视觉盲计算技术研究进展

李晓东[1],金鑫[1,2],周彬[3],邹冬青[4],孙红波[1],柳振中[5]

1. 北京电子科技学院网络空间安全系,北京 100070
2. 中电科大数据研究院有限公司,贵阳 550018
3. 北京航空航天大学计算机学院,北京 100191
4. 北京市商汤科技开发有限公司,北京 100084
5. 探探科技(北京)有限公司,北京 100020

摘要 云计算和大数据的广泛应用使得多媒体数据的隐私保护面临越来越严峻的挑战,而多方计算、同态密码、函数加密等密码技术为数据在密文下的盲计算奠定了基础。视觉盲计算是在不接触图像、视频等视觉数据原始内容的情况下对其进行检测、识别、检索及更复杂的处理,是计算机视觉与密码学等领域学科交叉的新方向,在视频监控、多媒体数据共享、云计算、移动计算等领域有广泛的应用前景。本文回顾视觉盲计算技术的发展历史,从隐私保护的视频监控、人脸检测、人脸识别、人脸检索、机器学习等方面综述了该领域关键技术的发展情况,展望了视觉盲计算技术的发展趋势。

关键词 视觉计算;云计算;同态密码;多方计算;隐私保护

随着云计算技术的深入应用、网络传输速度的不断加快、图像视频数据的持续增长,人们将越来越多的图像视频数据存储在云端,并且逐渐习惯于依赖云端的强大计算能力和优秀算法处理与分析图像视频。例如,百度云盘、时光相册等网盘中可以存储大量的图像视频,并且可以在云端完成图像分类、场景识别、人脸识别与检索,即检索某一个特定人物的所有照片,或者某几个特定人物的合影照片等。再如,美图等公司提供了在线图像处理美化服务,用户可以上传自己的照片到云服务器上进行处理,无需在本地终端安装软件。

这些图像视频智能云服务在带来巨大便利的同时,也带来了存储在云端的用户影像数据的隐私泄露问题,一旦云存储服务器被攻破,这些携带大量用户隐私的影像数据将直接泄露。例如,2014年8月31日,多位好莱坞女性艺人上传到苹果云存储服务iCloud上的私人照片约200多张被人盗取并上传至贴图网站http://www.4chan.org/,造成了恶劣的社会影响;再如,2018年3月,Facebook公司被曝光将5000万名用户个人信息数据泄露给剑桥分析公司,完全暴露用户隐私,为用户的人身和财产安全带来了巨大的安全隐患。这些事件的发生,使得人们逐渐意识到:图像视频等大数据的云存储与计算在给我们带来方便的同时,也带来了内容隐私泄露风险的网络空间安全新挑战。

早在2006年,Avidan等[1]提出了视觉盲计算(blind

收稿日期:2018-07-19;修回日期:2018-08-09
基金项目:国家自然科学基金项目(61772047)
作者简介:李晓东,副教授,研究方向为网络空间安全,电子信箱:lxd@besti.edu.cn;金鑫(通信作者),讲师,研究方向为计算美学、虚拟现实、计算机视觉,电子信箱:jinxin@besti.edu.cn
引用格式:李晓东, 金鑫,周彬, 等. 视觉盲计算技术研究进展[J]. 科技导报, 2018, 36(17): 68-74; doi: 10.3981/j.issn.1000-7857.2018.17.008

vision)的概念,并提出了利用标准的密码工具实现经典的Viola & Jones目标检测算法的盲计算版本,能够在同时保护终端图像和云端目标检测器参数不被泄露的前提下,进行远程人脸盲检测。但是其利用的密码算法计算过于缓慢,以致扫描一幅普通图像需要若干小时。

为了提高盲计算的性能,在多方计算的基础上,同态密码(homomorphic cryptography)、函数加密(functional encryption)、秘密共享(security sharing)及其他种类的密码算法被不断应用到盲计算中,盲计算的性能获得显著的提高。另一方面,视觉数据处理的种类逐渐增多,从最初的目标检测发展到目标识别、目标检索、机器学习等各种视觉盲计算方案。近年来,随着深度学习成为研究的热点,面向深度学习的视觉盲计算也得到了关注。

