서로 맞물린 암호행렬에 관한 연구

A Study on Interlocking Code Matrix

이 성 룡
한국외국어대학교 산업공학과
경기도 용인시 모현면 왕산리 산 89

Abstract

암호행렬은 행렬을 구성하고 있는 원소들의 특정한 조합이 암호를 형성하는 행렬로서 실제적인 문제를 해결하기 위한 수단으로 개발된 바 있다. 암호행렬은 구성원소들이 서로 긴밀하게 연관되어 있다는 점에서 여러 흥미로운 특성을 갖게 되는데 이러한 특성은 암호행렬로부터 암호를 쉽고 빠르게 해독한다든지 암호행렬을 필요에 따라 형태변환 시킨다든지 하는 것에 이용할 수 있다. 본 연구에서는 이러한 암호행렬의 생성에 기본이 되는 서로 맞물린 수열의 성질에 대해 우선 간략히 살펴보고 이러한 성질에 의해 특징지워지는 암호행렬의 특성을 체계적으로 규명함으로써 암호행렬이 향후 여러 방면에서 응용되기위한 이론적인 배경을 마련하고자 한다.

1. 서론

암호행렬이란 행렬을 구성하고 있는 원소들의 특정한 조합이 암호를 형성하도록 구성원소들을 배열한 행렬을 말한다. [그림-1]은 암호행렬의 한 예를 보여주는 것으로 행렬내 특정 위치에서의 암호는 주어진 위치에서의 원소와 그 주위의 원소값들로 구성된다. 암호를 구성하는 원소의 순서를 (가운데, 왼쪽, 위, 오른쪽, 아래) 라고 한다면 그림에서 표시된 위치에서의 암호는 (1 2 3 2 3) 이다.

암호행렬은 행렬을 구성하고 있는 암호들의 구성이나 상호 연관성 등에 의해 여러가지의 성질을 가질 수 있는데, 암호행렬 내의 어떤 암호든지 오직 한번만 존재하도록, 즉, 암호의 중복이 없도록, 구성되는 것이 그중 하나이다. 이러한 암호행렬은 구조화된 광원(structured light)을 사용하여 삼차원의 데이터를 추출하고자 하는 비젼(vision) 시스템 개발 과정에서 상응문제(correspondence problem)라 알려진 難題를 풀기 위하여 저자에 의해 처음으로 고안되었고, 유일하게(uniquely) 구성되는 암호행렬이라 부르게 되었다 [1, 2, 3].

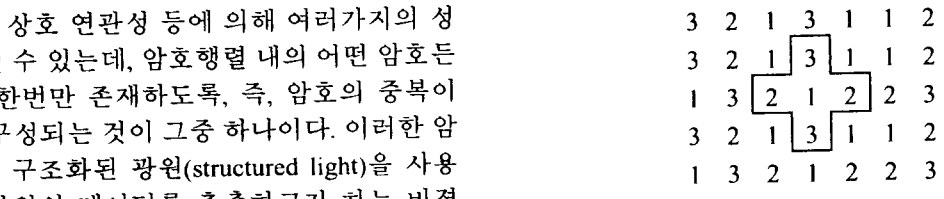
암호행렬은 행렬을 구성하고 있는 원소들이 서로 긴밀하게 연관되어 (맞물려) 있다는 점에서 여러 흥미로운 성질을 갖는다. 본 연구에서는 서로 맞물린 암호행렬이 갖는 기본적인 성격을 규명하고 이러한 행렬로부터 읽혀지는 암호의 특성을 살펴봄으로써 암호행렬의 응용시에 사용될 수 있는 이론적인 배경을 제공하고자 한다.

2 장에서는 암호행렬을 만들기 위한 기본 형태로서의 서로 맞물린 수열과 이러한 수열로부터 암호행렬이 생성되는 과정을 간략히 살펴본다. 3 장에서는 암호행렬이 갖는 일반적인 특성과 유일하게 구성되는 암호행렬 내에서의 암호에 관한 특성을 밝히고, 4 장에서 결론을 내린다.

