

디스플레이 시스템에서 발생하는 비의도적 전자기 방사에 의한 도청 위협에 강인한 보안 글꼴 및 색상 구조 설계

Design of Robust Security Fonts and Color Composition against Unintended Electromagnetic Emanations from Display Systems

최동훈 · 최원준 · 이의범 · 육종관

Dong-Hoon Choi · Won-Jun Choi · Euibum Lee · Jong-Gwan Yook

요 약

컴퓨터와 전자기술의 발전으로 사이버-전자전의 중요성이 점차 증가하면서 정보 보안의 역할이 점점 더 중요해지고 있다. 특히, 최근 몇몇 국가에서는 컴퓨터 모니터로부터 방출되는 전자파를 포착하여 해당 모니터의 디스플레이를 재구성하는 연구가 활발히 진행되고 있으며, 이러한 방식을 통해 화면에 표시된 기밀 데이터가 공격자에 의해 도난당할 경우, 크게는 국가 수준의 잠재적 보안 위협을 초래할 수 있다. 따라서, 본 논문에서는 전자파를 통한 정보 유출을 방지하기 위한 수단을 고찰하였으며, 구체적으로 보안 위협에 대응할 수 있는 TEMPEST 내성 글꼴과 글자 색과 글자 배경색의 색상을 활용한 추가적인 TEMPEST 대응 가능성에 대해 제안한다.

Abstract

With the advancement of computer and electronic technologies, the importance of cyber-electronic warfare has gradually increased, accentuating the role of information security. Recently, several countries have been actively researching the capture of electromagnetic waves emitted from computer monitors to reconstruct their displays. If confidential data displayed on a screen were to be stolen by attackers, they could potentially pose significant security threats, even at the national level. Therefore, this study explored a means of preventing information leakage via electromagnetic waves, specifically proposing using TEMPEST-resistant fonts and additional TEMPEST-resistant possibilities by utilizing font, text, and background colors in response to security threats.

Key words: TMDS, EMSEC (ElectroMagnetic SECurity), TEMPEST

I. 서 론

디지털 시대의 도래와 함께, 전자기기의 보편화는 정보 교환의 속도와 용이성에 혁신적인 이바지를 하였다.

하지만, 이러한 발전의 이면에는 전자파를 통한 정보의 무단 취득이라는 심각한 보안 위협이 존재하고 있다. 특히, 전자기기에서 미세하게 누설되는 전자파를 통해 의도하지 않게 정보가 유출될 수 있는데, 이 전자파에는 해당

「이 연구는 한국에너지기술평가원(KETEP)의 신에너지 기술의 표준화 및 인증 지원을 통해 대한민국 산업통상자원부로부터 재정적 지원을 지원받아 수행되었습니다 (번호 20217301010050).」

연세대학교 전기전자공학부(Department of Electrical and Electronic Engineering, Yonsei University)

· Manuscript received March 26, 2024 ; Revised April 4, 2024 ; Accepted May 3, 2024. (ID No. 20240326-030)

· Corresponding Author: Jong-Gwan Yook (e-mail: jgyook@yonsei.ac.kr)

기기에서 처리된 신호정보를 포함하기 때문에 원본 화면과 동일한 정보복원, 즉 모니터 도청이 가능하다. 이는 기존의 보안 대책이었던 패스워드 및 암호장치와 같은 시스템이 구축되었을지라도 화면상에 있는 정보를 물리적으로 복원하기 때문에 실효성이 없으며, 어떠한 흔적도 남지 않아 추적이 불가하다.

컴퓨터 모니터와 같은 전자기기에서 의도치 않게 발생하는 전자파를 수집 및 재구성함으로써 그 안에 포함된 전자정보를 도청, 탈취하는 기술을 템페스트(TEMPEST, transient electronic pulse emanation surveillance technology)라고 한다^{[1]~[6]}. 템페스트는 1985년 Van Eck에 의해 처음 학계에 보고된 이후, 주로 정보를 시각적으로 출력할 수 있는 컴퓨터 모니터를 대상으로 이루어져 왔으며, 최근에는 LCD 모니터 및 다양한 비디오 인터페이스의 등장으로 해당 장비들을 대상으로 하는 복원 연구가 진행되고 있다^[7]. 템페스트 프로세스의 일반적인 구성은 그림 1과 같이 구성된다. 첫째, 대상 모니터를 선정하고 전자파의 누설 발원지에 대한 정보를 확인하는 것으로 A/D 인버터, FFC 케이블, RGB 케이블들이 주요 누설원이다. 특히, FFC(flexible flat cable)의 경우, 패널과 A/D 인버터를 연결하는 선로이므로 RGB신호가 전송되는 곳이며, 완전한 차폐(shielding)가 되어 있지 않아 외부에서 쉽게 전자파 측정이 가능하다. 두 번째는 대상 모니터에서 누설된 전자파를 안테나 또는 근접 프로브(near-field probe)로 수신하여 자료화 하는 과정이다. 이 단계에서는 상황에 따라 대

역통과필터(band-pass filter) 및 저잡음 증폭기(low noise amplifier)를 이용해야 하는데, 이는 누설 전자파의 스펙트럼 신호 특성에 따라 다양한 주파수 성분이 포함되기 때문이다. 마지막 단계는 수집된 전자파를 분석하고 재구성하는 단계로써 정보복구 시스템을 이용해야 하며 이 시스템에 입력되는 정보에는 대상 모니터의 사양 정보가 있어야 한다. 또한, 재구성된 화면 정보의 화질개선을 위한 다양한 신호처리 기법이 적용된다. 최근, 다양한 연구를 통하여 사무실 환경과 같이 다중 모니터의 정보가 누설되는 환경에서도 연구가 수행되고 있다^{[8]~[10]}.