相对于传统盲计算,视觉盲计算在数据规模上面临更大的挑战。由于性能和通用性的原因,视觉盲计算技术目前还没有达到可以实用的程度,但随着密码方法的改进和计算机处理速度的提高,视觉盲计算将会逐步走向人们的现实生活。

1　视觉盲计算研究现状

盲计算是在不接触数据原始内容的情况下对其进行处理的方法和技术。视觉盲计算是盲计算的一种,是在不接触图像、视频等视觉数据原始内容的情况下对其进行各种处理的方法和技术。视觉盲计算既包括目标检测、目标识别等简单的视觉数据处理,也包括各种复杂的视觉数据处理。

以下将从隐私保护的视频监控协议、隐私保护的人脸检测协议、隐私保护的视频人脸识别协议、隐私保护的人脸检索协议、隐私保护的机器学习协议、视觉盲计算相关的密码学方法分析等方面介绍该领域关键技术的发展情况。

1.1　隐私保护的视频监控协议

2009年,Upmanyu等[2]在国际计算机视觉会议上提出了一种基于秘密分享的隐私保护视频监控协议,该方法利用中国剩余定理将视频采集端的视频分成K份随机视频,分别发送至K个服务器,每个服务器端独立进行视频监控处理并将得到的K个结果发给观察端,在观察端利用中国剩余定理将结果合并得到最终视频监控处理结果,采集端视频不暴露任何有意义信息给服务器和观察端。

2013年,Chu等[3]在国际多媒体会议上提出了一种云环境中隐私保护的视频运动目标实时检测方法,其应用场景如图1[3]所示:监控客户端采集视频数据并且经过加密处理后发送给服务器端,服务器端在加密后的视频数据中进行运动目标检测,并且将检测结果返回给监控客户端。该方法将每一个视频帧进行颜色翻转、像素重排、矩阵相乘和量化处理等操作得到加密后的视频帧,将加密后的视频帧发送给服务器,因为这个过程中没有改变视频帧的高斯统计性质,因此服务器端仍然可以运行基于混合高斯模型的视频运动目标检测方法,得到运动目标检测结果,并将结果返回给监控客户端,而不获得监控客户端原始视频的任何隐私信息。

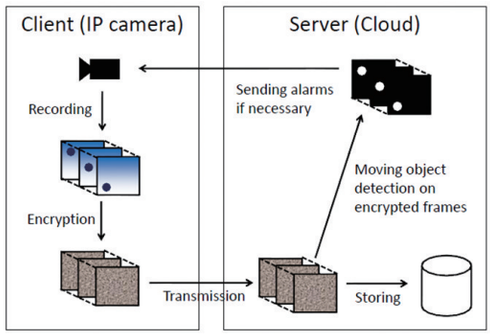

图1　隐私保护的视频运动目标实时检测协议

Fig. 1　Privacy preserving video moving object real-time detection protocol

2014年,Chu等[4]提出了一种隐私保护的多摄像机目标跟踪方法,所给出的基于扰乱电路(garbled circuits)的距离计算方法将更多的计算安排给单个监控端,如图2[4]所示,减少了多监控端的协作计算,在保证目标跟踪的准确率比传统非隐私保护的跟踪算法近似或更高的情况下,总体的时间开销只比非隐秘的跟踪算法高几秒。

1.2　隐私保护的人脸检测协议

已有的人脸检测算法有模板匹配模型、肤色模型、人工神经网络(artificial neural networks,ANN)模型、支撑向量机(support vector machine,SVM)模型、自适应增强(adaptive boosting,Adaboost)模型等,但是隐私保护的机器视觉人脸检测算法却很少。2004年,Viola等[5]提出了一种把安全多方计算协议应用到Viola & Jones目标检测算法的隐私保护的视频人脸检测协议。该协议

