International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Reserving Room before Encryption Using Reversible Data Hiding Through Encrypted Images

A. Mallareddy[1], P Anjibabu[2]

[1] Research Scholar (JNTUH), Department of Computer Science & Engineering,
Professor & HOD(CSE) Sri Indu Institute of Engineering & Technology, Sheriguda(M),
Ibrahimpatnam(M), RR Dt. Hyderabad – 501510.

[2] M.Tech Scholar (CSE) , Department of Computer Science & Engineering,
Sri Indu Institute of Engineering & Technology,
Sheriguda(M), Ibrahimpatnam(M), RR Dt. Hyderabad – 501510.

Abstract: ***Privacy has acquired considerable attention but is still largely ignored inside multimedia local community. Consider some sort of cloud research scenario the spot that the server can be resource-abundant, and is also capable regarding finishing the particular designated duties. It can be envisioned in which secure advertising applications using privacy preservation is going to be treated seriously. In view that the scale-invariant characteristic transform (SIFT) has become widely adopted in several fields, this project may be the first to the fact that privacy-preserving SORT (PPSIFT) and to address the condition of safeguarded SIFT characteristic extraction and also representation inside encrypted domain..***

Keywords: Feature Extraction, Privacy Preservation, Security

1. Introduction

Just lately, people include gotten helpful to accessing in addition to querying multimedia systems data using a server as a result of increase involving bandwidth capacity on the internet. In addition, if your remote server has strong computation/storage ability with abundant resources, the people can retailer their data for the server side and exploit the computational power provided by the server for you to execute their particular intended responsibilities. In this specific circumstance, the Web not simply provides a passive look for service but has a very interactive mechanism. This scenario is comparable to cloud computing and is particularly of useful use intended for multimedia info that demand immense computation and transmission. Under these kinds of framework, the transmitting of individual data in addition to permission on the server throughout accessing your stored info pose the challenge of privacy-preserving which is usually ignored inside multimedia neighborhood.

Although encryption is really a prevalent approach to securing transmitted data, the information in your encrypted form (i.e electronic., ciphertext) can impede operations which are usually conducted for the plaintexts. As a way to further procedure ciphertexts and have the corresponding leads to the plaintext domain, some studies have been devoted to several aspects involving encrypted domain operations. Only recently, secure word document search inside encrypted domain has become extended for you to secure multimedia systems data look for. While these studies have been done with content-based multimedia systems retrieval over either encrypted query, or the two encrypted query and databases, the applicable scale-invariant function transform (SIFT) conducted inside encrypted domain still will never be addressed. In below are a few, we can target benefit of privacy-preserving SORT (PPSIFT) in addition to explore its broad software. SIFT is surely an algorithm intended for detecting in addition to describing regional features throughout images, and contains been traditionally used in the community of computer vision in addition to pattern recognition automobile powerful attack-resilient function point discovery mechanism.

The contributions in this project throughout realizing comfort preserving SORT are summarized as follows. The Difference-of-Gaussian (DoG) transform has to be executed inside encrypted domain. We look into how Doggy transform can be performed within your Paillier cryptosystem, that's associated with the error chance analysis. Our setup of DoG inside encrypted domain is analog for you to implementations involving DCT in addition to DWT inside encrypted domain. We provide a homomorphic comparability strategy that can be conducted inside encrypted domain to ensure local extrema might be securely diagnosed for SORT feature place extraction. PPSIFT has the ability to achieve regional extrema extraction, descriptor working out, and descriptor related, all inside encrypted domain, without numerous rounds involving communication between your user in addition to server. On the other hand, only one-round involving pre-communication is important for synchronization involving data. PPSIFT has become evaluated to uncover its fineness in accomplishing both comfort and robustness within benchmark violence and datasets, in comparison with the authentic SIFT

2. Previous Work

In the last decade biometric identification and authentication have increasingly gained importance for a variety of enterprise, civilian and law enforcement applications. Examples vary from fingerprinting and iris scanning systems, to voice and face recognition systems, etc. Many governments have already rolled out electronic passports and IDs that contain biometric information (e.g., image, fingerprints, and iris scan) of their legitimate holders. In particular it seems that facial recognition systems have

become popular aimed to be installed in surveillance of public places, and access and border control at airports to name some. For some of these use cases one requires online search with short response times and low amount of online communication.