템페스트와 같이 잠재적인 위협을 초래할 수 있는 도청 방법에 대항하기 위해 설딩(shielding)과 전파 방해(jamming)와 같은 다양한 대응 수단으로써 제시되고 있다. 이 중, 차폐는 가장 효과적인 템페스트 대응 수단으로써 기기, 특정 구역을 금속 재료로 차폐하는 방법을 통하여 외부로의 전자파 정보 유출을 방어하는 방법이다. 그러나 비용과 시간을 많이 필요로 하는 단점이 존재하며, 이동성을 지닌 개인용 컴퓨터와 같은 장비에 적용하기에는 무게와 부피에 의해 사용자의 편의성을 심각하게 저해하는 큰 단점을 가지고 있다. 전자파 방해(electromagnetic inference) 또한 누설 전자파와 유사한 대역폭 특성이 있는 신호를 방사하여 본래의 정보에 혼란을 주는 수단이나, 이 역시 별도의 전파 방해 장비나 비디오 프로토콜별 다른 특성을 갖는 스펙트럼을 분석해야 하므로 실용성이 매우 떨어진다^{[11],[12]}.

본 논문에서는 위와 같은 어려움을 겪지 않고, 악의적인 외부 템페스트 공격에 일정 수준 대응할 수 있는 소프트웨어 템페스트 방법을 제안한다. 소프트웨어 템페스트의 대표적인 연구로는 보안성 있는 글꼴 설계 연구가 있으며, 이는 특별히 고안된 보안 글꼴을 활용함으로써 템페스트 공격을 통해 얻은 복원 화면으로부터의 정보 유출 가능성을 최소화하는 것이 목표이다^[13]. 하지만, 사전 수행된 관련 연구들은 대부분 유럽, 미국 등 템페스트를 주로 연구하는 국가에서 활용하는 문자인 라틴 알파벳(Latin script)을 대상으로 하다 보니 국내에서 활용할 수 있는 한글 글꼴에 관한 연구는 전혀 없는 실정이다. 따라서, 본 논문에서는 주요 한글 글꼴의 형태에 따른 누설 전자파 변화를 분석하고 템페스트 공격으로부터 정보를 보호할 수 있는 한

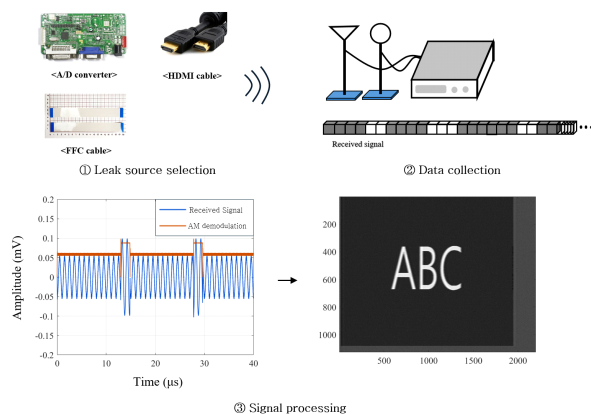


그림 1. 템페스트 프로세스

Fig. 1. TEMPEST process.

글 전용 템페스트 전용 폰트를 제시한다. 아울러, 제안하는 보안 글꼴의 효용성을 보다 강화할 수 있는 템페스트 공격에 강인한 색상 조합 활용 방법에 대해 추가로 제시한다.

먼저, 전자파를 통한 정보 유출의 위험에 대응할 수 있는 보안 글꼴의 설계 원칙을 개발하고 검증하였으며, 이후 색상, 그리고 글자들의 배치 방법 등 다양한 시각적 요소가 전자파를 통한 정보 유출에 미치는 영향이 실험적으로 검증되었다.

II. 대상 비디오 시스템의 스펙트럼 특성

2-1 전자기 고유 특성 분석을 활용한 보안 색상 분석

비디오 시스템에서 발생하는 누설 전자파는 회로상에 흐르는 전자 신호 상에서 급격한 전위차가 발생하였을 때 두드러지게 발생한다. 즉, 화면 정보를 구성하는 픽셀 정보를 담고 있는 비트열(bit-sequence)의 형태에 따라 각 픽셀의 전자기 고유 특성(electromagnetic signature)의 주파수 스펙트럼이 서로 상이하게 나타나게 된다. 컴퓨터 모니터가 출력하는 화면 정보는 일반적으로 수많은 색상의 화소(pixel)들로 구성되며, 각 화소는 RGB(red, green, blue) 채널별로 8비트 양자화 방식을 활용한다. 이때 채널별 8비트 화소 값을 $00_{(16)} \sim FF_{(16)}$ 범위 내의 2자리 수의 16진수로 표현할 수 있다. 그러나 이러한 정의 방식은 컴퓨터 내부 그래픽 처리 방식에서 활용되는 표현 방식일 뿐이며, 실제 비디오 신호 전송 인터페이스에 할당되는 비트 값은 일반적으로 변화 최소화 차분신호(TMDS: transition minimized differential signaling) 부호화(encoding) 방식을 거치게 된다. 해당 방식은 현재 대한민국에서 가장 높은 보급률을 가지는 고화질 멀티미디어 인터페이스(HDMI: high definition multimedia interface), 디지털 비주얼 인터페이스(DVI: digital visual interface)에 활용되는 디지털 프로토콜의 부호화 방식이며, 이는 8비트로 사전 정의된 화소별 RGB 색상 정보들이 그림 2에 나타난 바와 같이 10비트 형태로 변형되어 전송하게 된다.