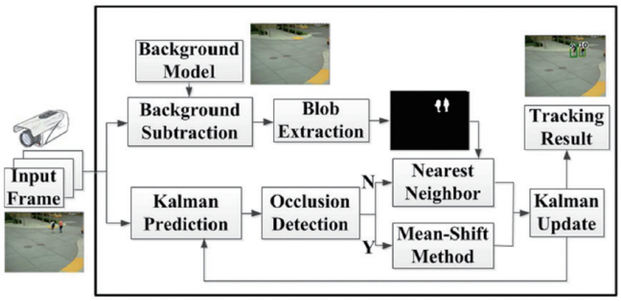

图2 隐私保护的视频目标跟踪算法:单个监控端的计算任务

Fig. 2 Private preserving video object track algorithm: one monitor side

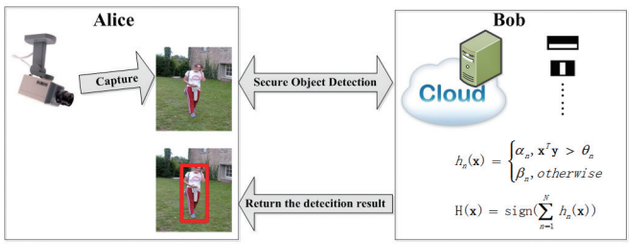

图3 云计算环境下的人脸检测场景

Fig. 3 Secure face detection scenario in cloud environment

利用不经意传输协议(oblivious transfer,OT)[6]构造了安全点积和安全阈值比较协议,进而构造了安全的分类器,实现了隐私保护的人脸图像检测。由于安全多方协议是计算密集型协议,把它应用到图像视频这样的大数据集上,计算速度较慢是其面临的主要问题。

2017年,Jin等[7]针对典型云计算环境下的人脸检测场景(图3[7]),提出了一种基于随机子图表示的隐私保护人脸图像检测协议,并在OpenCV上实现了隐私保护的人脸图像检测算法(图4[7]),其人脸检测速度获得成倍提高。