Moreover, face recognition is ubiquitously used also in online photo albums such as Google Picasa and social networking platforms such as Facebook which have become popular to share photos with family and friends. These platforms support automatic detection and tagging of faces in uploaded images. Additionally, images can be tagged with the place they were taken. The widespread use of such face recognition systems, however, raises also privacy risks since biometric information can be collected and misused to profile and track individuals against their will. These issues raise the desire to construct privacy-preserving face recognition systems. [1]

Inverted Index Encryption: Since the vocabulary tree is created by and thus known to the service provider, proper encryption of the inverted indexes generated by the content owner is needed. Otherwise, the server can look up the visual words present in each image from the word IDs, and thus infer the image content. We protect the inverted index by first performing a random permutation on the word IDs so that the ith word will now have an ID. Computing random permutation takes O(N) time and needs to be done only once on the user side. However, the server needs to guess the correct IDs from O(N!) possibilities, which is computationally infeasible given the typically large value of N. Scrambling word IDs alone is not secure enough, because the server can still use visual word frequencies to identify the words that appear more frequently. [2]

Recently, people are getting used to accessing and querying multimedia data on a server due to the increase of bandwidth capacity over the Internet. In addition, if the remote server has strong computation/storage capability with abundant resources, the users can store their data on the server side and exploit the computation power provided by the server to execute their intended tasks. Under this circumstance, Web not only provides passive search service but also is equipped with high interactive mechanism. This scenario is analogous to cloud computing, and is of practical use for multimedia data that demand immense computation and communication.

Under this kind of framework, the transmission of personal data and permission of the server in accessing the stored data, however, create the privacy issue that is usually ignored in the multimedia community. Although encryption is a prevalent way in securing the transmitted data, the data in the encryption form (*i.e.*, cipher text) will impede the operations that are usually conducted on the plaintexts. In order to further process cipher texts and obtain the corresponding results in the plaintext domain, some studies have devoted to encrypted domain operations on several aspects. [3]

In order to execute SIFT in a cipher text domain and still obtain results equivalent to those generated in the corresponding plaintext domain, the prerequisite is to seek a cryptosystem that can provide the required operations, such as addition, multiplication, and so on. In the original SIFT, in addition to common additive and multiplicative operations, the comparison operation is a must for finishing feature point detection. Nevertheless, the design of a cryptosystem that can possess homomorphic comparison is still a challenging issue. Therefore, our goal is to seek a cryptosystem that can provide additive and multiplicative homomorphism, and develop a new approach to achieve homomorphic comparison$*$.

To achieve operations in the cipher text domain and obtain results equivalent to those in the plaintext domain, homomorphic encryption has been widely investigated. We choose the Paillier cryptosystem as the platform for designing our secure SIFT method because Paillier cryptosystem provides additive and multiplicative homomorphism, achieves provable security based on modular arithmetic, and is computationally comparable to RSA. In fact, Paillier cryptosystem has been widely adopted in various applications. Some recent promising privacy-preserving applications include secure transform, face recognition, secure watermark detection, sensor network surveillance, and secure distortion computation. [3]

In SIFT detection, a pixel is decided as a key point if and only if it is a local extremum in the scale space defined by difference-of-Gaussian (DoG) functions. A local extremum at a pixel is found if its DoG magnitude is larger than those of its neighbors. The idea behind our method is based on the observation that an original key point will not be detected by SIFT if another extremum is maliciously generated nearby. In other words, there are two equal extrema in a detection region such that the duplicate extremum is enforced to be at one of the eight neighbors in the scale space to evade key point detection. [4]

Currently available solutions for secure manipulation of signals apply some cryptographic primitives in order to build a secure layer on top of the signal processing modules. An example of this approach is represented by the encryption of compressed multimedia signals: the multimedia content is first of all compressed through a state-of-the-art compression scheme, and next encryption of the compressed bit stream is carried out. Consequently, the bit stream must be decrypted before the content can be decompressed and processed. These solutions typically assume that the involved parties or devices trust each other, and thus cryptography is used only to protect the data against third parties or to provide authenticity. Unfortunately, this may not be sufficient in some applications, since the owner of the data may not trust the processing devices, or those actors that are required to manipulate them. As a first example, let us consider a situation where a user (say Alice) resorts to a continuous monitoring healthcare system to analyze her medical/biological data in order to get a fast prealert diagnosis helping her to stay healthy. Very likely she will not trust the service provider that will be required to analyze Alice's data while they are encrypted. At the same time, the service provider may want to keep its processing algorithms secret since they represent the basis for its business.