TMDS 부호화를 활용하는 이유는 DC 오프셋(offset)을 최소화하여 컴퓨터 시스템 내에서 불필요한 전력 누수가 발생하는 것을 막고, 두드러지는 반복성을 제거하여 누설

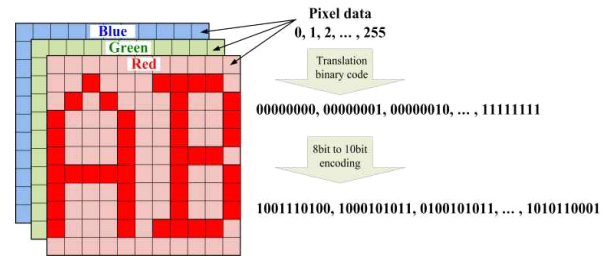


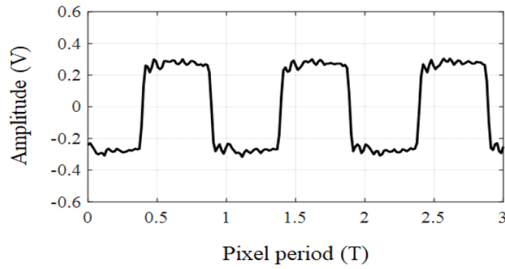
그림 2. TMDS 부호화 프로세스

Fig. 2. TMDS encoding process.

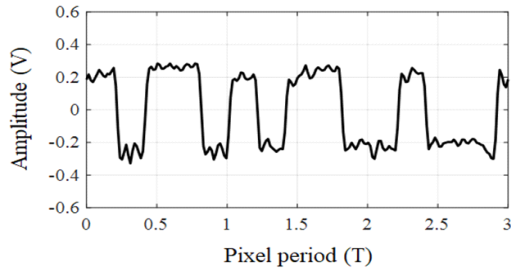
전자파가 특정 주파수 대역에 몰려 존재하는 것을 막는 것이다. 이러한 특성들은 수 미터에 이르는 짧지 않은 신호 전송 시스템상에서 신호의 무결성을 유지하기 위해 중요한 요소이며, 추가로 같은 화소 정보가 전달되더라도 다양한 스펙트럼 구조를 갖게 되는 원인이 된다.

그림 3은 HDMI 케이블상에 존재하는 RGB 전송 선로 중 Red 전송 선로에 흐르는 전자 신호를 오실로스코프와 능동형 차동 프로브(active differential probe)를 활용하여 세 주기만큼의 시간 길이에 대해 측정한 결과이다. 앞서 소개한 TMDS 부호화 방식으로 인해 기존 검정 색상을 의미하였던 비트 값 $00_{(16)}$ 은 $0000111110_{(2)}$ 1개의 비트 종류가 지속적으로 반복되어 나타나게 되며, 하얀 색상을 의미하였던 비트 값 $FF_{(16)}$ 의 경우 $1100111100_{(2)}$, $1100111100_{(2)}$, $0011000001_{(2)}$ 의 비트가 번갈아 가며 나타나게 된다. 마지막으로 본 논문에서 제안하고자 하는 대체 하얀 화소값 ($F1_{(16)}$)의 경우 검정 색상과 유사하게 $1111100000_{(2)}$ 의 1개의 비트 종류가 반복되어 나타나게 됨을 확인할 수 있다^[14].

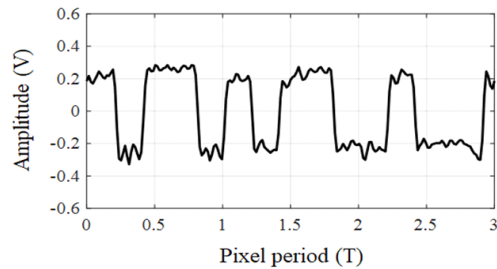
이어지는 그림 4에서는 앞서 소개한 3가지 색상 정보를 지닌 TMDS 부호화된 전자 신호들을 고속 푸리에 변환(FFT)을 수행한 결과를 나타낸다. 이로부터, 전자 신호에서 발생하는 누설 전자파의 주파수 특성이 매우 넓은 대역에 걸쳐 발생하는 것을 확인할 수 있으며, 이는 굳이 스펙트럼상에 나타난 누설 전자파를 전 대역에 걸쳐 수집할 필요 없이 신호 대 잡음비(SNR) 확보 차원에서 상당한 이점을 가져갈 수 있는 협대역 수집 장치를 활용하여도 검정 화소와 하얀 화소의 주파수별 특성이 두드러지게 차이나는 점을 활용하여 유의미한 화면 정보의 추출이 가능함을 의미한다^{[6],[9],[10],[15],[16]}.



(a) 검정 화소($00_{(16)}$)의 측정 결과
(a) Measurement results of black pixel ($00_{(16)}$)



(b) 흰색 화소($FF_{(16)}$)의 측정 결과
(b) Measurement results of white pixel ($FF_{(16)}$)



(c) 제안하는 대체 흰색($F1_{(16)}$) 화소의 측정결과
(c) Measurement results of the proposed alternative white pixel ($F1_{(16)}$)

그림 3. 색상별 신호 측정 결과

Fig. 3. Results of signal measurement by color.

