논문 2011-48CI-1-17

# 히스토그램 기반의 강인한 계층적 GLOCAL 해쉬 생성 방법

## ( Robust Hierarchical GLOCAL Hash Generation based on Image Histogram )

최 용 수*, 김 형 중**, 이 달 호***

( Yong Soo Choi, Hyoung Joong Kim, and Dal Ho Lee )

요 약

최근 들어, 웹 응용의 하나로 이미지를 통합 관리하는 이미지 거래소(Image Stock), 이미지 도서관(Image Library)과 같은 응용들이 많이 만들어 지고 있다. 이미지의 등록, 관리, 검색에는 주로 이미지 해쉬라는 기술이 구분자(Identifier)로서 쓰이며 해쉬의 분별력을 높이기 위한 연구들이 많이 진행되어지고 있다. 본 논문에서는 계층적 히스토그램을 이용한 GLOCAL(Global to Local) 이미지 해쉬 생성 방법을 제안하였다. 많은 연구들이 이미지 처리 및 기하학적 공격에 강한 히스토그램 기반의 이미지 해쉬 기법들을 제안하였으며 제안된 논문에서는 GLOCAL 해쉬 생성과 가중치(Weighting Factor)를 적용하여 해쉬의 안정성을 높이는데 기여하였다. GLOCAL 해쉬 생성 방법에 의해 기존의 알고리즘들은 좀더 풍부한 길이의 이미지 해쉬를 생성하였다. 즉, 이미지 해쉬의 근본 목적인 Identification과 Discrimination 이라는 두 가지 목적을 잘 달성하였으며 그 결과는 통계학적 가설 검정(Statistical Hypothesis Testing)을 통해 기존의 알고리즘과 비교하였으며 대부분의 공격종류에 대해 제안된 알고리즘이 향상된 성능을 보여줌을 확인하였다.

Abstract

Recently, Web applications, such as Stock Image and Image Library, are developed to provide the integrated management for user's images. Image hash techniques are used for the image registration, management and retrieval as the identifier and many researches have been performed to raise the hash performance. This paper proposes GLOCAL image hashing method utilizing the hierarchical histogram which based on histogram bin population method. So far, many researches have proven that image hashing techniques based on histogram are robust image processing and geometrical attack. We modified existing image hashing method developed by our research team. The main idea is that it makes more fluent hash string if we have histogram bin of specific length as shown in the body of paper. Finally, we can raise the magnitude of hash string within same context or feature and strengthen the robustness of hash.

**Keywords**: Image Hash, Hierarchical Hash Generation, Robustness, Statistical Hypothesis Testing

## I. 서 론

일반적으로 해쉬함수는 데이터 무결성(Integrity) 및 메시지 인증 등에서 사용할 수 있는 함수로써 정보보호의 여러 메커니즘에서 이용되는 핵심 요소기술이다. 해쉬함수란 입력 데이터 스트링을 고정된 길이의 출력인 해쉬코드로 대응시키는 함수로서 두 가지 기본 요구조건을 가진다. 첫째, 주어진 해쉬코드에 대하여 이 해쉬코드를 생성하는 데이터 스트링을 찾아내는 것은 계산

* 정회원-교신저자, ** 평생회원, 고려대학교 정보경영공학전문대학원
(Graduate School of Information Management & Security, Korea University)
*** 정회원, 경원대학교 전자공학과
(Department of Electronic Engineering, Kyungwon University)
※ "본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2010년도 문화콘텐츠산업기술지원사업의 연구결과로 수행되었음", 또한 "이 연구는 2010년도 경원대학교 지원에 의한 결과임."
접수일자: 2010년11월19일, 수정완료일: 2010년12월30일

상 실행 불가능하며, 둘째 주어진 데이터 스트링에 대하여 같은 해쉬코드를 생성하는 또 다른 데이터 스트링을 찾아내는 것은 계산상 실행 불가능하다는 두 가지 성질을 만족하는 함수를 말한다. 대체적으로 파일 시스템에서 입력파일의 고유한 저장공간을 만들고 검색에 이용하기 위해 해쉬함수를 많이 이용해 왔다. 파일의 길이에 관계없이 키를 이용하여 고정된 길이를 가지는 해쉬코드로 압축하여 생성하고 생성된 해쉬를 기반으로 해당 파일의 저장 및 검색에 이용한 것이다.

이미지 해쉬 생성 방법은 이미지를 고정 길이의 이진 스트링으로 매핑하는 기술이며 생성된 해쉬는 구분자(Identifier) 또는 요약자(Descriptor)로 쓰인다. 이미지 해쉬 함수는 지각적으로 동일한 이미지에는 동일한 해쉬 값이 생성될 확률이 높도록 설계되어야 한다. 반면, 지각적으로 다른 이미지는 독립적인 해쉬 값을 생성해야 한다. 더욱이, 해쉬 함수는 안전(악의적인 공격에 강인)해야 함과 동시에 악의적인 공격자가 알려진 이미지의 해쉬 값을 예측하지 못하여야 한다. 이미지 해쉬는 이미지 데이터베이스의 이미지를 정렬하고 검색하는데 사용되기도 하지만 워터마크 삽입을 위한 비디오 프레임을 선택에도 사용한다[1~5].

