2009

Watermarking protocol for protecting user's right in content based image retrieval

Jun Zhang
University of Wollongong

Lei Ye
University of Wollongong, lei@uow.edu.au

Watermarking protocol for protecting user's right in content based image retrieval

Abstract

Content based image retrieval (CBIR) is a technique to search for images relevant to the user's query from an image collection. In last decade, most attention has been paid to improve the retrieval performance. However, there is no significant effort to investigate the security concerning in CBIR. Under the query by example (QBE) paradigm, the user supplies an image as a query and the system returns a set of retrieved results. If the query image includes user's private information, an untrusted server provider of CBIR may distribute it illegally, which leads to the user's right problem. In this paper, we propose an interactive watermarking protocol to address this problem. A watermark is inserted into the query image by the user in encrypted domain without knowing the exact content. The server provider of CBIR will get the watermarked query image and uses it to perform image retrieval. In case where the user finds an unauthorized copy, a watermark in the unauthorized copy will be used as evidence to prove that the user's legal right is infringed by the server provider.

Keywords

Content based image retrieval, water- marking protocol, user’s right problem

Disciplines

Physical Sciences and Mathematics

Publication Details

Zhang, J. & Ye, L. (2009). Watermarking protocol for protecting user's right in content based image retrieval. IEEE International Conference on Multimedia and Expo, 2009. ICME 2009 (pp. 1082-1085). Piscataway, USA: IEEE.

WATERMARKING PROTOCOL FOR PROTECTING USER'S RIGHT IN CONTENT BASED IMAGE RETRIEVAL

Jun Zhang and Lei Ye

School of Computer Science and Software Engineering,
University of Wollongong,
Wollongong, NSW, 2522 Australia

ABSTRACT

Content based image retrieval (CBIR) is a technique to search for images relevant to the user's query from an image collection. In last decade, most attention has been paid to improve the retrieval performance. However, there is no significant effort to investigate the security concerning in CBIR. Under the query by example (QBE) paradigm, the user supplies an image as a query and the system returns a set of retrieved results. If the query image includes user's private information, an untrusted server provider of CBIR may distribute it illegally, which leads to the user's right problem. In this paper, we propose an interactive watermarking protocol to address this problem. A watermark is inserted into the query image by the user in encrypted domain without knowing the exact content. The server provider of CBIR will get the watermarked query image and uses it to perform image retrieval. In case where the user finds an unauthorized copy, a watermark in the unauthorized copy will be used as evidence to prove that the user's legal right is infringed by the server provider.

Index Terms— Content based image retrieval, watermarking protocol, user's right problem

1. INTRODUCTION

Content based image retrieval (CBIR) is a technique to search for images relevant to the user's query from an image collection. In CBIR, the content of an image is normally characterized by visual features, such as, color, texture and shape. Under the query by example (QBE) paradigm, the user supplies an image as a query and all images in the image collection are ranked in accordance with their similarity to the user's query. Then the top k images will be returned and displayed to the user. In last decade, most attention has been paid to improve the retrieval performance of CBIR system [1, 2]. However, there is only a few effort to investigate the security concerning in CBIR. Fleck *et.al* demonstrated a content-based retrieval strategy to tell whether there are naked people present in an image [3]. Li proposed a security mechanism for CBIR in which hierarchical queries with different authorization on a large image collection are implemented based on digital watermark [4]. Actually, with the popularity of information retrieval in ordinary users, the security concerning, especially the user's right, is becoming more and more obvious, which motivates the work presented in this paper.

Normally the user's right is ignored in CBIR. There two implicit assumptions shared by most existing CBIR schemes: (1) a query does not includes any user's private information which should not be distributed illegally; (2) the server providers of CBIR are always trustworthy who do not collect the users' information and use it without authorization. However, these are not always true in practical applications of CBIR. If a user's query image should be protected, an unfaithful server provider of CBIR may distribute it without authorization, which will lead to the user's right problem. For example, in medical applications, a medical image is used as a query [5] which including the user's health information should not be distributed without authorization. In another case, an artist may use an unpublished creation as a query to search similar images but the unauthorized copies of the query image are forbidden.

To address the user's right problem, we propose an interactive watermarking protocol. This idea comes from the digital watermark based copy deterrence [6, 7, 8, 9], which embeds a distinct watermark in each copy of the multimedia data. Later, if unauthorized copies are found, the origin of the copy can be determined by retrieving the unique watermark corresponding to each buyer. This discourages unauthorized duplication and distribution. The recent work show that a watermarking protocol is necessary to achieve secure copy deterrence [7, 8, 9]. In our watermarking protocol, an invisible watermark is inserted into the query image by the user in encrypted domain without knowing the exact content. The server provider of CBIR will get the watermarked query image and uses it to perform image retrieval. In case where the user finds an unauthorized copy, a watermark in the unauthorized copy will be used as evidence to prove that the user's legal right is infringed by the server provider. The security analysis demonstrates that the proposed watermarking protocol can protect the user's right effectively.