2. 서로 맞물린 수열과 암호행렬의 생성

2.1. 서로 맞물린 수열

본 연구에서 수열이란 일정한 길이를 갖는 수의 나열을 의미하며 괄호( ) 안에 표기하기로 한다. 자연수(natural number)의 집합 $\mathbf{N}$ 이 주어지고 어떤 수열을 이루는 요소(primitive)의 갯수 p 가 정해질 때, 요소의 집합 P 는 $\{1, 2, 3, ..., p\} \in \mathbf{N}$ 으로 나타낼 수 있다. 예를 들어 $P = \{1, 2\}$ 의 경우 (2 2 1 2 1) 은 P 로부터 만들 수 있는 수열



[그림-1] 암호행렬과 암호의 예

중 하나이다.

서로 맞물린 수열에서 '서로 맞물림' 이란 어떤 수열에서 주어진 길이의 인접한 수들이 서로 의미있게 연관되어 있음을 뜻한다. 이러한 연관성을 나타내기 위하여 수열 내의 서로 인접하는 k 개의 요소로 이루어지는 수열을 '길이가 k 인 부분수열' 이라 정의한다. 예를 들어 수열 (2 2 1 2 1) 에서 길이가 3 인 부분수열을 순서대로 나열하면 (2 2 1), (2 1 2), (1 2 1) 이 된다. 여기에서 두번째 부분수열 (2 1 2) 의 첫 두 요소인 2 와 1 은 첫번째 부분수열인 (2 2 1) 의 끝 두 요소인 2 와 1 이다. 마찬가지로 세번째 부분수열 (1 2 1) 의 첫 두 요소인 1 과 2 는 두번째 부분수열인 (2 1 2) 의 끝 두 요소인 1 과 2 이다. 즉, 이 예에서 각 부분수열 들은 두개의 원소씩 서로 연관되어(맞물려) 있다고 말할 수 있다. 일반적으로는 전체 길이가 l 인 수열에는 길이가 k 인 부분수열이 $l-k+1$ 개 있음을 알 수 있다.

주어진 수열에서 부분수열의 길이에 따라 서로 맞물린 성질에 대한 해석이 달라질 수 있다. 예를 들어 수열 (2 2 1 2 1) 에서 길이가 3 인 부분수열은 (2 2 1), (2 1 2), (1 2 1) 로 부분수열간에 중복됨이 없으나 같은 수열에서 길이가 2 인 부분수열은 (2 1), (2 1), (1 2), (2 1) 로 같은 형태의 부분수열이 중복됨을 알 수 있다. 주어진 P 로 구성된 어떤 수열에서 길이가 k 인 부분수열을 고려할 때 중복된 부분수열을 발견할 수 없다면 유일성(uniqueness)을 갖는다고 하고 이러한 수열을 $\mathbf{U}(p, k)$ 로 표기한다.

P 와 k 가 주어질 때 수열에 대한 서로 맞물린 성질 중 다른 하나로서 완전성(completeness)을 정의할 수 있다. 주어진 수열로부터 만들어질 수 있는 길이가 k 인 모든 부분수열의 집합이 P 에 속하는 원소들을 사용하여 만들 수 있는 k 의 길이에 해당하는 모든 순열(permutation)을 포함하고 있을 때 그 수열을 완전한 수열이라 부르며 $\mathbf{C}(p, k)$ 로 표기한다.

그리고, 유일성과 완전성을 모두 갖춘 수열을 완벽성(perfectness) 을 갖고 있다고 정의하며 $\mathbf{P}(p, k)$ 로 표기한다. 이러한 서로 맞물린 수열의 성질에 대한 상세한 내용은 [4] 에 나타나 있다.