이와 반대로 검정 화소($00_{(16)}$)와 제안된 대체 하얀 화소($F1_{(16)}$)의 경우 실제 디스플레이 화면 상에 나타나는 색상 대비는 매우 두드러지지만, 누설 전자파 스펙트럼의 분포가 유사하게 나타남을 알 수 있다. 즉, 이러한 사실로부터 기존에 문서에 사용되는 색상 대비를 크게 변화시키지 않음에도 불구하고, 디스플레이 시스템에서 발생하는 누설 전자파의 화소별 주파수 특성을 활용한 정보 추출에 어려움을 야기할 수 있을 것이라는 사실을 유추할 수 있다.

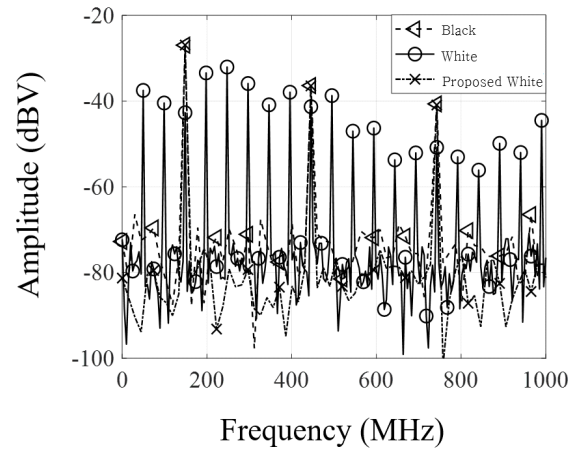


그림 4. 색상별 누설 전자파의 스펙트럼

Fig. 4. Spectrum of three kinds of pixels.

2.2 제안하는 보안 글꼴

비디오 시스템에서 발생하는 누설 전자파를 수집하여 복원하기 위해선 앞서 간략히 언급한 수집 신호의 충분한 SNR 확보뿐만 아니라 충분한 대역폭 확보 또한 중요하다. 우선 본 논문에서는 여러 선행 연구들에서 깊이 있게 다뤄진 화면 중첩(frame-averaging)을 기본적으로 활용하기 때문에 충분한 SNR 확보는 가능한 상황임을 가정한 다^{[6],[8],[9],[10]}. 물론, 대역폭 또한 전자파 수집을 위해 구성되는 RF 시스템의 설계환경상의 시스템의 잡음 상수(noise figure)와 SNR과 상관관계가 있으므로 이들을 완전히 독립적으로 고려할 수는 없다. 그러나, 본 절에서 다루고자 하는 대역폭 관련 내용은 화면 정보를 구성하는 기저대역 성분들 상에서 잠재적으로 발생할 수 있는 위신호 현상(aliasing)의 발현 정도이다. 이는 비디오 시스템의 전송 방식이 전송하고자 하는 화면 정보의 왼쪽 위 끝으로부터 오른쪽 아래 끝의 방향의 순차 전송(progressive) 방식을 채택함으로부터 기인한다.

더 나은 이해를 위해, 그림 5에 비디오 시스템의 이미지 재구성 방식을 나타냈다. 비디오 정보는 전송된 3개의 데이터 채널과 제어 데이터를 통해 이미지로 변환된다. 이를 통해, 대역폭과 관련된 사항은 수평 성분들에 크게 영향을 미칠 수 있다는 것을 예상할 수 있다. 그림 6에 나타난 바와 같이, 대상 글씨의 크기가 작아질수록 화소 값

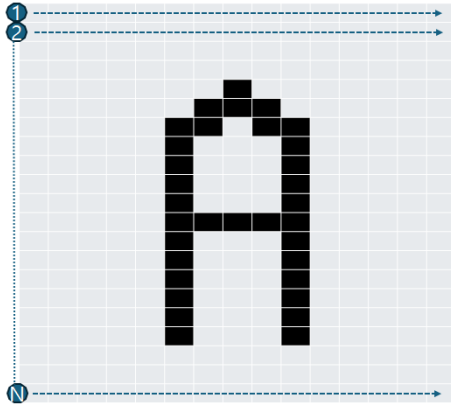


그림 5. 이미지 주사 순서
Fig. 5. Image scanning order.

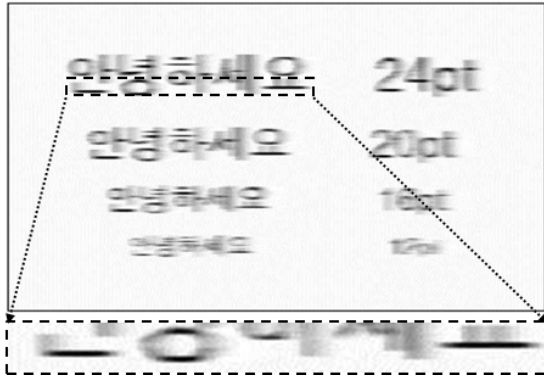


그림 6. 대역폭이 제한된 비디오 정보
Fig. 6. Bandwidth-limited video information.

의 변화는 더 역동적으로 변화하게 되며, 이는 결과적으로 수집하고자 하는 특정 주파수 대역 내에서 상대적으로 넓은 주파수 대역폭을 점유하는 기저 대역폭을 형성한다는 사실을 미루어 짐작할 수 있다. 실제로 그림 6은 RF 수집 장치의 아날로그-디지털 변환장치(ADC)의 대역폭을 20 MHz로 제한하여 HDMI에서 누설되는 정보를 복원한 결과이며, 확대된 그림을 통하여 제한된 대역폭에 의해 이미지 정보가 좌우로 흐려지는 현상(blur)이 발생함을 확인할 수 있다. 결과적으로 좌우로 글자 간격이 좁을수록 넓은 대역폭이 요구된다는 것을 유추할 수 있었기에, 이를 기반으로 그림 7과 같은 글꼴을 제작하였다. 제안된 글꼴의 형태는 자음과 모음의 간격이 매우 좁아 제한된 대역폭에 의해 누설 전자파를 이용하여 정보를 복원



그림 7. 제안된 글꼴 형태
Fig. 7. Proposed font shapes.