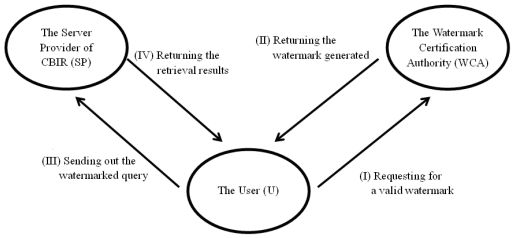

Fig. 1. Interactions among the server provider of CBIR, the user, and the watermark certification authority.

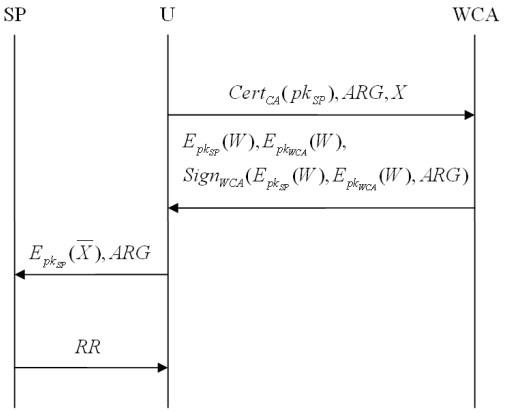

Fig. 2. Details of the interactions

2. WATERMARKING PROTOCOL

In the practical applications of CBIR, an ordinary user may have two different requirements. In one case, the user supplies a common image as the query and only cares about the retrieval results. In the other case, the user supplies a private image as the query and the content of the query image should be protected. The former case has been addressed by most existing CBIR schemes [1, 2]. In this paper, we focus on the later case and propose an interactive watermarking protocol to protect the user's right. The proposed watermarking protocol comprises of two sub-protocols: protection protocol and arbitration protocol.

2.1. Protection protocol

In the protection protocol, the interaction occurs among the user (U), the server provider of CBIR (SP) and the watermark certification authority (WCA). U is an ordinary user who supplies an image as the query and gets the retrieval results from SP. SP is the server provider who manages the CBIR system. In this paper, SP is untrusted who may distribute the user's query image without authorization. WCA is a trusted watermark certification authority who is in charge of issuing the valid watermarks. Fig.1 shows the secure image retrieval model with user's right protection and Fig.2 visualizes the details of the following steps.

1. To protect copyright of his query image, U sends $Cert_{CA}(pk_{SP}), ARG, X$ to WCA and requests a valid watermark. $Cert_{CA}(pk_{SP})$ is a common digital certification of SP which is issued by the trusted certification authority (CA) and publicly available on the SP's website [10]. ARG is a common agreement signed by U which is also publicly available and explicitly states the rights and obligations of both parties, particularly including that the user's query must not be distributed without authorization.

2. When WCA receives $Cert_{CA}(pk_{SP}), ARG$ and X, it verifies the validity of the certificate, and aborts the transaction if it is invalid. Otherwise, it generates a watermark W specific to this transaction. Since X is also transmitted to WCA, it is possible for WCA to create a more robust watermark according to the characteristics of X. After W is successfully generated, WCA computes $E_{pk_{SP}}(W)$, $E_{pk_{WCA}}(W)$ and $Sign_{WCA}(E_{pk_{SP}}(W), E_{pk_{WCA}}(W), ARG)$. The signature $Sign_{WCA}(E_{pk_{SP}}(W), E_{pk_{WCA}}(W), ARG)$ binds W and ARG, which is used to avoid the unbinding problem [9]. After that, WCA sends these data back to U.

3. Upon receiving the response, U performs the watermark insertion in the encrypted domain by computing $E_{pk_{SP}}(\bar{X}) = E_{pk_{SP}}(X \oplus W) = E_{pk_{SP}}(X) \oplus E_{pk_{SP}}(W)$, without knowing the actual watermark, W. Note that $\oplus$ is an watermark insertion operation and $E_{pk_{SP}}$ is privacy homomorphic with respect to $\oplus$. For example, the well-known RSA cryptosystem [11] is a privacy homomorphism with respect to multiplication. The Paillier public key cryptosystem [12] is also a privacy homomorphism with respect to addition. Afterwards, U sends $E_{pk_{SP}}(\bar{X})$ and ARG to SP to request retrieval results. Then, U stores all information, $Cert_{CA}(pk_{SP}), E_{pk_{SP}}(W), E_{pk_{WCA}}(W), X, ARG$, $Sign_{WCA}(E_{pk_{SP}}(W), E_{pk_{WCA}}(W), ARG)$. These data is to against possible unauthorized distribution of the private query image.