2.2. 암호행렬의 생성

암호행렬은 서로 맞물린 수열로부터 생성적(generative)인 기법을 사용하여 만든다. 암호행렬을 생성하는 방법은 유한상태천이(finite state transition)를 사용하는 도약연산(jump operation)으로 암호행렬의 첫째 열을 정의한 후 이 수열의 각 원소에 주어진 수 만큼의 상태천이를 반복하여 새로운 열들을 생성함으로써 행렬을 구성한다. 이때 암호행렬의 첫째열과 같이 도약연산의 기본이 되는 수열을 기본수열이라 부르고 상태천이(도약)의 수를 제공하는 수열을 도약수열이라 부르며 도약연산은 '기본수열 ⊙ 도약수열' 로 나타낸다. 예를 들어 (1 2 3) ⊙ (1) 은 (2 3 1) 을 생성하며 여기에 도약수열 (2) 를 이어서 적용시키면 (1 2 3) (=(2 3 1) ⊙ (2)) 이 얻어진다. 이때 같은 결과가 도약연산을 수열로 적용시킨 즉 (1 2 3) ⊙ (1 2) 에 의해서도 얻어질 수 있음을 안다.

서로 맞물린 암호행렬의 대표적인 예인 유일하게 구성되는 암호행렬을 생성하기 위해서는 기본수열을 $\mathbf{P}(p, 3)$, 즉 주어진 P 와 길이가 3 인 부분수열에 대해 완벽성을 지닌 서로 맞물린 수열로 하여야 하고, 도약수열 또한 $\mathbf{P}(p, 2)$ 이어야 한다. 이때 주어진 P 에 대해 $\mathbf{P}(p, 3)$ 와 $\mathbf{P}(p, 2)$ 를 발생시킬 수 있는 일반적인 방법이 저자에 의해 개발된 바 있고 [1], 이 방법에 의하면 $p = 3$ 일때의 기본수열은 (3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3) 이고 도약수열은 (3 1 2 1 1 3 2 2 3 3) 이다. 이러한 기본수열과 도약수열을 이용하여 생성된 유일하게 구성된 암호행렬이 [그림-2] 에 나타나 있다.

3. 암호행렬과 암호의 특성

암호행렬을 각 행의 관점에서 보면 각 행은 어떤 원소값에 도약수열을 적용시켜 생성됨을 안다. 즉, 예를 들어 (1) ⊙ (3 1 2) 는 $(1\ 1\ 2\ 1)^{\mathrm{T}}$ 를 생성하게 된다. 이러한 도약연산은 다음과 같은 흥미로운 성질을 갖는다.

정리 1 : 도약연산 (n) ⊙ $\mathbf{U}(p, k)$ 는 또다른 하나의 $\mathbf{U}(p, k+1)^{\mathrm{T}}$ 를 생성한다.

3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3
3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3
1 1 2 1 3 2 1 2 2 3 1 2 3 3 2 3 2 2 2 1 1 3 1 3 3 3 1 1 1
3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3
1 1 2 1 3 2 1 2 2 3 1 2 3 3 2 3 2 2 2 1 1 3 1 3 3 3 1 1 1
2 2 3 2 1 3 2 3 3 1 2 3 1 1 3 1 3 3 3 2 2 1 2 1 1 1 2 2 2
2 2 3 2 1 3 2 3 3 1 2 3 1 1 3 1 3 3 3 2 2 1 2 1 1 1 2 2 2
1 1 2 1 3 2 1 2 2 3 1 2 3 3 2 3 2 2 2 1 1 3 1 3 3 3 1 1 1
3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3
3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3
3 3 1 3 2 1 3 1 1 2 3 1 2 2 1 2 1 1 1 3 3 2 3 2 2 2 3 3 3

[그림-2] $p = 3$ 일때 유일하게 구성되는 암호행렬

증명 : 도약수열 $\mathbf{U}(p, k) = (\delta_1, \delta_2, ..., \delta_l)$ 라 하고, $\mathbf{U}(p, k)$ 에서 두개의 서로 다른 부분수열 $(\delta_i, \delta_{i+1}, ..., \delta_{i+k-1})$ 과 $(\delta_j, \delta_{j+1}, ..., \delta_{j+k-1})$, $i \neq j$ 를 정의하자. 이때 부분수열의 길이가 k 이면 도약연산의 결과는 $k+1$ 인 수열이 됨을 안다. $(\delta_i, \delta_{i+1}, ..., \delta_{i+k-1})$ 을 사용한 도약연산에서 길이가 $k+1$ 인 부분수열 $(x_1, x_2, ..., x_{k+1})^T$ 가 얻어지고 $x_2 = x_1 \odot (\delta_i)$ 라 한다면, 이 부분수열이 유일하다는 것을 보이는 것은 $\mathbf{U}(p, k)$ 를 적용한 전체 연산 결과에서 $(x_1, x_2, ..., x_{k+1})^T$ 와 같은 부분수열이 다른곳에서는 존재하지 않음을 보이는 것과 같다.