하는 과정에서 글자 형태의 구분에 어려움이 발생한다.

Ⅲ. 실험을 통한 검증

3-1 실험 환경 설정

본 연구의 실험적 검증은 전자파적합성(electromagnetic compatibility) 시험용 챔버(chamber) 내에서 수행되었다. 실험 구성은 그림 8에 도시된 바와 같이, 대상 모니터는 수집 장비로부터 5 m의 거리에 배치하였으며, 실험에 사용된 대상 모니터는 24인치 Full HD(FHD) 해상도를 지원하는 모델로 선택되었으며, 일반적인 사무 환경에서의 사용을 모사하기 위해 1,920×1,080의 화면 해상도와 60 Hz의 주사율로 설정하였다(표 1).

수집 장비로는 20 MHz에서 3,000 MHz의 광범위한 주파수 대역을 측정할 수 있는 log periodic dipole array antenna를 사용하였다. 이와 함께, 소프트웨어 정의 라디오(SDR), 대역통과필터(band pass filter), 그리고 저잡음 증폭기(low noise amplifier)가 활용된다. 사용된 대역통과필터는 중심 주파수를 기준으로 약 5 %의 부분대역폭(fractional bandwidth)을 제공한다.

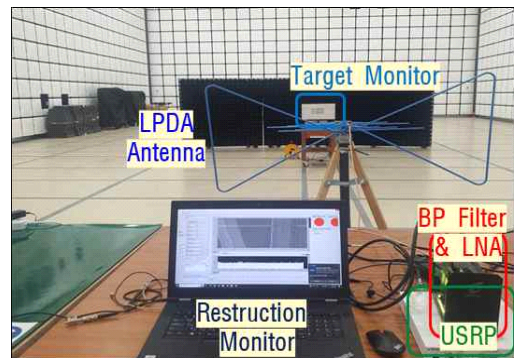


그림 8. 실험 환경
Fig. 8. Experimental environment.

표 1. 실험에 사용된 비디오 시스템의 사양

Table 1. Specifications of the video system used in the experiment.

Parameters	Value
Resolution	1,920×1,080 (FHD)
Vertical synchronization	60 Hz
Horizontal synchronization	67.5 kHz
Pixel frequency	148.5 MHz
Interface	HDMI

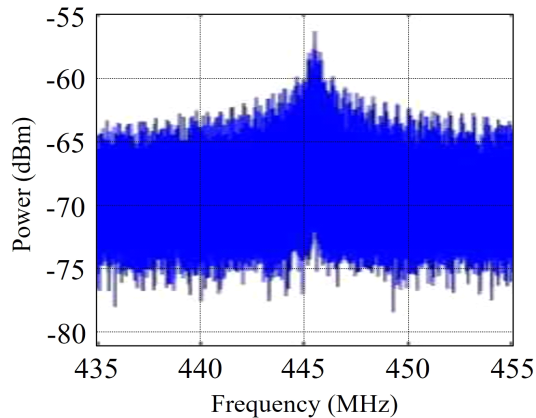


그림 9. 대상 모니터의 주파수 스펙트럼

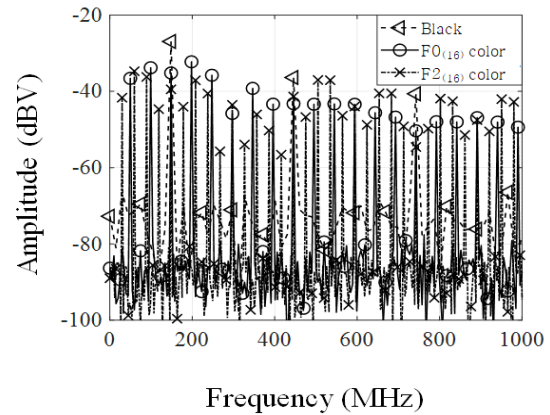
Fig. 9. Frequency spectrum of the target monitor.

본 실험의 목적은 일반적으로 사용되는 흰색 배경과 본 논문에서 제안한 흰색 배경의 조합이 모두 누설 전자파를 발생시키는지 확인하고, 누설된 정보로부터 복원된 정보의 형태 변화를 분석한다. 그림 9는 중심 주파수 445 MHz에서 약 20 MHz의 샘플링 주파수를 활용하여 수집된 신호의 스펙트럼 특성을 보여준다. 이러한 실험 설정 값은 본 논문에서 제안하는 기법의 실효성 검증을 목적으로 설정되었다.

3-2 배경 색상효과에 대한 실험적 검증

본 연구에서 제안하는 대체 흰색($F1_{(16)}$)의 효과를 검증하기 위해 앞서, $F1_{(16)}$ 과 색상 값이 유사한 흰색 계열의 $F0_{(16)}$ 및 $F2_{(16)}$ 를 실험의 배경색 또한 선정하여 추가적 분석하였다.

그림 10에 나타난 바와 같이, $F0_{(16)}$ 와 $F2_{(16)}$ 는 제안하는

그림 10. $F0_{(16)}$ 와 $F2_{(16)}$ 그리고 검정 색상($00_{(16)}$)의 스펙트럼
Fig. 10. Spectrum of $F0_{(16)}$ 와 $F2_{(16)}$ and black($00_{(16)}$).