이미지 해쉬 또한 컨텐츠의 저장 및 검색에 쓰기위한 목적은 동일하나 두 가지 정도의 측면에서 전통적인 해쉬와 틀리다고 할 수 있다. 첫째, 이미지의 특성(히스토그램, 컨텍스트 등)을 이용하여 해쉬스트링을 생성한다. 둘째, 이미지의 특성을 이용하므로 동일한 해쉬가 생성되는 경우가 발생한다. 특히, 인간의 시각에서는 전혀 틀린 이미지일지라도 동일한 해쉬가 생성되는 것이 가능하므로 무결성의 법칙을 위반하게 된다. 이미지는 행렬(Matrix) 형태로 구성되어 있기에 최근에는 행렬의 연산을 이용하여 고유한 해쉬를 생성해내는 방법들이 연구되어지고 있지만 여전히 완벽한 이미지 해쉬를 생성해 내는 것은 어려운 영역이다[6~10].

전술한 바와 같이 이미지에 있어 전체 데이터를 모두 쓰지 않는 이상 고유한 해쉬를 생성해 내는 것은 현재로서는 쉽지 않으므로 틀린 이미지에 대한 높은 변별력(Discrimination) 그리고 동일하거나 비슷한 이미지(필터나 잡음첨가와 같은 일반적인 신호처리 공격이나 회전, 자르기 등과 같은 기하학적 공격)에 대한 동일성(Identification) 능력을 향상시키는데 주로 중점을 두고 연구를 수행하고 있다. 특히 히스토그램 평활화(Histogram Equalization)공격은 대부분의 이미지 해쉬 생성 알고리즘에서 매우 취약적인 것으로 밝혀지고 있으며 향후 이미지 해쉬 생성 알고리즘 개발에 있어 상당히 중요한 연구 영역이 될 것이다[11~17].

본 논문에서는 대부분의 영상처리 공격 및 기하학적 공격에 강인한 히스토그램 기반 해쉬 생성방법을 이용하며 동일한 길이의 히스토그램으로 더 높은 무결성을 지닌 해쉬가 발생되도록 계층적 해쉬 생성 방법을 제안하였다.

Ⅱ장에서는 히스토그램 기반 해쉬 생성 방법에 대해서 소개한다. Ⅲ장에서는 본 논문에서 제안하는 계층적 GLOCAL 해쉬 생성 방법에 대해 설명한다. Ⅳ장에서는 제안된 방법을 실제의 이미지 데이터베이스에 적용한 실험과 통계적 가설 검정 방법에 의한 결과를 기존의 알고리즘과 비교하며 마지막으로, Ⅴ장에서 결과를 바탕으로 제안된 방법에 대해 결과를 논한다.

## Ⅱ. 히스토그램 기반 해쉬 생성

### 1. 히스토그램 Bin 기반의 해쉬 생성

이미지 해쉬 생성 기술은 (그림 1)과 같은 순서에 의해 이미지의 특징검출 및 압축하여 이진 스트링(Hash Value)를 생성한다. 이미지특징 중 히스토그램을 이용한 것이 히스토그램 기반의 이미지 해쉬 생성 기술이며 Perceptual 해쉬의 한 종류로서 많은 연구가 되어지고

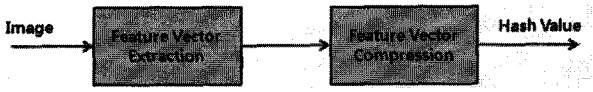


그림 1. 이미지 해쉬 생성 블럭도
Fig. 1. The Block Diagram of Image Hash Generation.

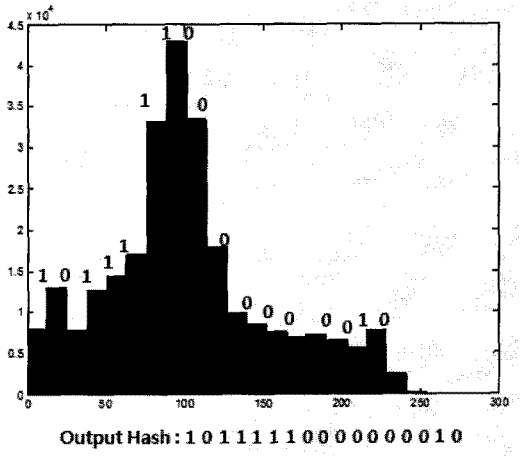


그림 2. 히스토그램 빈 기반의 해쉬 생성
Fig. 2. Hash Generation based on Histogram Bin.