4. After receiving $E_{pk_{SP}}(\bar{X})$ and ARG, SP decrypts it with sk_{SP} by computing $\bar{X} = D_{sk_{SP}}(E_{pk_{SP}}(\bar{X}))$ and searches for the images relevant to $\bar{X}$ in its image collection or Internet. Then SP returns the retrieval results RR to U. The retrieval results can be plain text like that in the practical information retrieval applications. According to ARG, SP should not distribute $\bar{X}$ without authorization.

At last, U receives the retrieval results and this transaction is closed.

2.2. Arbitration protocol

The arbitration protocol is designed for resolving the dispute between U and SP. When an unauthorized copy Y of a certain digital content X is found, the arbitration protocol can be used to trace the pirate responsible and gather undeniable evidence. In this paper, we consider that U knows who creates the unauthorized copy since it only sends $\bar{X}$ to one SP for requesting retrieval results. U first collects the evidence information, $Cert_{CA}(pk_{SP}), Sign_{WCA}\left(E_{pk_{SP}}\left(W\right), E_{pk_{WCA}}\left(W\right), ARG\right)$, $E_{pk_{SP}}\left(W\right), E_{pk_{WCA}}\left(W\right), X, ARG$, and sends them along with Y to an arbitrator (ARB).

Upon receiving $Cert_{CA}(pk_{SP}), E_{pk_{SP}}\left(W\right), E_{pk_{WCA}}\left(W\right), X, Y, Sign_{WCA}\left(E_{pk_{SP}}\left(W\right), E_{pk_{WCA}}\left(W\right), ARG\right)$, ARB verifies the validity of the certificate and the signature. If any of them is invalid, he rejects the case. Otherwise, ARB sends $E_{pk_{WCA}}\left(W\right)$ to the WCA and asks the WCA to decrypt it. After getting W, ARB runs the corresponding watermark detection and extraction algorithm (with X, Y and W as inputs) to determine the existence of W in Y. If W is indeed found in Y, ARB turns to the CA and asks for the real identity behind pk_{SP}. Once the identity of the SP who owns pk_{SP} is revealed, ARB judges the SP to be guilty and closes the case. If W is not detected in Y, the SP is considered innocent.

3. SECURITY ANALYSIS

In this section, we examine the security of the proposed watermarking protocol. Three key problems are explored: the user's right problem, the unbinding problem and the anonymity of users.

- The user's right problem. As mentioned above, in the practical applications of CBIR an untrusted server provider may distribute the user's private query image without authorization. Our watermarking protocol is proposed to solve this problem. On the one hand, SP is unable to remove the watermark W since it has only the watermarked query image $\bar{X}$ without the knowledge of the original image X and the watermark W. Once an unauthorized copy is found, U can get enough evidence to prove that it is distributed by SP without authorization. On the other hand, U can not fabricate piracy to frame SP since the watermark insertion is performed in encrypted domain and U has no idea of the watermark W and the watermarked query image $\bar{X}$. The arbitration mechanism in the protocol can discourage the unauthorized distribution, which provides a way to protect the user's right.

- The unbinding problem. In a buyer-seller watermarking protocol, this problem means that a dishonest seller may transplant a watermark embedded in a pirated copy into a copy of higher-priced digital content to fabricate piracy [9]. In the context of CBIR, this problem changes to that a dishonest user may transplant a watermark embedded in a pirated copy into a copy of higher-priced digital content to fabricate piracy. This problem does not exist in our proposed watermarking protocol since the signature $Sign_{WCA}\left(E_{pk_{SP}}\left(W\right), E_{pk_{WCA}}\left(W\right), ARG\right)$ explicitly binds W to ARG, which uniquely specifies a particular query image X. It is impossible for U to transplant the watermark into a copy of higher-priced digital content.

- The anonymity of users. It is optional for a buyer to keep its identification anonymous in a buyer-seller watermarking protocol. An approach based on anonymous digital certification is proposed in [9]. However in CBIR, the anonymity of users is necessary and most ordinary users have no digital certification. In the proposed watermarking protocol, the user can keep anonymous who does not need to provide the digital certificate issued by trusted certification authorities. In the protection protocol, U needs to perform the watermark insertion in the encrypted domain in which the public key of SP is necessary. U can get other information from SP's website or WCA. No information on the identification of U is necessary in this stage. In the arbitration protocol, U just needs to send all evidence information to ARB in which no information about its identification involved. So the anonymity of the user is retained in the whole transaction.

4. DISCUSSION

The watermarking protocol is proposed to protect the user's right in the practical applications of content based image retrieval. The related work is a family of buyer-seller watermarking protocol [7, 8, 9, 10]. The proposed watermarking protocol and conventional watermarking protocol are different since they are applied in different applications for different purposes. Although we focus on content based image retrieval in this paper, the user's right problem also exists in other media retrieval, such as audio and video, if they apply QBE paradigm. And the proposed watermarking protocol is also suitable to content based audio retrieval or content based video retrieval.