대체 흰색 $F1_{(16)}$ 과 매우 유사한 색상 값임에도 불구하고, 검정 색상 화소의 주파수 스펙트럼과 매우 다른 주파수 특성을 지닌다. 이는 앞서 언급한 것과 같이 화소 별로 서로 다른 주파수 특성의 차이를 활용한 화소 값 구분이 쉽게 가능함을 의미하며, 결과적으로 잠재적인 정보 유출을 초래할 수 있음을 시사한다.

실험에 사용된 글꼴 크기는 48 pt로 설정하였으며, 모든 글자의 색상은 통일성을 위해 검정 색상($00_{(16)}$)으로 고정하였다. 그림 11(a)는 실험에 사용된 대상 이미지를 나타내며, 그림 11(b)~그림 11(d)는 누설 전자파를 활용하여 복원한 정보의 결과를 보여준다. 해당 실험에서는 큰 글자 크기로 인해 누설 전자파를 수집하여 복원함으로써, 좁은 대역폭으로 인한 블러 현상의 영향을 최소화하였다. 이는 두 색상 간의 전자파 특성의 유사성을 명확히 비교 분석할 수 있는 중요한 실험적 접근이다.

그림 11(b)~그림 11(d)를 통해, 색상 정보의 미묘한 차이에도 불구하고, 서로 다른 누설 전자파 특성으로 인해 분명하게 문자와 배경이 구분되는 것을 관찰할 수 있다. 따라서, 본 실험은 제안된 색상이 누설 전자파를 통한 정보복원에 미치는 영향을 실증적으로 검증하는 데 중요한 역할을 하며, 색상 선택이 전자파 누설의 특성을 변화시킬 수 있음을 입증한다.

3-3 글꼴 효과에 대한 실험 검증

본 연구에서 제안한 글꼴 형태의 효율성을 실험적으로

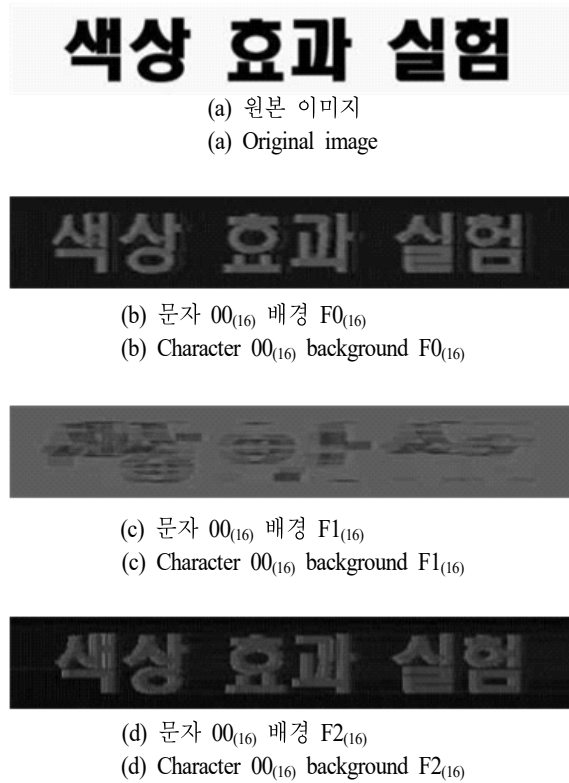


그림 11. 색상 조합에 따른 실험 결과

Fig. 11. Experimental results according to color combinations.

검증하기 위하여, 그림 12(a)에 제시된 바와 같이 다양한 글꼴 크기(48, 24, 12 pt)를 적용한 이미지를 구성하고, 이를 통해 누설 전자파의 수집 및 복원 과정을 진행한다. 실험의 초점은 제안된 글꼴이 누설 전자파를 통한 정보복원 시 가독성이 어떻게 변화되는지 분석하는 데 있다.

그림 12(b)는 48 pt 크기의 글자를 복원한 결과를 보여주며, 이 크기에서는 모든 글꼴 형태에서 글자 인식에 어려움이 없음을 확인할 수 있다. 이는 글자의 크기가 클수록 요구되는 대역폭이 감소하기 때문에 발생하며, 매우 큰 글꼴의 형태에 의해 제안된 글꼴에도 충분한 간격이 발생하여 좁은 대역폭에서도 정보복원이 원활하게 이루어진다. 즉, 글씨의 크기가 TEMPEST 대책에 매우 중요한 요소이다. 반면, 그림 12(c) 및 그림 12(d)는 각각 24 pt와 12 pt 크기의 글자를 복원한 결과를 제시하고 있다. 작은 글자 크기에서는 자음과 모음의 간격이 현저히 줄어들어,

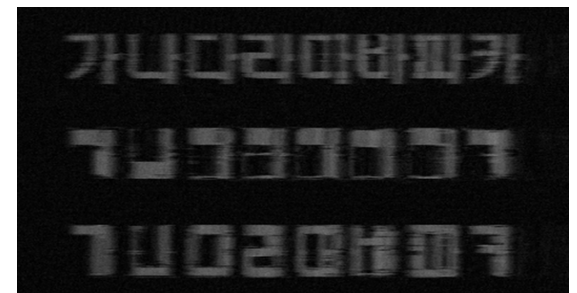
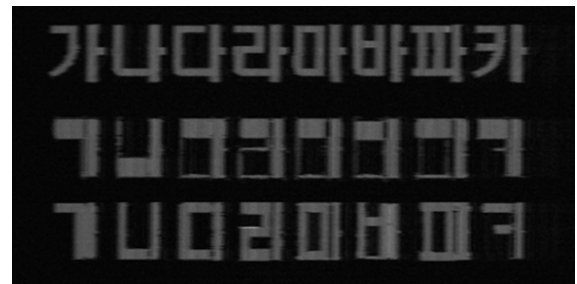


그림 12. 글꼴 형태와 크기에 따른 실험 결과

Fig. 12. Experimental results according to font shapes and sizes.