있다[18].

일반적으로 히스토그램 기반 해쉬 생성 기법에서 Bin Population을 이용한 방법이 일반적 신호처리 및 기하학적 공격에 강한 것으로 알려져 있으며, Bin의 크기가 클수록 강인성은 증대됨이 입증되어왔다[18].

일반적인 히스토그램 Bin 기반의 해쉬 생성 방법은 (그림 2)와 같이 히스토그램을 구간(Bin)으로 분할한 다음 각 Bin의 빈도 값의 차를 이용하여 hash를 생성한다[20]. (그림 2)의 예에서는 i번째 Bin의 빈도가 i+1번째 Bin의 빈도보다 작으면 1, 반대일 경우 0의 해쉬 비트를 생성한다.

## III. 히스토그램 기반의 계층적 해쉬 생성

2장에서 언급한 바와 같이 Bin 기반의 히스토그램 해쉬 생성이 강인하다는 주장이 명백하다면, 더 넓은 Bin을 이용하게 되면 해쉬는 더욱 강건할 것이다. 하지만 Bin의 크기가 커질수록 생성되는 해쉬의 길이는 작아진다. 이와같은 Bin의 넓이와 생성 해쉬의 길이의 상관관계를 재정립하기 위해, 본 논문에서 해쉬의 강건성은 유지한 채 생성되는 해쉬의 길이는 더욱 길어지도록 계층적 해쉬 생성 방법을 제안하는 것이다. 간단한 예로, (그림 2)와 같은 히스토그램 빈 기반 방법에서 8개의 Bin을 가진다고 가정하면 7 비트의 해쉬를 생성하는 것이 가능하다. 하지만 (그림 3)과 같이 제안하는 계층적 해쉬 생성 방법에서는 11 비트의 해쉬열이 생성되는 것이다. 본 논문에서는 이러한 해쉬 생성기법을 GLOCAL(Global to Local) 해쉬 기법이라 명명한다.

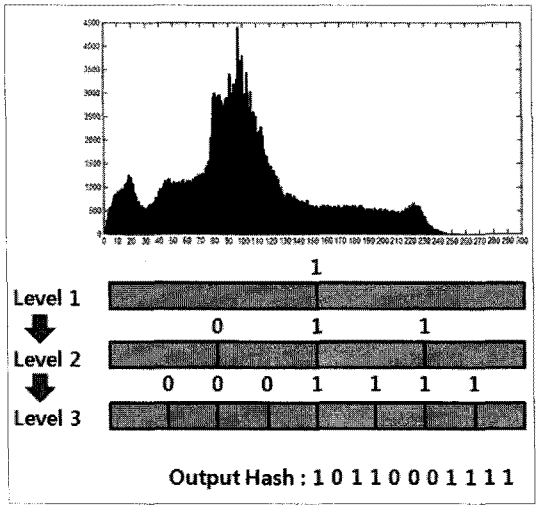


그림 3. 히스토그램 기반의 제안된(GLOCAL) 해쉬 생성 과정

Fig. 3. Proposed Hash Generation based on Histogram.

(그림 3)은 GLOCAL 해쉬 생성의 개념을 표현한 것으로 다음과 같은 과정을 따르게 된다.

Level 1: 히스토그램을 두 개의 Bin으로 나누고 Bin의 크기를 비교하여 해쉬를 생성한다.

Level 2: 상위 Level에서 하나의 Bin을 2개의 Bin으로 나누어 2배의 Bin이 생성되도록 만든 후 해쉬를 생성한다.

반복: 사용자가 정한 Level 까지 위의 Level 2 과정을 반복한다. 이때 Bin의 개수 n(Bin)은 $2 \le n(Bin) \le unique(I)$이다. 여기서 unique 함수는 입력영상 $I$의 컬러의 개수를 의미한다.

원본 히스토그램의 Bin분할을 Level 3까지 진행한다고 가정하면, Bin의 수($N$)는 $2^3$=8이며 일반적인 해쉬는 $N-1$ 비트의 해쉬열이 생성가능하다. 반면, 제안된 방법에서 해쉬의 길이는 Level의 수에 따라 아래 수열과 같이 생성된다.

$$L_1, L_2 = 2L_1 + 1, \ldots, L_i = 2L_{i-1} + 1 \quad , 단, i = Level수 \tag{1}$$

여기서, $L_1$은 Level 1의 해쉬 길이를 의미하므로 1, $L_i$는 $i$번째 Level에서 생성되는 해쉬의 길이를 의미한다. 제안된 해쉬의 길이를 등비수열을 이용하여 계산하면 아래식과 같이 표현되어 진다.