As a second example, we may consider a situation where a user wants to query a database (e.g. a database containing biometric data) without revealing to the database owner (say Bob) what he/she is looking for (again this necessity may be

due to privacy reasons). It is evident that the availability of tools that allow to process an encrypted query would represent a valuable help to solve this problem. [5]

3. Proposed System

A. Paillier Cryptosystem

In this module to help execute SIFT in a ciphertext domain whilst still being obtain results corresponding to those generated in the corresponding plaintext sector, the prerequisite is usually to seek any cryptosystem that may provide the specified operations, for instance addition and also multiplication. Within the original SIFT, in improvement to typical additive and also multiplicative operations, the contrast operation is really a must with regard to finishing feature point diagnosis. We make use of the Paillier cryptosystem because the platform with regard to designing the secure SIFT method because it provides item homomorphism and also plaintext multiplication, achieves provable security based on modular maths. A couple of private and also public important factors are arranged. Let v and q be a pair of large primes, and also let N = v * q. Let Z denote the set of non-negative integers that have multiplicative inverses modulo. We additionally select grams ∈Z∗N to satisfy gcd and also λ = lcm(p − 1, q − 1) could be the private key. The couple of N and also g defines people keys. Allow message for being encrypted always be denoted since m. The ciphertext springs with your uniformly decided on key and also integer amounts modulo is required. Decrypting your ciphertext h, we make use of the private key λ and acquire the plaintext 1..

B. Gaussian Encryption

In this particular module initial step on the SIFT framework for taking out the element points would be to execute Difference-of-Gaussian turns. For this, the image is convolved along with Gaussian filters, which are assigned unique variances equivalent to weighing machines, and this differences in between two neighboring Gaussian-blurred photographs are taken. Feature things are then chosen because local extrema on the DoG photographs, which come about at a number of scales. Especially, a Canine image made at 2 neighboring weighing machines ρi and also ρj. To be able to preserve this users privateness, the image I is usually encrypted utilizing homomorphic encryption. This resultant encrypted information are portrayed as: Ie(x, y) where by E means the Paillier cryptosystem and also r could be the uniformly chosen key. Pertaining to implementation, the first Gaussian filtering coefficients are adjusted because integers considering that the Paillier cryptosystem can only operate inside the integer website.

C. Feature Point Detection

In this particular module the particular challenging task may be the local extrema removal operating within the encrypted sector. The uniformly chosen crucial r should be variable in order to meet semantic security. Under this particular circumstance, provided the plaintext meters, the resulting ciphertexts c's will change according towards used individual keys r's, resulting in one-to-many mapping. In the two-dimensional situation, like the particular images regarded here, the particular uniformly chosen key, influenced by the location of your pixel, is needed. Hence, a Canine image within the encrypted sector using various r's could be derived that is a function on the uniformly chosen key r that may be dependent on a pixel's position (x, y). Since the particular Gaussian kernel H is mixed up in calculation associated with Rρ, we know that Rρ is dependent upon the support of G() instead of the image dimension. In the particular proposed technique, in addition towards encrypted query data, the extra data would have to be sent to server with regard to subsequent privacy-preserving processing would be the secure thresholds To 's..

D. Feature Point Descriptor

In this module all of us describe the best way to derive SIFT feature descriptors from the plaintext site, which is then extended towards the ciphertext site. An alignment assignment is executed per detected function point. Then, a normalized 16×16 area expanded from your region within the derived orientation is made from which in turn feature descriptors usually are obtained the following. An SIFT feature descriptor is made for the actual 16 × 07 region, that is further broken down into fifteen 4 × four blocks, around a feature point. In addition, the calculation from the feature descriptor is accomplished at the scale the place that the feature is detected. For every 4 × four block, the actual gradient value and alignment are, respectively, computed per position (x, y) inside 4 × four block. Then, the histogram involving weighted magnitudes outlined on numerous restrictive directions is derived. For function descriptor extraction conducted from the encrypted site, the weighted magnitudes located at the four axes i. e., positive in addition to negative x-axes in addition to positive in addition to negative y-axes usually are calculated on this project, that'll constitute a new 4-dimensional vector. Since quite a total involving sixteen four × four blocks in a very 16×16 area, a 64-dimensional function descriptor is made. It need to be noted that no more than four hard to follow directions are used in this project as the operation from the secure intrinsic product5 is necessary to derive the actual included angle using the two sides not both equally coinciding using the x in addition to y axes..

4. Results

The concept of this paper is implemented and different results are shown below, The proposed paper is implemented in Net technology on a Pentium-IV PC with minimum 20 GB hard-disk and 1GB RAM. The propose paper's concepts shows efficient results and has been efficiently tested on different Image Datasets.