만약 $(x_1, x_2, ..., x_{k+1})^T$ 와 같은 부분수열이 다른곳에 존재하고 이것을 $y_2 = y_1 \odot (\delta_j)$ 인 $(y_1, y_2, ..., y_{k+1})^T$ 라 하면 $x_1 = y_1, x_2 = y_2, ..., x_{k+1} = y_{k+1}$ 이 된다. 따라서 $x_1 \odot (\delta_i) = x_2 = y_2 = y_1 \odot (\delta_j) = x_1 \odot (\delta_j)$ 가 되므로 $|\delta_i - \delta_j| = mp$, $m \in \mathbf{N}$ 가 된다. 여기서 $\delta_i, \delta_j \leq p$ 가 됨을 알고 있으므로 $0 \leq |\delta_i / p - \delta_j / p| = m < 1$ 이 되어 이러한 관계식을 만족하는 가능한 m 값은 0 뿐이다. 따라서 $\delta_i = \delta_j$ 가 되고 이와 같은 과정을 모든 x 와 y 에 대해서 수행한다면 $(\delta_i, \delta_{i+1}, ..., \delta_{i+k-1}) = (\delta_j, \delta_{j+1}, ..., \delta_{j+k-1})$ 라는 결론에 도달하게 되어 $\mathbf{U}(p, k)$ 가 유일성을 갖는다는 것과 모순된다. ■

정리 2 : $n \in P$ 인 모든 n 에 대하여 도약연산 $(n) \odot \mathbf{P}(p, k)$ 으로부터 얻어지는 각 수열은 길이가 $k+1$ 인 부분수열에 대해 유일성은 보존하나 완전하지는 않다. 그러나 서로 상호보완적(complementary)으로 이들 모두는 길이가 $k+1$ 인 부분수열의 완전한 집합을 형성한다.

정리 2 를 증명하기에 앞서 정리 2가 의미하는 바를 예를 통해 살펴보면 다음과 같다.

예 : $P = \{1, 2, 3\}$ 이라 하자. (1) $\odot$ $\mathbf{P}(3, 2)$ 은 $(1) \odot (3\ 1\ 2\ 1\ 1\ 3\ 2\ 2\ 3\ 3) = (1\ 1\ 2\ 1\ 2\ 3\ 3\ 2\ 1\ 1\ 1)^T$ 가 되고, $(2) \odot \mathbf{P}(3, 2)$ 은 $(2\ 2\ 3\ 2\ 3\ 1\ 1\ 3\ 2\ 2\ 2)^T$ 가 되고, $(1) \odot \mathbf{P}(3, 2)$ 은 $(1) \odot (3\ 1\ 2\ 1\ 1\ 3\ 2\ 2\ 3\ 3) = (3\ 3\ 1\ 3\ 1\ 2\ 2\ 1\ 3\ 3\ 3)^T$ 가 된다. 이때 얻어진 세 개의 수열들은 길이가 3 인 부분수열에 대해 각각 유일성을 갖고 있다. 이 세 개의 수열로부터 길이가 3 인 부분수열들을 구해보면 서로 중복됨이 없이 P 로부터 형성될 수 있는 모든 순열을 포함하는 완전한 집합이 됨을 안다.

증명 : 완벽성을 갖는 수열은 정의에 의해 유일성을 갖고 있음을 알고 정리 1 에 의해 이러한 수열을 도약수열로 하여 형성되는 수열또한 유일성을 갖게 됨을 안다. 여기서 얻어진 수열이 완전하다면 얻어진 수열은 $\mathbf{P}(p, k+1)$ 이되므로 수열의 길이가 $p^{k+1}+k$ 임을 쉽게 알 수 있는데, 도약연산 $(n) \odot \mathbf{P}(p, k)$ 은 $(p^k+k-1)+1 = p^k+k$ 가 되어 연산의 결과로부터 얻어진 수열은 완전하지 않음을 안다.