$$L_{total} = \sum_{1}^{i} L_1 + L_2, \ldots, + L_i = 4(r^{i-1} - 1) - i + 2 \tag{2}$$

여기서 $r$은 매 Level 증가 시 Bin 분할 배수, $i$는 Level 의 수 이다. (그림 3)의 예에서, $L_1$=1, $r$=2, $i$=3 이므로 11 비트의 해쉬를 생성하는 것이다. 해쉬 길이의 차를 수식으로 표현하면 다음 식 3과 같다.

$$4(r^{i-1} - 1) - i + 2 - (ar^{i-1} - 1) \tag{3}$$

하지만, 본 논문의 실제 실험환경에서는 (그림 3)의 Level 진행 순서를 역으로 변형하였다. 먼저 마지막 Level의 Bin(가장 작은 너비의 Bin)의 넓이를 구한다음 단계를 증가할수록 이웃하는 Bin을 통합하는 방향으로 구현을 하였다. 2개의 Bin부터 분할을 시도하는 경우에는 해쉬 생성 중간에 해쉬의 강인성을 보장하는 Bin의

표 1. 64 Bins 기준 제안 방법의 해쉬 생성 능력
Table 1. Hash Generation Performance based on 64 Bins.

| Numbers of Level | Proposed |
|---|---|
| 2 | 94 bits |
| 3 | 109 bits |
| 4 | 116 bits |
| 5 | 119 bits |
| 6 | 120 bits |

넓이를 측정하는 단계가 삽입되어야 하므로 이러한 문제를 해결하기 위해 최소의 Bin 크기부터 시작하여 Bin을 통합하는 순서로 진행을 한다.

히스토그램의 Bin이 64개일 경우, 인접하는 Bin의 비교를 통해 해쉬를 생성하는 일반적인 방법을 쓰게되면 63 비트의 해쉬를 생성하게 된다. 하지만 계층적 해쉬 생성 방법인 GLOCAL해쉬 생성을 적용하면 아래 표 1과 같이 Level을 늘려갈수록 기존 해쉬 길이에 비해 점점 더 가된 길이의 해쉬를 생성하게 된다.

표 1의 해쉬 증가량을 Level 1(63 비트)를 기준으로 표시하면 아래의 (그림 4)와 같이 표시된다. Level의 수가 증가할수록 증가율은 감소하나 3단계의 Level만 적용하여도 70% 해쉬길이를 증가시키므로 고정길이 히스토그램 대비 높은 해쉬 생산성을 보일 수 있다.

또한, 이미지 해쉬의 목적을 크게 두 가지 1) 일정한 변형을 포함하였어도 동일한 이미지를 같다고 판정을 하는 것 2) 비슷해 보이지만 틀린 이미지를 경우 판별하는 것. 이므로 두 가지 조건을 동시에 만족하는 해쉬 생성 방법을 찾아내는 것이 필요하다. 본 논문의 3장에서 통계학적 가설 검증을 통하여 제안한 해쉬 생성 방법을 이용하여 위의 두 조건을 최대한 만족하는 임계점을 찾는다.

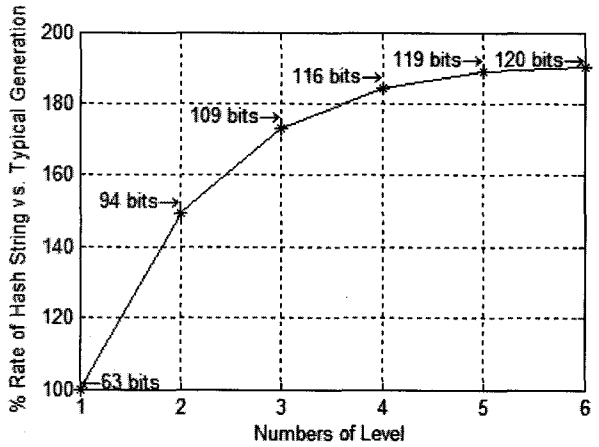


그림 4. 제안된 해쉬 생성 방법의 성능
Fig. 4. Proposed Hash Generation Performance.

## IV. 실험 및 결과

본 논문의 구현에 있어 프로그래밍은 MATLAB Ver 7.2에서 작성하였으며 실험 이미지로는 Corel Draw Database의 이미지 1173개를 사용하였다. 이 데이터베이스는 사물, 풍경, 동물, 컴퓨터 그래픽 등 다양한 사진을 포함하고 있다. 영상처리 및 기하학적 공격은 16종류(대표적인 공격 중 선택)이며: JPEG 압축 Quality factor 70%~100%: 4가지, 노이즈 첨가 0.001~0.01: 3가지, 회전 1°~10°: 4가지, 히스토그램 평활화: 1가지, 이미지 잘라내기 10%~25%: 2가지, Median 필터 크기 3×3~5×5: 2가지를 사용하였다. 또한 객관적인 비교를 위하여 현재 개발된 이미지 해쉬 생성 알고리즘 중 강력하다고 알려진 두 가지 기술(SVD: Singular Vector Decomposition와 NMF: Non-Negative Matrix Factorization 기반 해쉬 생성 알고리즘[1~2])을 함께 구현 및 평가하였다.

