암호화된 영상에서의 2차원 영상 필터링

채효철 ○, R. S. 라마크리시나
광주과학기술원 정보기전공학부 뉴웨이브컴퓨팅 연구실
chaehc○@gist.ac.kr, rsr@gist.ac.kr

2D Image Filtering on Encrypted Image

HyoChul Chae○, R. S. Ramakrishna
NWCL, School of Information & Mechatronics, Gwangju Institute of Science and Technology

영상 필터링은 컴퓨터비전, 의료영상처리, 생체인식등의 영상처리분야에서 전처리방법으로 널리 쓰이고 있다. 만약 사용자의 민감한 영상정보를 요구하지 않으면서 필터링을 할 수 있는 방법이 개발된다면 환자의 의료영상이나 지문과 같이 프라이버시 보호가 필요한 정보를 원격으로 처리할 때 신뢰성 있는 서비스를 사용자에게 제공할 수있을 것이다. 본 논문에서는 준동형(Homomorphic) 암호를 사용하여 사용자의 민감한 영상의 완전한 정보를 요구하지 않는 안전한 영상 필터링 프로토콜을 제시한다. 이 프로토콜은 이전에 제안된 프로토콜 [1]과는 달리 암호화된 영상에서 임의의 횟수만큼 필터링을 연속적으로 적용할 수 있고 암호화된 영상만 가지고 공개적으로 필터링된 영상을 구할 수 있으므로 [1]과는 달리 신뢰기관을 필요로 하지 않는다. 특히 영상 필터링을 연속으로 적용하더라도 [1]과 달리 통신비용이 추가로 늘어나지 않는 장점이 있다.

안전한 영상 필터링 문제는 함수(영상 필터링)를 참가자 A와 B가 자신의 입력정보(A는 영상 정보, B는 필터링 알고리즘 파라미터)를 서로에게 공개하지 않으면서 안전하게 함수를 계산하여 필터링된 영상을 얻는 문제이며 안전한 다자간 계산 프로토콜의 특별한 경우로 생각 할 수 있다. 안전한 다자간 계산이론[4]에 따르면 어떠한 다항식시간 함수도 안전한 다자간 계산 프로토콜로 변환할 수 있으며 다양한 변환 방법 또한 존재한다. 이러한 변환방법을 변조된 회로변환(Garbled Circuit Transformation)이라 하는데 이 방법으로 변환된 프로토콜은 매우 비효율이기 때문에 함수가 간단한 경우를 제외하고는 실제 프로토콜에서는 거의 사용되지 않는다. 영상처리에서 사용되는 영상 필터링은 대용량의 영상을 고속으로 처리해야 하기때문에 변조된 회로변환기법을 사용할 수 없다. 따라서, 영상처리에 특화된 효율적인 다자간 계산 프로토콜의 개발이 필요하다. 최근 [1]에서는 변조된 회로변환기법을 사용하지 않는 효율적인 프로토콜을 처음 제시하였다. [1]에서는 이 문제를 두 행렬의 곱으로 변환하여 [3]에서 제시된 효율적이고 안전한 프로토콜을 이용하여 이 문제를 해결하였다. [1]에서는 두 가지 프로토콜을 제시하는데, 첫번째 프로토콜은 상대적으로 효율적이지만 선형필터를 연속으로 적용할 수 없다. 하지만 실제 영상처리에서는 선형 필터를 여러번 연속으로 사용하는 경우가 많기 때문에 이 프로토콜은 실용적이지 못하다. 두 번째 프로토콜은 첫 번째 프로토콜에서 지원되지 않는 연속 필터링 기능을 신뢰기관을 도입하여 가능하게 하였다. 그러나 신뢰기관의 도입은 시스템이 복잡해 지고 통신비용이 필터를 연달아 적용하는 횟수에 따라 늘어나는 단점이 있다.

안전한 영상 필터링 문제는 다음과 같이 정의된다: Alice 는 W x H 크기의 민감한 영상 $\mathbf{x}$ 를 가지고 있으며 $\mathbf{x}(i,j)$는 좌표 (i,j)에서의 픽셀 값을 나타낸다. Bob 은 필터 파라미터 θ을 가지고 있다. 선형 필터링의 경우 θ는 L x L 크기의 마스크 h 로 정의된다. 이제 영상 $\mathbf{x}$ 에 필터가 적용된 영상은 $y(m,n) = f(\mathbf{x},\theta)$ 으로 정의된다. 목표는 Alice 와 Bob 간의 다음을 만족하는 프로토콜을 구축하는 것이다: 1. Alice 는 필터링 된 영상 $f(\mathbf{x},\theta)$을 얻는다. 이때 Alice 는 $f(\mathbf{x},\theta)$ 에서 필터링 파라미터에 대한 정보를 얻을 수 있는 것을 제외하고는 θ에 대한 유용한 정보를 얻을 수 없다. 2. Bob 은 영상 $\mathbf{x}$ 에 대한 아무런 정보도 얻을 수 없다. 선형 필터링의 경우, θ는 필터 마스크 $h = \{h(m,n) : -L/2 \le m,n \le L/2\}$ 로 정의되며 선형 필터링 연산은 다음과 같이 정의된다.

$$y(m,n) = x * h = \sum_{i=-\frac{L}{2}}^{\frac{L}{2}} \sum_{j=-\frac{L}{2}}^{\frac{L}{2}} x(m-i,n-j)h(i,j) \qquad (1)$$

본 논문에서 제안하는 프로토콜은 덧셈연산을 보존하는 준동형암호(Additive Homomorphic Encryption)의 특성을 이용한다. 덧셈연산을 보존하는 준동형암호 $E_r(\cdot)$의 정의는 다음과 같다: 1. $E_r(\cdot)$는 확률적 암호화 알고리즘이이다. 2. $c_1=E_s(m_1)$과 $c_2=E_t(m_2)$가 주어졌을 때 $c_1c_2=E_r(m_1+m_2)$를 만족하는 r 이 항상 존재한다. 3. $c=E_r(m)$와 정수 i 가 주어졌을 때 누구나 $c'=E_s(m\cdot i)$를 계산할 수 있어야 한다.