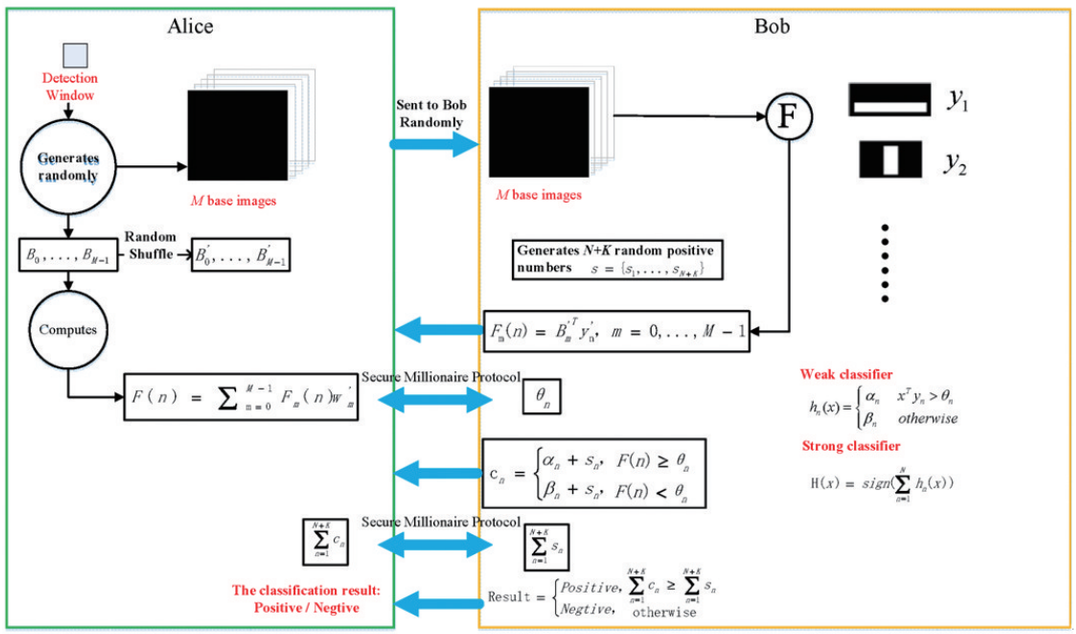

图4 基于随机子图表示的隐私保护人脸图像检测协议

Fig. 4 Random base image based secure face detection protocol

1.3 隐私保护的视频人脸识别协议

2010年,国际安全与隐私会议(IEEE Symposium on Security and Privacy)最佳论文获得者Osadchy等[8]提出了一种隐私保护的人脸识别协议,其应用场景如图5[8]所示:服务器端存储了嫌疑犯的人脸图像数据库,监控端拍摄公共场所的图像,并将图像传输给服务器,服务器通过隐私保护的人脸识别方法,获得监控端所传图像中是否包含了嫌疑犯,而不获得其他任何隐私信息,同时客户端也无法获知嫌疑犯数据库的任何信息。该协议通过人脸图像紧致表示与隐私保护的汉明距离计算方法,实现了隐私保护的人脸识别。首先将人脸图像紧致表示为一个900维的向量,然后利用不经意传输算法与统计同态加密方法实现了隐私保护的汉明距离算法,通过比较监控端查询人脸与服务器端的嫌疑犯人脸的汉明距离,确定所查询人脸是否属于嫌疑犯,如图6[8]所示。

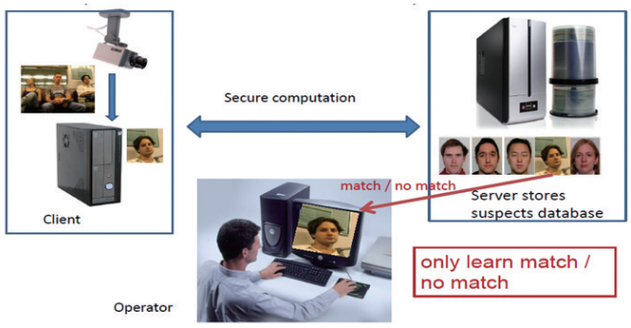

图5　隐私保护的人脸识别应用场景

Fig. 5　Private preserving face identification application scenario

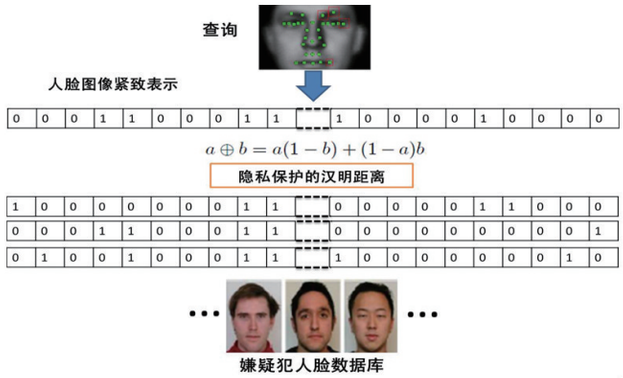

图6　隐私保护的人脸识别协议

Fig. 6　Private preserving face identification protocol

1.4　隐私保护的人脸检索协议

人们习惯于把成千上万的照片存储在云平台上，从而需要在手机等移动终端快速检索与指定照片相关的其他照片。2017年，针对该场景（图7[9]），利用函数加密实现了隐私保护的移动用户云端人脸图像检索（图8[9]）。

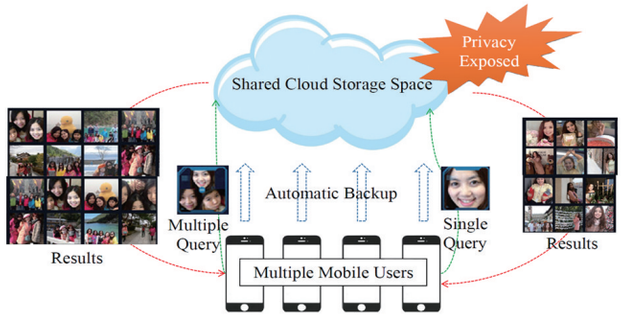

图7　移动用户云端人脸图像检索场景

Fig. 7　Scenario of face retrieval in the cloud for mobile users

1.5　隐私保护的机器学习协议

2015年，美国麻省理工学院的Bost等[10]提出一种加密域数据的机器学习分类协议。该工作构建了3种隐私保护的分类器：超平面决策、朴素贝叶斯、决策树，并且可以通过Adaboost将这些分类器进行合并，给出了