Figure 1: Data Set for Proposed system

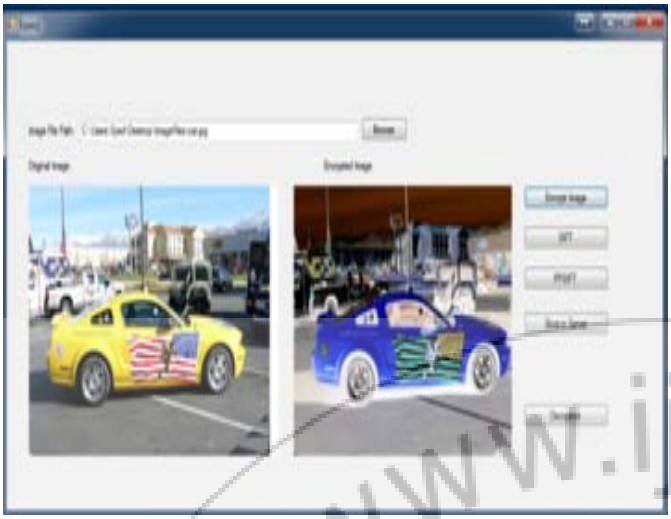

Figure 2: Proposed system performing Privacy

Figure 3: Features of Original Image

Figure 4: Comparative Features of Original and Privacy Image

5. Conclusions

We have proposed the homomorphic encryption-based privacy-preserving SIFT (PPSIFT) approach to deal with the privacy-preserving trouble encountered in the cloud calculating environment, the place that the server can certainly finish this tasks connected with SIFTbased programs without mastering anything to breach this user's privacy. In PPSIFT, probably the most challenging trouble, i. age., homomorphic comparison, has been solved within this paper. We show that the proposed Paillier cryptosystem-based PPSIFT system achieves provable security dependant on DLP and RSA, but this computational complexity needs to be further lessened, even when the current method is built to be executed within the server part that are the owners of powerful methods. We think that the offered work is definitely an important step toward privacy-preserving multimedia applications within an environment where by privacy is really a major concern.

References

[1] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," *Proc. SPIE*, vol. 7254, pp. 1–11, Jan. 2009.
[2] J. Shashank, P. Kowshik, K. Srinathan, and C. Jawahar, "Private content based image retrieval," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2008, pp. 1–8.
[3] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Homomorphic encryption-based secure sift for privacy-preserving feature extraction," *Proc. IS&T/SPIE Media Watermark., Forensics, Security*, vol. 7880, pp. 788005-1– 788005-17, Jan. 2011.
[4] Z. Yang, S. Kamata, and A. Ahrary, "NIR: Content based image retrieval on cloud computing," in *Proc. IEEE Int. Conf. Intell. Comput. Intell. Syst.*, vol. 3. Nov. 2009, pp. 556–559.
[5] B. Moskovich and M. Osadchy, "Illumination invariant representation for privacy preserving face identification," in *Proc. IEEE Comput. Vis. Pattern Recognit. Workshop*, Jun. 2010, pp. 154–161.
[6] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Proc. 9th Int. Symp. Privacy Enhancing Technol.*, 2009, pp. 235–253.
[7] J. Krizaj, V. Struc, and N. Pavesic, "Adaptation of sift features for robust face recognition," in *Proc. Int. Conf. Image Anal. Recognit.*, 2010, pp. 394–404.
[8] A. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacypreserving face recognition," in *Proc. 12th Annu. Int. Conf. Inf. Security Cryptol.*, 2009, pp. 229–244.
[9] C. Velardo and J. L. Dugelay, "Face recognition with daisy descriptors," in *Proc. ACM Multimedia Security Workshop*, 2010, pp. 95–100.
[10] U. Park, S. Pankanti, and A. K. Jain, "Fingerprint verification using sift features," *Proc. SPIE*, vol. 6944, pp. 69440K-1–69440K-9, Mar. 2008.
[11] Z. Ye, X. Chen, and Z. Li, "Video based mobile location search with large set of sift points in cloud," in *Proc. MCMC Workshop ACM Multimedia Conf.*, 2010, pp. 25–30.
[12] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Secure and robust sift," in *Proc. ACM Multimedia*, 2009, pp. 637–640.

Author Profile

Prof. A. Mallareddy., Head of the Department, Computer Science & Engineering, Sri Indu Institute of Engineering & Technology, Sheriguda (Vi),IBP(M),RR Dist-501510. Prof. A. MALLAREDDY, has done his M. Tech in Computer Science & Engineering from JNTUH and Pursuing Ph. D (CS) in Cloud Security from JNTUH. He has 09 years of teaching experience. Currently working as Professor and Head of the Department CSE at Sri Indu Institute of Engineering & Technology, sheriguda (Vi), Ibrahimpatnem (M) R.

R. Dist, He has guided many projects for UG and PG students. He is a Life member of CSI.

Pandi Anji Babu M. Tech Scholar, Computer Science & Engineering, Sri Indu Institute of Engineering & Technology Sheriguda (Vi),IBP(M),RR Dist-501510. He has done B.Tech in Computer Science & Engineering from JNTUK and Pursuing M. Tech from JNTUH. He is self-motivated, hard-worker and detail oriented. H is interested in research of new things