이제 각 n 과 여기에 도약연산을 적용시켜 얻어진 각각의 수열에는 길이가 $k+1$ 인 부분수열이 몇 개씩 존재하는지 살펴본다. 만약 도약연산에 의해 완벽한 수열이 생성되었다면 $\mathbf{P}(p, k+1)$ 가 되고, 그 안에서 길이가 $k+1$ 인 수열은 $(p^{k+1}+k) - (k+1) + 1$ 개가 발생한다. 그러나 각각의 생성된 수열에는 $(p^k+k) - (k+1) + 1$ 개의 부분수열이 있다. 여기서 이들의 比 $[(p^{k+1}+k) - (k+1) + 1] / [(p^k+k) - (k+1) + 1]$ 를 구해보면 p 가 됨을 알 수 있고 이는 곧 $|P|$ 가 됨을 의미한다. 또한 각각의 발생된 수열은 유일성을 갖고 각기 서로 다른 원소로 부터 도약연산에 의해 생겨났으므로 중복된 부분수열이 없음을 안다. 따라서 도약연산 $(n) \odot \mathbf{P}(p, k)$ 으로부터 얻어지는 수열들은 길이가 $k+1$ 인 부분수열의 완전한 집합을 형성한다. ■

이제까지 도약연산에 의해 특징 지워지는 암호행렬의 성격에 대해 살펴보았는데, 이를 기반으로 암호행렬내의 암호의 특성을 알아볼 수 있다. 앞으로의 논의는 암호들의 서로 맞물린 성질과 이제까지 살펴본 행렬자체의 성질을 가장 잘 나타낼 수 있는 유일하게 구성되는 암호행렬에 대해서만 하기로 한다.

따름정리 1-1 : 유일하게 구성되는 암호행렬내의 어떠한 한 암호를 구성하는 세로방향의 수열 $W_{i,j}^{\ v}$ 은 그 수열을 포함하는 행 j 에서 유일하게 존재한다.

증명 : 유일하게 구성되는 암호행렬은 $\mathbf{P}(p, 3) \odot \mathbf{P}(p, 2)$ 의 결과로부터 얻어지는 행렬로서 [그림-1] 에서 보듯이 한 암호를 가로방향의 세 개의 수와 세로방향의 세 개의 수로 볼 수 있다. 이때 이들 각각은 행과 열의 부분수열이므로 정리 1 에 의해 암호를 구성하는 세로방향의 수열은 그 수열을 포함하는 행에서 유일하게 존재함을 안다. ■

정리 3 : 유일하게 구성되는 암호행렬에서 $W_{i,j}^{\ v}$ 에 도약연산을 시켜 얻어질 수 있는 수열은

오직 그 수열이 나타난 열, 즉, 열 i 에서만 나타난다.

증명 : $W_{i,j}^{v} = (x_{i-1,j}, x_{i,j}, x_{i+1,j})^{T}$ 에 도약연산을 적용하여 만들어 지는 수열을 $(x_{k-1,l}, x_{k,l}, x_{k+1,l})^{T}$ 이라 할 때 $i = k$ 임을 보이면 된다.