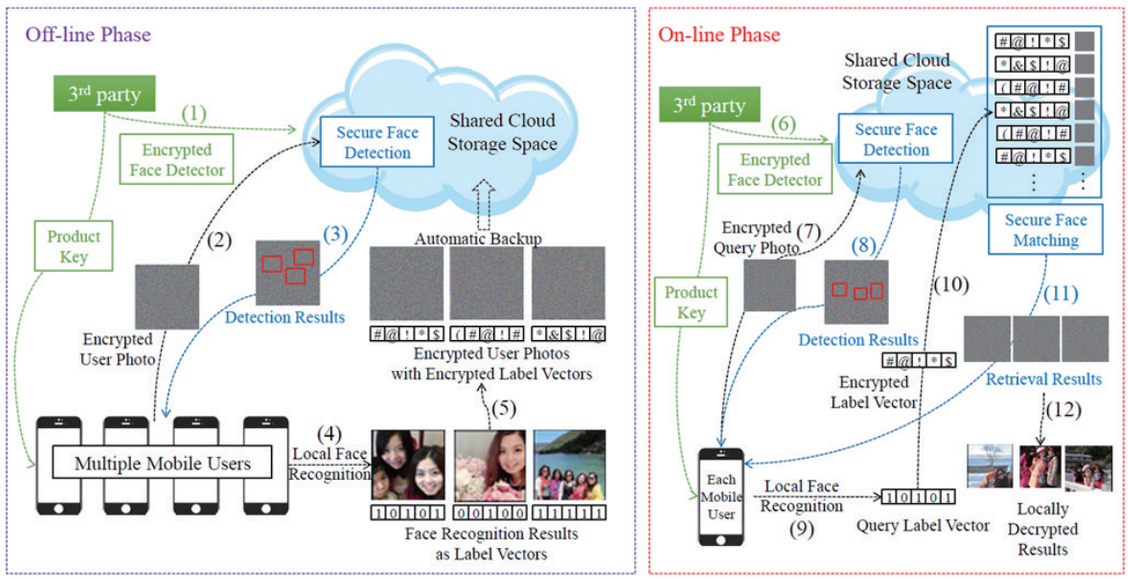

图8　隐私保护的移动用户云端人脸图像检索协议

Fig. 8　Privacy preserving face retrieval protocol in the cloud for mobile users

一个盲处理模块库,通过合并这些盲处理模块,能够合成更复杂的隐私保护分类器,可以应用在用户视频图像的人脸检测等方面,然而该方法忽略了各个盲处理模块之间配合的安全问题。

1.6 视频盲处理相关的密码学方法分析

可用于视觉盲计算的密码学方法主要包括同态加密、安全多方计算、函数加密等。

同态加密是利用加密体制的同态性质对加密后的数据实施各种操作。理想的同态加密是全同态加密[11-26],它可以在不拥有解密密钥的前提下,对加密后的数据实施任意操作。虽然全同态加密体制在2009年实现了构造上的理论突破,但全同态加密的性能距离实用仍相差较远。目前应用较多的是部分同态加密,它不能像全同态加密那样对密文进行任意处理,因此必须与特定的视觉应用场景相结合。

安全多方计算的目标是在可能有不诚实的参与者的前提下,构造协议让诚实参与者获得正确的函数值,并能保证每个参与者的输入是秘密的。安全多方计算最早由Yao[27]在1982年提出。近年来,安全多方计算出现了一些新的研究进展[28-34]。安全多方计算的运行效率仍大幅度低于采用可信第三方的计算,为此使用其他密码学工具或数学工具为具体问题构造安全多方计算协议也是一个研究方向。