제안하는 프로토콜은 프로토콜 1, 2 에서 자세히 기술되며 알고리즘 1, 2 에서는 각 프로토콜에서 사용되는 알고리즘을 설명한다.

알고리즘1. Compress(·)

입력: $c_1=E(m_1)$, $c_2=E(m_2)$, …, $c_t=E(m_t)$, m_i는 σ비트

출력: $c^*= E(m_1 + m_2 2^{\sigma} + \cdots + m_t 2^{\sigma t})$

1. $c = c_t$
2. for i=t-1..1
3. $c = c^{2^t} c_i$

알고리즘2. Decompress(·,·)

입력: $c^*= E(m_1 + m_2 2^{\sigma} + \cdots + m_t 2^{\sigma t})$, 개인키 SK

출력: m_1, m_2,…, m_t

1. m = D(SK,c)
2. for i=1..t=⌊|N|/σ⌋
3. m_i = m mod 2^{σ} , m = m / 2^{σ}

프로토콜1. Alice(·)

입력: 공개키 PK, 비밀키 SK, 영상정보 x

출력: 필터가 적용된 영상 f(x)

1. Send public-key <PK> to Bob
2. Send $<c_{ij}=E[x(i,j)]>$ to Bob for i=1..W, j=1..H
3. Recv blocks $<c_1>,\ldots,<c_p>$ from Bob
4. Recover filtered image by running Decompress(SK,c_i) for i=1..p

프로토콜2. Bob(**h**)

입력: 필터 파라미터 h(·,·)

1. Recv public-key <PK> from Alice
2. Recv encrypted image $<c_{ij}>$ from Alice
3. Calculate $d_{i,j}=\prod_{i=-\frac{L}{2}}^{\frac{L}{2}}\prod_{j=-\frac{L}{2}}^{\frac{L}{2}} c_{m-i,n-j}^{h(i,j)}$
4. Divide the pixels of image into WH/$\left\lfloor\frac{|N|}{\sigma}\right\rfloor$ blocks and run compress(·,·,..) for the block where each block consists of $\left\lfloor\frac{|N|}{\sigma}\right\rfloor$ pixels
5. Send each compressed block to Alice

제안된 프로토콜은 표1에서 볼 수 있듯이 기존의 프로토콜 [1]과 달리 선형 필터링을 반복 적용하는 회수에 상관없이 일정한 통신비용을 가진다. [1]에서는 암호를 사용하지 않고 매우 효율적인 방법을 제시했으나 연속된 필터링 적용횟수에 따라 통신비용이 늘어나는 단점이 있으며 신뢰기관이 항상 존재해야 하는 가정이 필요하다.

프로토콜	총 통신비용: 필터링 k=1번 적용	추가 통신비용: 필터링 k(≥2)번적용
[1] 첫번째	$(W\cdot H)\sigma\cdot(1+L^2)$	지원안함
[1] 두번째: 신뢰기관도입	$(W\cdot H)\sigma\cdot(2+4L^2)$	$2(W\cdot H)\sigma\cdot(1+L^2)(k-1)$
제안프로토콜:	$(W\cdot H)2\|N\|(1+1/\left\lfloor\frac{\|N\|}{\sigma}\right\rfloor)$	0

본 논문에서는 준동형(Homomorphic) 암호를 사용하여 사용자의 민감한 영상의 완전한 정보를 요구하지 않는 안전한 선형 필터링 프로토콜을 제시한다. 이 프로토콜은 이전의 프로토콜과 비교했을 때 신뢰기관을 도입할 필요가 없고 선형필터링을 연속으로 적용하더라도 통신비용이 늘어나지 않는다. 하지만 연속으로 적용하는 횟수가 적으면 이전 프로토콜 보다 높은 통신비용을 가진다. 향후 안전성을 유지하면서 통신비용을 줄이는 것이 과제라고 할 수 있겠다.

참고논문

[1] Nan, H., S.-C. Cheung, and T. Nguyen. 2006. Secure Image Filtering. Appeared in IEEE International Conference on Image Processing, ICIP 2006.

[2] Avidan, S.; Butman, M., "Blind Vision", *European Conference on Computer Vision (ECCV)*, May 2006

[3] W.L. Du, Yunghsiang S. Han and S. Chen, "Privacy-preserving multivariate statistical analysis: Linear regression and classification," Proceedings of the Fourth SIAM International Conference on Data Mining, pages 222-233, 2004.

[4] R. Cramer, I. Damgard, and J.B. Nielsen. Multiparty computation from threshold homomorphic encryption, 2000. IACR ePrint archive manuscript.