### 1. 통계학적 검증 방법

본 논문에서는 제안된 방법에 의해 생성된 해쉬 알고리즘의 성능을 객관적이고 논리적으로 증명하기 위하여 통계학적 가설검정 방법을 이용하였다. 통계학적 가설검증을 수행함에 있어 정의는 다음과 같다.

- 귀무가설($H_0$): 두 이미지는 틀리다.
- 대립가설($H_1$): 두 이미지는 지각적으로 동일하다.
- 유의수준(significance level) : 제 1종 오류를 범할 확률의 허용한계를 미리 정해줄 때 이 한계값.

본 논문의 실험에서는 16가지의 공격 형태를 가지게

표 2. 가설 검증에 따른 에러의 종류
Table 2. Error Types according to Hypothesis Testing.

| | | 판단 | |
|---|---|---|---|
| | | $H_0$ | $H_1$ |
| 가설 | $H_0$ | | Type I error |
| | $H_1$ | Type II error | |

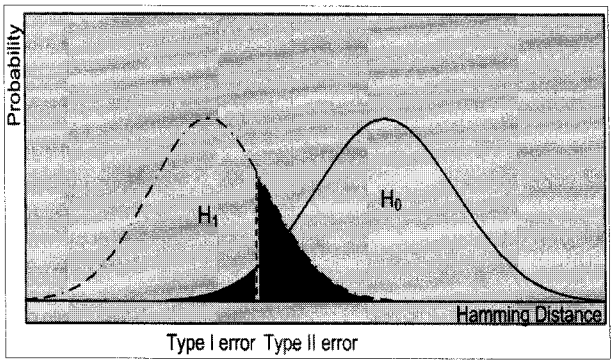


그림 5. 제 1종, 2종 오류의 개념도
Fig. 5. The Concept of Type I and II error.

되므로 기준이 되는 귀무가설을 "두 이미지는 틀리다"로 정하고 각 공격별로 대립가설의 확률 분포도를 각각 적용하게 된다. 즉, 표 2에 나타난 제 1종 오류는 다른 이미지를 지각적으로 같다고 판단하는 경우이며, 제 2종 오류는 지각적으로 동일한 이미지를 다른 이미지로 판단하는 경우를 말하게 된다.

(그림 5)와 같이 귀무가설($H_0$)에 대한 해밍거리의 확률분포가 오른쪽 그래프와 같으며 대립가설($H_1$)에 대한 해밍거리의 확률분포는 왼쪽 그래프와 같다. 여기서 귀무가설에 대한 제 1종 오류(파랑색 영역)의 유의수준에 따라 경계 값(세로 점선)이 얻어지고 이에 따른 대립가설의제 2종 오류(빨강색 영역)를 계산할 수 있다.

본 논문의 실험환경에서는 16가지의 영상처리 및 기하학적 공격을 수행하였으므로 다음과 같은 순서에 의해 제 1,2종 오류를 얻어낸다.

단계 1: 귀무가설에 대한 제 1종 오류의 유의수준을 5%로 정한다. 통계학적 가설검정에서 일반적으로 5%의 제 1종 오류 수준을 정하는 것이 가장 대표적이므로 본 논문에서도 같은 수치를 사용하였다.

단계 2: 제 1종 오류 확률에 해당하는 귀무가설의 경계 값을 얻는다.

단계 3: 귀무가설의 경계 값을 적용하여 대립가설의 제 2종 오류 확률을 계산한다.

단계 4: 16가지의 공격에 대해 Step 3의 동작을 반복수행하며 각 공격에 대한 제 2종 오류의 확률을 얻는다.

위의 Step 1~4에 의해 얻어진 가설 검정 분포도를 (그림 6)과 (그림 7)처럼 얻을 수 있다. 실제 16개의 가설검정 분포도를 가지지만 예시를 위해 두 종류의 분포도만을 도시하였다. (그림 6)은 대립가설로서 "원본 이미지와 Noise Addition공격을 받은 이미지는 동일하다."를 가지며 (그림 6)은 "원본 이미지와 1° 회전 공격을 받은 이미지는 동일하다."를 대립가설로 가진다. SVD 및 NMF 해쉬 알고리즘에 대한 제 2종 오류도 위와 동일한 방법(단계 1~4)에 의해 얻어낸다.

