 476 – 480, 2010.

Tabel 1. Simulation Results

		Thumbnails (Queries)									
		Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8	Image 9	Image 10
Protected Images	Image 1	**0.0272**	6.5339	10.2684	8.5125	9.9134	8.9880	9.6889	15.8901	26.3213	12.4257
	Image 2	6.5516	**0.0187**	12.8477	7.2107	11.1280	11.0530	7.5645	19.8658	30.7199	11.8105
	Image 3	10.2314	12.7943	**0.0358**	9.1494	2.9375	6.3008	10.3595	8.5035	19.3576	5.8361
	Image 4	8.5237	7.1850	9.1754	**0.0173**	7.0994	4.3388	7.6537	15.1455	23.5204	7.8728
	Image 5	9.9550	11.1377	2.9604	7.1086	**0.0243**	5.0466	10.7151	8.8810	19.7351	3.6539
	Image 6	8.9969	11.0303	6.3320	4.3190	5.0598	**0.0083**	9.6928	12.0618	20.3751	8.0672
	Image 7	9.6872	7.5366	10.3571	7.6255	10.7127	9.6659	**0.0378**	15.9138	25.0827	12.1028
	Image 8	15.8960	19.8346	8.4589	15.1324	8.8886	12.0388	15.9274	**0.0216**	10.9211	8.0386
	Image 9	26.3002	30.6606	19.2850	23.4644	19.7146	20.3284	25.0289	10.8591	**0.0624**	18.8646
	Image 10	12.4477	11.7935	5.8401	7.8717	3.6350	8.0649	12.1117	8.0579	18.9120	**0.0276**