函数加密(functional encryption)由Sahai等[35]在2008年首次提出,即:在具有授权密钥的前提下,可通过密文计算出明文的特定函数,而不能获得明文。近年来函数加密取得了一些理论上的进展,虽然在效率上离实用还有较大的差距[36-37]。

2 视觉盲计算研究建议

目前,视觉盲计算主要面临的问题是计算效率低,原因在于一方面盲计算开销本身就比较大,而另一方面视觉计算涉及的又是大规模数据。多方计算理论上能够解决所有视觉盲计算问题,但其计算开销与通信开销都非常大,难以实用。另外,视觉盲计算的大多数问题是解决盲委托计算,即视觉数据在云端的盲计算,而多方计算的场景是多方拥有隐私,会带来不必要的通信开销。全同态密码能够彻底解决云端视觉数据的盲委托计算,但其计算开销很大,同样难以满足实用的要求。解决视觉盲计算效率低的方法主要包括:(1)利用部分同态密码构造视觉盲计算协议。部分同态密码仅支持特定的同态计算,因此一种方法是针对特定视觉计算任务,选择或构造专门的部分同态密码算法;另一种方法是针对已有的部分同态密码算法,改造视觉处理算法,进而构造盲计算协议。(2)利用秘密分享技术,基于多个独立委托计算方的相互牵制,构造盲计算协议。(3)压缩视觉数据。在盲计算前,提取视觉数据特征,然后对特征构造盲计算协议。

视觉盲计算的目标是构造一个通用的视觉盲计算任务库(图9)。为了达到这个目标,首先是支持基本的视觉运算的盲计算,如汉明距离、点积、欧氏距离,在基于神经网络的视觉计算中还要支持神经元的激励函数,通常的方法是用多项式逼近神经元的激励函数。其次,要支持目标检测、目标识别、目标检索等视觉计算任务的盲计算。在此基础上,可以提供标准接口的视觉盲计算任务库。这样,各种隐私保护的视觉计算业务就可以通过调用视觉盲计算任务库实现安全的视觉计算。

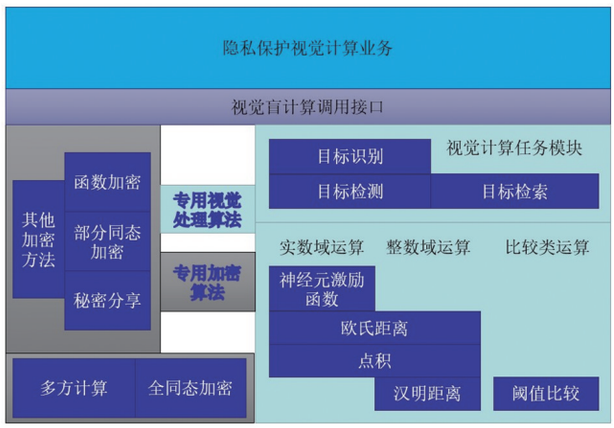

图9 视觉盲计算框架展望

Fig. 9 Prospect of blind vision

3 结论

视觉盲计算是视觉计算与密码技术的结合。在应用方面,云计算、移动计算等对视觉计算提出了越来越多的隐私保护需求和挑战。在视觉盲计算协议构造方面,深度学习已成为视觉计算的热点,有必要深入研究面向深度学习的盲计算技术,另一方面,密码技术近年来取得一系列的突破,属性加密、函数加密等新的密码方法也为视觉盲计算提供了更多的支持。在应用的推动下,随着视觉计算、密码技术的发展,视觉盲计算将会逐步走进人们的日常生活。

参考文献(References)

[1] Avidan S, Butman M. Blind vision[C]//Proceedings of 9th European Conference on Computer Vision. Berlin: Springer-Verlag, 2006: 1-13.

[2] Upmanyu M, Namboodiri A M, Srinathan K, et al. Efficient privacy preserving video surveillance[C]//IEEE 12th International Conference on Computer Vision. Piscataway NJ: IEEE, 2009: 1639-1646.