$W_{i,j}^{v}$ 에 도약수열 (n) 을 적용시켜 도약연산을 행하면 $x_{k-1,l} = x_{i-1,j} \odot (n)$, $x_{k,l} = x_{i,j} \odot (n)$, $x_{k+1,l} = x_{i+1,j} \odot (n)$ 이다. 이 때 $x_{k,l}$ 은 $x_{k-1,l}$ 에 (δ_{k-1}) 의 도약을 적용시켜 얻어진 것이라는 것을 상기하면, $x_{k,l} = x_{k-1,l} \odot (\delta_{k-1}) = ((x_{i-1,j} \odot (n)) \odot (\delta_{k-1}) = (x_{i-1,j}) \odot (n+\delta_{k-1})$ 이며, 또한 같은 논리로 $x_{k,l} = x_{i,j} \odot (n) = ((x_{i-1,j}) \odot (\delta_{i-1})) \odot (n) = (x_{i-1,j}) \odot (n+\delta_{i-1})$ 이다. 따라서 $|(n+\delta_{k-1}) - (n+\delta_{i-1})| = mp$, $m \in \mathbf{N}$ 이 됨을 알 수 있는데 $0 \le |\delta_{k-1} / p - \delta_{i-1} / p| = m < 1$ 이므로 m 은 0 이어야 한다. 따라서 $\delta_{k-1} = \delta_{i-1}$ 이고 $\delta_k = \delta_i$ 이 된다. 만약 $i \neq k$ 이라면 이것은 유일하게 구성되는 암호행렬을 구성하는데 사용된 도약수열이 유일하지 않다는 것이므로 모순된다. ■

정리 3은 유일하게 구성되는 암호행렬에서 특정 암호를 쉽고 빠르게 찾는데 이용될 수 있는 성질을 제공한다. 정리 3의 논리를 행에 대해서도 적용한다면, 유일하게 구성되는 암호행렬은 암호행렬의 생성에 사용되는 기본수열이 완벽성을 갖고 이 기본수열로부터 도약연산이 적용되어 나머지 열들이 생성되므로 임의의 암호에 대해 행의 위치 j 는 그 암호를 구성하는 가로방향의 수열 $W_{i,j}^{h}$ 로부터 찾아낼 수 있음을 안다. 이러한 논의로부터 다음의 방법이 제시된다.

방법 : 유일하게 구성되는 암호행렬에서 임의의 암호 $W_{i,j}$ 의 위치 (i, j)는 행렬내에서 유일하게 결정되며, 열의 값 i 는 암호의 $W_{i,j}^{v}$로부터 도약연산을 시켜 얻을 수 있는 수열을 암호행렬의 첫 행으로부터 찾음으로써, 행의 값 j 는 $W_{i,j}^{h}$ 로부터 도약연산을 시켜 얻을 수 있는 수열을 암호행렬의 첫 열로부터 찾음으로서 쉽게 발견된다.

4. 결론

본 연구에서는 삼차원 비젼시스템의 개발시 실제적인 문제를 해결하기 위해 고안되었던 서로 맞물린 암호행렬이 갖고 있는 본질적인 특성에 대해 살펴보고자 하였다. 이를 위해 우선 암호행렬의 생성에 사용된 서로 맞물린 수열의 성질과 이러한 수열들로부터 암호행렬을 만드는 연산에 대해 간략히 알아보았고, 생성된 암호행렬이 갖는 기본적인 성격을 규명하였다. 또한 이러한 암호행렬로 부터 읽혀지는 암호의 특성을 살펴봄으로써 암호행렬의 응용시 적용될 수있는 이론적인 배경을 제공하였다.

본 연구에서 밝혀진 서로 맞물린 암호행렬의 특성들은 암호행렬의 형태변화나 암호의 해독 등에 이용될 수 있다. 이러한 이론적 성격을 바탕으로 암호행렬의 또다른 특성들을 발견하여 서로 맞물린 암호행렬의 응용분야를 확장하는 일 등은 앞으로의 과제로 남는다.

참고문헌

[1] P.M. Griffin, L.S. Narasimhan, and S.R. Yee, "Generation of uniquely encoded light patterns for range data acquisition," *Pattern Recognition*, vol.25, no.6, pp.609-616, 1992.

[2] P.M. Griffin and S.R. Yee, "The use of a uniquely encoded light pattern for range data acquisition," *Proc. 13th Annual Conf. Computers & Industrial Engineering*, vol.21, nos.1-4, pp.359-363, 1991.

[3] S. R. Yee and P. M. Griffin, "Three-dimensional imaging system," *Optical Engineering*, vol.33, no.6, pp.2070-2075, 1994.

[4] S. R. Yee, "Interlocking Number String and Code Matrix, *Proc. of ICC & IE '95*, pp.1465-1468, 1995.