## 2. 제안된 해쉬 생성 방법과 기존의 방법 비교

앞의 장에서 언급한 바와 같이 Type I 에러(유의 수준)를 약 5%로 정한 후 경계 값(Critical Value)을 구하고, 경계 값에 기반해 여러 가지 공격에 대한 Type II 에러를 측정하여 표 3에서 기술하였다. 데이터베이스의 이미지를 n(=1173)개 사용하므로 귀무가설의 집합은 $\frac{n\times(n-1)}{2}$개의 해밍 거리를 가진다. 왼쪽의 식에 적용하면 실험에서는 687,378개의 해밍거리를 가지게 된다. 이 귀무가설의 분포에 유의수준 5%를 적용함으로서 경계 값을 얻게 되고, 1173개 이미지는 공격별로 1173개의 사본 공격이미지를 가지게 되므로 각 공격 유형별로 대립가설은 1173개의 해밍거리집합을 가지게 된

표 3. 16가지 공격에 대한 Type II 에러의 비교
Table 3. Comparison of Type II errors against 16 Types of attack.

| | Proposed | SVD | NMF |
|---|---|---|---|
| JPEG 70% | 0 % | 0 % | 0.17 % |
| JPEG 80% | 0 % | 0 % | 0.34 % |
| JPEG 90% | 0 % | 0 % | 0 % |
| JPEG 100% | 0 % | 0 % | 0 % |
| Noise Addition 0.001 | 1.71 % | 6.56 % | 10.83 % |
| Noise Addition 0.005 | 1.62 % | 6.99 % | 10.91 % |
| Noise Addition 0.01 | 0.68 % | 7.50 % | 11.34 % |
| Rotation 1° | 3.24 % | 1.79 % | 41.77 % |
| Rotation 2° | 6.48 % | 5.54 % | 71.18 % |
| Rotation 5° | 8.01 % | 30.69 % | 89.77 % |
| Rotation 10° | 28.39 % | 64.36 % | 95.14 % |
| Histogram Equalization | 93.86 % | 23.70 % | 38.87 % |
| Cropping 10% | 3.07 % | 40.58 % | 66.92 % |
| Cropping 25% | 0.00 % | 6.65 % | 32.57 % |
| Median 3×3 | 0.09 % | 0.09 % | 1.79 % |
| Median 5×5 | 0.85 % | 0.68 % | 6.14 % |

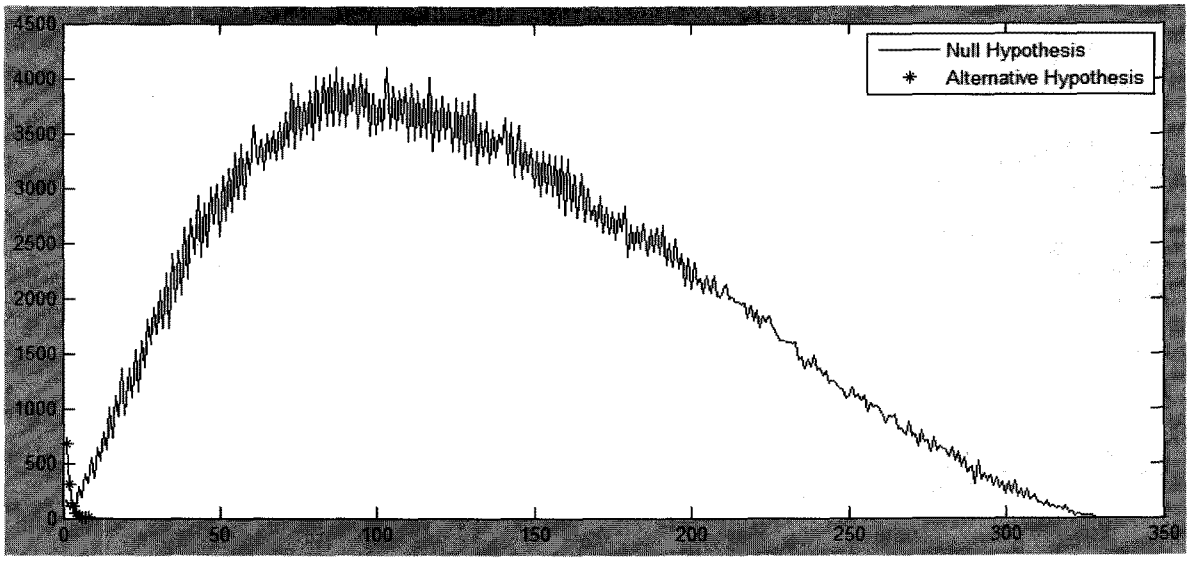


그림 6. 잡음첨가 공격에 대한 Hypothesis Testing
Fig. 6. Hypothesis Testing for Noise Addition Attack.