[3] Chu K Y, Kuo Y H, Hsu W H. Real-time privacy-preserving moving object detection in the cloud[C]//ACM International Conference on Multimedia. New York: ACM, 2013: 597-600.

[4] Chu C T, Jung J, Liu Z, et al. STrack: Secure tracking in community surveillance[C]//ACM International Conference on Multimedia. New York: ACM, 2014: 837-840.

[5] Viola P, Jones M. Robust real-time face detection[J]. International Journal of Computer Vision, 2004, 57(2): 137-154.

[6] Ishai Y, Kilian J, Nissim K, et al. Extending oblivious transfers efficiently[C]//International Cryptology Conference. Berlin: Springer-Verlag, 2003: 145-161.

[7] Jin X, Yuan P, Li X, et al. Efficient privacy preserving Viola-Jones type object detection via random base image representation[C]//IEEE International Conference on Multimedia and Expo. Piscataway NJ: IEEE, 2017: 673-678.

[8] Osadchy M, Pinkas B, Jarrous A, et al. SCiFI: A system for secure face identification[C]//2010 IEEE Symposium on Security and Privacy (SP). Piscataway NJ: IEEE, 2010: 239-254.

[9] Jin X, Ge S M, Song C G. Privacy preserving face retrieval in the cloud for mobile users[J]. arXiv.org, 2017, arXiv: 1708.02872.

[10] Bost R, Popa R A, Tu S, et al. Machine Learning classification over encrypted data[C]//Network and Distributed System Security Symposium 2015. Internet Society, 2015, doi: 10.14722/ndss.2015.23241.

[11] Rivest R. On data banks and privacy homomorphism[M]//Foundations of Secure Computation. Pittsburgh: Academic Press, 1978: 168-177.

[12] Gentry C. Fully homomorphic encryption using ideal lattices [C]//Proceedings of the Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 169-178.

[13] Gentry C. A fully homomorphic encryption scheme[M]. Palo Alto: Stanford University, 2009.

[14] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes[J]. Lecture Notes in Computer Science, 2010, 2009: 420-443.

[15] Stehlé D, Steinfeld R. Faster fully homomorphic encryption [C]//EUROCRYPT 2010. Berlin: Springer-Verlag, 2010: 377-394.

[16] Gentry C, Halevi S. Implementing gentry′s full homomorphic encryption scheme[C]//EUROCRYPT 2011. Berlin: Springer-Verlag, 2011: 129-148.

[17] Gentry C, Halevi S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits[C]//2011 IEEE 52nd Annual Symposium on Foundations of Computer Science. Piscataway NJ: IEEE, 2011: 107-109.

[18] Dijk M V, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers[C]//International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 24-43.

[19] Mandal A, Tibouchi M, Tibouchi M. Fully homomorphic encryption over the integers with shorter public keys[C]//Conference on Advances in Cryptology. Berlin: Springer-Verlag, 2011: 487-504.

[20] Coron J, Naccache D, Tibouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers[C]//Advances in Cryptology—EUROCRYPT 2012. Berlin: Springer-Verlag, 2012: 446-464.

[21] Cheon J H, Kim J, Lee M S, et al. CRT-based fully homomorphic encryption over the integers[J]. Information Sciences, 2015, 310: 149-162.

[22] Coron J S, Lepoint T, Tibouchi M, et al. Batch fully homomorphic encryption over the integers[C]//EUROCRYPT 2013. Berlin: Springer-Verlag, 2011: 315-335.

[23] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from Ring-LWE and security for key dependent messages [C]//CRYPTO 2011. Berlin: Springer-Verlag, 2011: 505-524.

[24] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[C]//Foundations of Computer Science 2011. Piscataway NJ: IEEE, 2011: 97-106.

[25] Brakerski Z, Gentry C, Halevi S. Packed ciphertexts in LWE-based homomorphic encryption[M]//Public-Key Cryptography—PKC 2013. Berlin: Springer-Verlag, 2013: 1-13.