In the protection protocol the underlying watermarking scheme is not required to be linear. That is, we do not require the computation of the watermark insertion to be performed on an element-by-element basis [8]. As long as privacy homomorphism is preserved, any kind of watermarking schemes, including those that do not tolerate the permutation of watermarks, can be adopted [9]. Furthermore, WCA has the original query image X, it can create a more robust watermark. With only one watermark the quality of $\bar{X}$ can be promised, so the retrieval performance will not be affected by

the watermark. In the arbitration protocol, the assistance of SP is not necessary. If an unauthorized copy is found, U can collect all evidence information and sends them to ARB. With the assistance of WCA, ARB can determine if SP should take charge of this pirated copy. The character is much useful in practical applications of CBIR.

In the proposed watermarking protocol, the trusted third parties, CA and WCA, can be memoryless. CA takes charge of issuing common digital certification. When later asked by ARB to reveal the real identity behind a certain certificate, CA simply decrypts the data item stored in the extension field of the certificate and derives the real identity. WCA also does not need to remember anything. Once a watermark is generated, it is encrypted with SP's public key and handed over to U. When requested by ARB to disclose a specific watermark, WCA just decrypts the ciphertext provided by ARB. The server provider of CBIR (SP) can be memoryless too. Upon receiving a request for image retrieval, SP decrypts the ciphertext from U to get the watermarked query image and performs image retrieval. Then SP returns the retrieval results to U and has nothing to remember. For user's right protection, U has to store necessary information. It is reasonable because in real-world the accuser, U, should provide enough evidence to prove that the accused SP has distributed the copies of a certain digital content without authorization.

5. CONCLUSIONS

With the explosively growing amount of information made available in digital form, the information retrieval plays a more and more important role in our work and daily life. Most researches focus on improving the retrieval performance and few efforts have been paid to the security problems of retrieval systems. In this paper, we concentrated on the security problems of content based image retrieval (CBIR). We found most conventional CBIR schemes suffer from the user's right problem. Under the query by example (QBE) paradigm, the user supplies an image as a query and the system returns a set of retrieved results. If the query image includes user's private information, an unfaithful server provider of CBIR may distribute it illegally. We proposed an interactive watermarking protocol to address this problem. In case where the user finds an unauthorized copy, a watermark in the unauthorized copy will be used as evidence to prove that the user's legal right is infringed by the server provider. So the user's right can be protected. It should be pointed out that the user's right problem also exist in other media retrieval systems, such as audio and video, if they apply QBE paradigm. And the proposed watermarking protocol is also suitable to content based audio retrieval or content based video retrieval. In the future, more attacks and risk analysis will be explored. The content based watermarking techniques and image retrieval techniques will be seamlessly combined to improve the effectiveness of the user's right protection.

6. REFERENCES

[1] A. W. M. Smeulders, M. Worring, S. Santini, A. Gupta, and R. Jain, "Content-based image retrieval at the end of the early years," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 12, pp. 1349–1380, Dec. 2000.

[2] Y. Liu, D. S. Zhang, G. J. Lu, and W. Y. Ma, "A survey of content-based image retrieval with high-level semantics," *Pattern Recognition*, vol. 40, no. 1, pp. 262–282, Jan. 2007.

[3] M. M. Fleck, D. A. Forsyth, and C. Bregler, "Finding naked people," in *European Conf. on Computer Vision II*, 1996, pp. 592–602.

[4] X. Li, "Watermarking in secure image retrieval," *Pattern Recognition Letters*, vol. 24, no. 14, pp. 2431–2434, Oct. 2003.

[5] H. Muller, N. Michoux, D. Bandon, and A. Geissbuhler, "A review of content-based image retrieval systems in medical applications - clinical benefits and future directions," *Int.l J. Medical Informatics*, vol. 73, no. 1, pp. 1–23, Feb 2004.

[6] I. Cox, J. Bloom, and M. Miller, *Digital Watermarking: Principles & Practice*. San Mateo, CA: Morgan Kaufman, 2001.

[7] L. Qiao and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights," *J. Visual Commun. Image Represent*, vol. 9, no. 3, pp. 194–210, 1998.

[8] N. Memon and P. W. Wong, "A buyerseller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[9] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1618–1626, Dec. 2004.

[10] F. Frattolillo and S. DOnofrio, "A web oriented watermarking protocol," in *Proc. of world academy of science, engineering and technology*, vol. 7, Aug. 2005, pp. 91–96.

[11] R. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, 1978.

[12] P. Paillier, "Public key cryptosystems based on composite degree residuosity classes," in *Proc. Eurocrypt'99*, J. Stern, Ed., 1999, pp. 223–238.