좁은 대역폭의 영향으로 인해 가독성이 크게 저하되는 현상을 관찰할 수 있다. 특히 12pt 크기에서는 글자 간의 구분이 매우 어려워져, 정보의 정확한 복원이 힘들었다는 점에서, 제안된 글꼴의 효과적인 사용에 있어 글자 크기와 글꼴의 형태가 중요한 변수임을 보인다. 하지만 제안된 글꼴의 경우에도 글자의 크기가 확보된 시점에서 정보의 누설을 피할 수 없다. 이러한 문제를 해결하기 위해, 제안한 색상과 글꼴을 적용하여 TEMPEST 내성 효과가 24pt 크기에서도 나타나는지 검증하였다.

3.4 글꼴 및 색상효과의 적용과 실험 결과 분석

본 연구에서 제안된 글꼴 형태와 색상($F1_{(16)}$)의 효과를 동시에 적용하여 정보 유출 방지 효과를 실험적으로 검증하였다. 초기 실험 결과, 글자 크기가 큰 경우 충분한 대역폭을 통해 정보 유출이 확인되었다. 이에 따라, 제안된 배경색($F1_{(16)}$)과 글꼴 형태를 결합하여 추가 실험을 수행하였다. 그림 12(a)에서 보인 바와 같이, 선택된 글꼴에 대해 제안된 배경색을 적용하고, 모든 글자 크기를 24pt로 통일하여 실험을 진행한다.

그림 13은 상기된 두 조건에서 얻은 복원 결과를 나타



(a) 문자(24 pts) $00_{(16)}$ 배경 $F1_{(16)}$

(a) Character (24 pts) $00_{(16)}$ background $F1_{(16)}$



(b) 문자(24 pts) $00_{(16)}$ 배경 $F1_{(16)}$

(b) Character (24 pts) $00_{(16)}$ background $F1_{(16)}$

그림 13. 제안된 글꼴 형태와 색상효과를 동시에 적용한 실험 결과

Fig. 13. Experimental results with proposed font and color composition.

내며, 실험을 통해 얻은 두 글꼴 모두에서 배경과 글자 사이의 대비가 유사해지며, 글자의 테두리가 뚜렷하게 나타나는 현상이 관찰된다. 이러한 글자 테두리 형성은 비디오 시스템이 이미지를 처리하는 과정에서 배경색과 글자 색상의 변화를 부드럽게 표현하려 시도하면서, 지정된 색상이 아닌 다른 색상이 할당되어 나타난 결과로 인한 것으로 분석된다. 제안하는 배경 색상 할당 방식이 적용된 일반 글꼴의 경우, 어느 정도 글자 형태가 인식되어 정보의 유출 가능성이 있음을 확인할 수 있었던 반면 제안된 글꼴과 배경 색상을 모두 적용하면 글자 인식이 매우 어려워져, 정보 유출 방지에 효과적임을 실험을 통해 입증하였다.

이러한 실험 결과는 제안된 글꼴 및 색상효과가 정보 보호에 있어서 상호 보완적으로 작용할 수 있음을 시사한다. 특히, 제안된 글꼴과 색상을 결합함으로써, 누설 전자파를 통한 정보복원 과정에서의 가독성을 현저히 저하해, 더 효과적인 정보 유출 방지가 가능함을 확인할 수 있다. 이는 누설 전자파를 이용한 정보 유출 위험을 최소화하는 데 이바지를 할 수 있기를 기대한다.

IV. 결 론

본 연구는 전자파를 통한 정보 유출이라는 현대적 보안 위협에 대응하기 위한 새로운 접근 방식을 탐색하였다. 특히, 글꼴의 크기, 굵기, 간격, 색상 등을 조정하여 보안성을 강화한 새로운 한글 글꼴 설계에 초점을 맞췄다. 이러한 방식은 전통적인 물리적 보안 대책이 예산적 제약 등으로 인해 실현하기 어려운 상황에서, 효율적이고 비용 효과적인 대안을 제시한다.

본 연구를 통해 개발된 글꼴은 전자파 도청과 같은 정보 유출 시도에 대한 저항력을 향상하는 데 이바지할 수 있다. 특히, 색상효과를 활용한 연구는 단순히 문서 처리 소프트웨어의 설정을 조정함으로써 적용할 수 있는, 매우 실용적인 보안 대책을 제시한다.

향후 연구에서는 구조적 유사성 지수(SSIM, structural similarity index)과 같은 기법을 적용하여, 정보가 복원된 문자의 인식률을 정량적인 결과로 도출한다. 일반적으로 비교를 위한 기준 이미지가 필요한 SSIM은 우리의 실험

에서 정보 복원의 품질을 정확한 반영이 어렵다. 현재의 한계를 극복하기 위해 대상 비디오 시스템을 기반으로 유출된 전자기파 신호의 모의 버전의 분석이 필요하다. 이러한 시뮬레이션을 통해 우리는 적절한 참조 기준선을 설정하여 SSIM을 우리의 복원 과정의 효과를 평가하는데 유용한 도구로 활용한다.