[26] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]//33rd Annual Cryptology Conference. Berlin: Springer-Verlag, 2013: 75-92.

[27] Yao A C. Protocols for secure computations[C]//23rd Annual Symposium on Foundations of Computer Science. Piscataway NJ: IEEE, 2008: 160-164.

[28] Hirt M, Maurer U, Lucas C. A dynamic tradeoff between active and passive corruptions in secure multi-party computation [C]//33rd Annual Cryptology Conference. Berlin: Springer-Verlag, 2013: 203-219.

[29] Boyle E, Goldwasser S, Tessaro S. Communication locality in secure multi-party computation[C]//Theory of Cryptography Conference on Theory of Cryptography. Berlin: Springer-Verlag, 2013: 356-376.

[30] Rastogi A, Mardziel P, Hicks M, et al. Knowledge inference for optimizing secure multi-party computation[C]//Eighth ACM Sigplan Workshop on Programming Languages and Analysis for Security. New York: ACM, 2013: 3-14.

[31] Lee E J, Abbe E. A shanndon approach to secure multi-party computations[C]//52nd Annual Allerton Conference. Piscataway NJ: IEEE, 2014: 1287-1293.

[32] 刘木兰, 张志芳. 密钥共享体制和安全多方计算[M]. 北京: 电子工业出版社, 2008.
Liu Mulan, Zhang Zhifang. Secret sharing system and secure multi-party computation[M]. Beijing: Publishing House of Electronics Industry, 2008.

[33] Chen H, Cramer R. Algebraic geometric secret sharing schemes and secure multi-party computation over small fields[C]//Advances in Cryptology—CRYPTO 2006. Berlin: Springer-Verlag, 2006: 521-536.

[34] Chen H, Cramer R, Goldwasser S, et al. Secure computation from random error correcting codes[C]//Proceedings of the 26th Annual International Conference on Advances in Cryptology. Berlin: Springer-Verlag, 2007: 291-310.

[35] Sahai A, Waters B. Slides on functional encryption[EB/OL]. [2018-05-31]. http://www.cs.utexas.edu/bwaters/presentations/files/functional.ppt.

[36] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption[C]//Proceedings of the 29th Annual International Conference on Advances in Cryptology. Berlin: Springer-Verlag, 2010: 62-91.

[37] Goldwasser S, Kalai Y, Popa R A, et al. Reusable garbled circuits and succinct functional encryption[C]//ACM Symposium on Theory of Computing. New York: ACM, 2013: 555-564.

Recent advances on blind vision

LI Xiaodong[1], JIN Xin[1,2], ZHOU Bin[3], ZOU Dongqing[4], SUN Hongbo[1], LIU Zhenzhong[5]

1. Department of Cyber Security, Beijing Electronics Science and Technology Institute, Beijing 100070, China
2. CETC Big Data Research Institute Co.,Ltd., Guiyang 550018, China
3. School of Computer Science and Engineering, Beihang University, Beijing 100191, China
4. Sense Time, Beijing 100084, China
5. Tantan App., Beijing 100020, China

Abstract With the rapid development of multimedia technology and the Internet, privacy protection of multimedia data is facing more and more challenges. The widespread application of cloud computing and big data, on the other hand, has further exacerbated people´s concerns about privacy security. However, multiparty computation, homomorphic cryptography, functional encryption and other cryptographic techniques have made possible the blind computation of data under ciphertext. In particular, visual blind computing is to detect, identify, search, and deal with data without touching their original contents such as images and videos. As a new direction in the combination of computer vision and cryptography, it has a wide range of applications in video monitor, multimedia data sharing, cloud computing, mobile computing and other fields. This paper reviews the development history of visual blind computing technology, summaries the key technologies for video monitor, face detection, face recognition, face retrieval, machine learning and so on, and looks into the development trend of visual blind computing technology.

Keywords visual computing; cloud computing; homomorphic cryptography; multiparty computation; privacy protection

（责任编辑　刘志远）