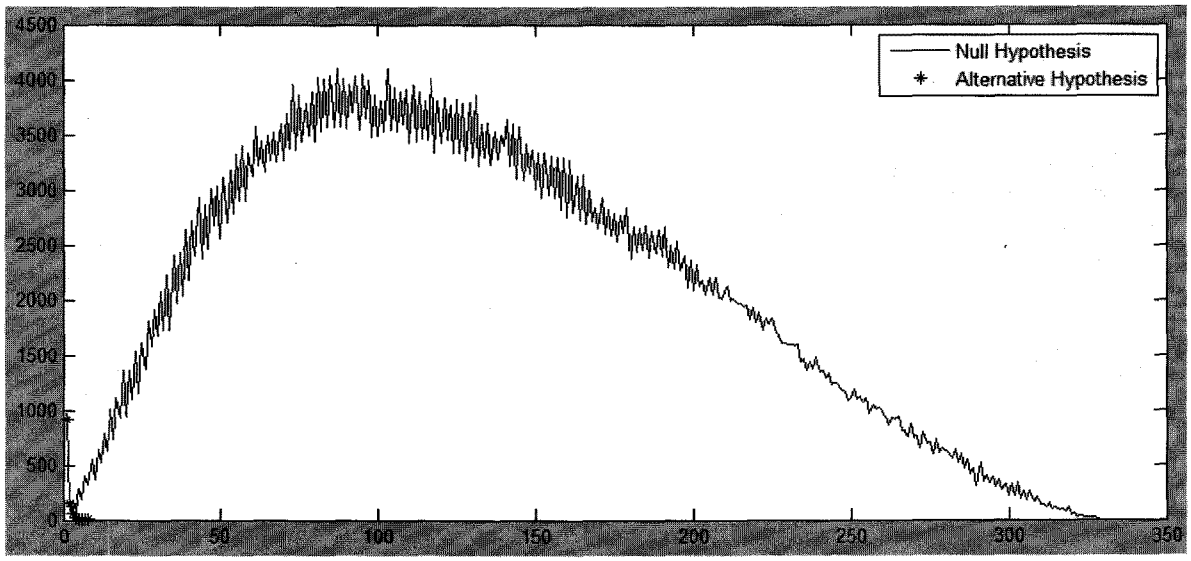


그림 7. 1° 회전 공격에 대한 Hypothesis Testing
Fig. 7. Hypothesis Testing for 1° Rotation attack.

다. 각각 16개 해밍거리 분포 표에 귀무가설에서 얻은 경계 값을 적용하여 아래 표 3을 얻을 수 있다.

표에서 보는 바와 같이 대부분의 공격에서 기존의 강력한 알고리즘인 SVD, NMF보다 향상된 성능을 보임을 확인할 수 있다. 하지만 히스토그램 평활화 공격은 여전히 취약함을 보이지만 대부분의 히스토그램 기반 해쉬 알고리즘이 가진 약점이라고 본다면 성공적인 분별능력을 보였다고 할 수 있다. 특히, JPEG과 같은 압축 변형에 대해서는 거의 완벽한 판별력을 제공하였고 대부분의 Noise Addition, 5° 이상의 Rotation 그리고 Cropping과 같은 변형들에 대해서도 뛰어난 향상을 보인 것이 측정되었다.

## V. 결 론

본 논문에서는 히스토그램 Bin기반의 해쉬생성 방법에서 해쉬 생성을 효율을 증가시키도록 GLOCAL (Global to Local) 해쉬 생성 알고리즘을 제안하였다. 실제 데이터베이스를 이용한 실험을 통해 얻은 해밍거리의 집합에 대해 통계학적 가설검증 기법을 이용하여

제안 방법의 성능을 비교 평가하였다. 실험을 통해 해쉬 생성의 효율성을 높이는 것을 증명하였으며 강력한 해쉬 생성 알고리즘으로 알려진 SVD 그리고 NMF 방법과 비교를 함으로서 객관적인 비교를 수행하여 대부분의 공격 방법에서 월등히 향상된 결과를 보임을 확인하였다. 대부분의 변형에 대해 0~5% 정도의 낮은 Type II 에러를 보였으며 히스토그램 평활화 공격에서의 높은 에러율은 대부분의 히스토그램 기반 알고리즘들에서 보여준 특성이므로 제안한 알고리즘만의 단점이라고 평가하기는 어렵다.

향후, 해쉬 bit들에 가중치의 부여하는 기준 및 가중치의 변화량 등을 조정함으로서 좀 더 향상된 강인성을 가진 해쉬를 생성해 낼 수 있을 것으로 예상한다. 즉, 일반적인 해쉬 생성 방법과 비교할 때 동일한 수의 해쉬 비트에러를 생성하더라도 가중치에 따라 새로운 해밍거리를 생성하도록 하는 것이 가능할 것이다. 또한, Bin의 분할 및 병합을 다양하게 수행함으로서 보다 효율적인 용량의 해쉬를 생성해 내는 것도 큰 이슈가 될 것으로 평가한다.