References

- [1] H. S. Lee, D. H. Choi, K. Sim, and J. G. Yook, "Information recovery using electromagnetic emanations from display devices under realistic environment," *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1098-1106, Aug. 2019.
- [2] T. L. Song, Y. R. Jeong, and J. G. Yook, "Modeling of leaked digital video signal and information recovery rate as a function of SNR," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 2, pp. 164-172, Dec. 2015.
- [3] M. G. Kuhn, "Compromising emanations of LCD TV sets," *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 564-570, Jun. 2013.
- [4] H. Tanaka, "Information leakage via electromagnetic emanation and effectiveness of averaging technique," in *Proceedings of 2008 International Conference on Information Security and Assurance(ISA 2008)*, Busan, Apr. 2008, pp. 98-101.
- [5] R. Birukawa, T. Mizuki, H. Sone, and Y. Hayashi, "A practical evaluation method for EM information leakage by using audible signal," in *Proceedings of the 2019 Joint International Symposium on Electromagnetic Compatibility, Sapporo and Asia-Pacific International Symposium on Electromagnetic Compatibility(EMC Sapporo/APEMC)*, Sapporo, Jun. 2019, pp. 250-253.
- [6] E. Lee, D. H. Choi, T. Nam, and J. G. Yook, "A quantitative analysis of compromising emanation from TMDS interface and possibility of sensitive information leakage," *IEEE Access*, vol. 10, pp. 73997-74011, Jun. 2022.
- [7] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, no. 4, pp. 269-286, Dec. 1985.
- [8] H. S. Lee, D. H. Choi, K. Sim, and J. G. Yook, "Information recovery using electromagnetic emanations from display devices under realistic environment," *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1098-1106, Aug. 2019.
- [9] D. H. Choi, E. Lee, and J. G. Yook, "Reconstruction of video information through leaked electromagnetic waves from two VDUs using a narrow band-pass filter," *IEEE Access*, vol. 10, pp. 40307-40315, Mar. 2022.
- [10] P. De Meulemeester, B. Scheers, and G. A. E. Vandenbosch, "A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels," *IEEE Transactions on Electromagnetic Compatibility*, vol. 62, no. 3, pp. 663-672, Jun. 2020.
- [11] E. Lee, D. H. Choi, T. Nam, and J. G. Yook, "Counter-TEMPEST: Information spoofing based on the EM-leakage signature of TMDS system," in *2023 International Symposium on Electromagnetic Compatibility - EMC Europe, Krakow, Sep. 2023*, pp. 1-5.
- [12] T. L. Song, Y. R. Jeong, H. S. Jo, and J. G. Yook, "Noise-jamming effect as a countermeasure against TEMPEST during high-speed signaling," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1491-1500, Nov. 2015.
- [13] M. G. Kuhn, R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," in *International Workshop on Information Hiding*, Berlin, Springer-Verlag, 1998, vol. 1525, pp. 124-142.
- [14] *High-Definition Multimedia Interface Specification*, HDMI Licensing Version 1.3A, Nov. 2006.
- [15] E. Lee, D. Choi, T. Nam, W. Choi, and J. Yook, "An analysis of electromagnetic signatures from triangularly modulated spread spectrum clocking signals," *IEEE Transactions on Electromagnetic Compatibility*, pp. 1-

12, Apr. 2024.

- [16] T. Nam, D. H. Choi, E. Lee, H. S. Jo, and J. G. Yook,
"Data generation and augmentation method for deep

learning-based VDU leakage signal restoration algorithm," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 5220-5234, Apr. 2024.

최 동 훈 [연세대학교/석·박사통합과정]

<https://orcid.org/0000-0002-7626-8922>



2016년 8월: 전남대학교 전자통신공학과 (공학사)

2016년 9월~현재: 연세대학교 전기전자공학과 석·박사통합과정

[주 관심분야] EMI/EMC, Antenna, TEMPEST Side Channel Attack 등

이 의 범 [연세대학교/박사과정]

<https://orcid.org/0000-0003-3943-4319>



2018년 2월: 건국대학교 전자공학과 (공학사)

2020년 2월: 건국대학교 전자공학과 (공학석사)

2020년 2월~현재: 연세대학교 전기전자공학과 박사과정

[주 관심분야] RF Circuit Design, EMC/EMI, TEMPEST 등

최 원 준 [국군방첩사령부/소령]

<https://orcid.org/0009-0009-2349-2902>



2024년 2월: 연세대학교 전기전자공학과 (공학석사)

2024년 3월~현재: 국군방첩사령부 소령

[주 관심분야] EMSEC, Anti-TEMPEST, Side Channel Attack 등

육 중 관 [연세대학교/교수]

<https://orcid.org/0000-0001-6711-289X>



1987년 2월: 연세대학교 전자공학과 (공학사)

1989년 2월: 연세대학교 전자공학과 (공학석사)

1996년 12월: University of Michigan 전기전자공학과 (공학박사)

1997년 1월~1998년 9월 : University of Michigan Research Fellow

1998년 10월~1999년 2월: Qualcomm Inc. Senior Engineer

1999년 3월~2000년 2월: 광주과학기술원 조교수

2000년 3월~현재: 연세대학교 전자공학과 교수

2012년~2013년: IEEE Distinguished Lecturer (EMC Society)

[주 관심분야] 마이크로파 시스템 해석 및 설계, 안테나 시스템, RF MEMS, Bio-Radar and Sensors, Computational Electromagnetics, EMI/EMC, HEMP, TEMPEST