## 참 고 문 헌


[1] M. Johnson and K. Ramchandran, "Dither-Based Secure Image Hashing Using Distributed Coding," *Proc. IEEE Int. Conf. Image Processing*, September 2003.

[2] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," *Proceedings of the Computer Vision and Pattern Recognition*, pp. 257-263, 2003.

[3] H. J. Kim, S. Y. Kim, and H. Kim, "A new image hash computation method," *International Workshop on Ubiquitous Convergence Technology*, 2007.

[4] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copymove forgery in digital images" *Proceedings of Digital Forensic Research Workshop*, 2003.

[5] 이석환, 권기룡, "키 기반 블록 표면 계수를 이용한 강인한 3D 모델 해싱," *전자공학회논문지*, 제47권 CI편, 제 1호, 1-14쪽, 2010년.

[6] V. Monga and M.K. Mhcak, "Robust and Secure Image Hashing via Non-Negative Matrix Factorizations," *IEEE Transactions on Information Forensics and Security*, Vol. 27, No. 3, pp. 379-391, 2005.

[7] N. L. Johnson, S. Kotz, and N. Balakrishnan, "Continuous Uni-variate Distributions," John Wiley \& Sons Inc, vol 2, New York, 1995.

[8] Suleyman S. Kozat, and R. Venkatesan, M. Kivanc Mihcak, "Robust Perceptual Image Hashing via Matrix Invariants," *Proceedings of International Conference on Image Processing*, pp.3443-3446, 2004.

[9] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2, pp. 215-230, June 2006.

[10] Z. J. Tang, S. Z. Wang, X. P. Zhang, W. M. Wei and S. J. Su, "Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization," *Journal of Ubiquitous Convergence Technology*, Vol.2 No.1, pp. 18-26, 2008.

[11] E. Y. Chang, C. Li, J. Z. Wang, P. Mork, and G. Wiederhold, "Searching near replicas of images via clustering," *SPIE Multimedia Storage and Archiving Systems VI*, pp. 281-292, 1999.

[12] Y. Ke, R. Sukthankar, and L. Huston, "An efficient parts-based near-duplicate and sub-image retrieval system," *Proceedings of the ACM International Conference on Multimedia*, pp. 869-876, 2004.

[13] Li Chen and F. W. M. Stentiford, "Comparison of near-duplicate image matching," *European Conference on Visual Media Production*, pp. 38-42, 2006.

[14] J. J. Foo, J. Zobel, R. Sinha, and S. M. M. Tahaghoghi, "Detection of near duplicate images versions for web search," *Proceedings of the ACM International Conference on Image and Video Retrieval*, 2007.

[15] 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 Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22, pp. 1349-1380, 2000.

[16] B. Wang, Z. Li, M. Li, and W.-Y. Ma, "Large-scale duplicate detection for Web image search," *IEEE International Conference on Multimedia and Expo*, pp. 353-356, 2006.

[17] M. Yang, G. Qiu, J. Huang, and D. Elliman, "Near-duplicate image recognition and content-based image retrieval using adaptive hierarchical geometric centroids," *International Conference on Pattern Recognition*, pp. 958-961, 2006.

[18] S. Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," *Proceedings of the ACM Multimedia and Security Workshop*, pp. 121-128, 2007.

## 저 자 소 개

**최 용 수(정회원)-교신저자**

1998년 강원대학교 제어계측공학과 공학사.
2000년 강원대학교 제어계측공학과 공학석사.
2006년 강원대학교 제어계측공학과 공학박사.
2006년~2007년 연세대학교 첨단융합건설연구단 연구교수.
2007년~현재 고려대학교 정보경영전문대학원 연구교수.
2008년~현재 대한전자공학회 컴퓨터소사이어티 논문편집위원장
<주관심분야 : Multimedia Hashing, Information Hiding, Watermarking, Steganography>

**이 달 호(정회원)**

1982년 서울대학교 제어계측공학과 공학사
1985년 서울대학교 제어계측공학과 공학석사
1992년 서울대학교 제어계측공학과 공학박사
1992년~현재 경원대학교 전자공학과 교수
1992년 University of Southern California, 방문연구원
<주관심분야 : 시스템 식별, 필터링 기법, INS 응용, Data Hiding>

**김 형 중(평생회원)**

1978년 서울대학교 제어계측공학과 공학사.
1986년 서울대학교 제어계측공학과 공학석사.
1989년 서울대학교 제어계측공학과 공학박사.
1990년~2006년 강원대학교 교수.
2006년~현재 고려대학교 정보경영전문대학원 교수.
2008년 대한전자공학회 컴퓨터소사이어티 회장
<주관심분야 : Parallel Computing, Image Hashing, Data Compression, Reversible Data Hiding>