**ỨNG DỤNG WATERMARKING AUDIO VÀO PHÂN PHỐI NHẠC SỐ**

Đặng Xuân Duy Khương Trương Thanh Nam TS. Dương Minh Đức Trường Đại Học Công Nghệ Thông Tin Trường Đại Học Công Nghệ Thông Tin Trường Đại Học Công Nghệ Thông Tin Khoa Công nghệ phần mềm Khoa Công nghệ phần mềm Khoa Công nghệ phần mềm  
 [khuongdangxuanduy@gmail.com](mailto:khuongdangxuanduy@gmail.com) [nam31780@gmail.com](mailto:nam31780@gmail.com) [ducdm@uit.com.vn](mailto:ducdm@uit.com.vn)

**Abstract – Watermarking là một trong những lĩnh vực nghiên cứu rất nổi bật. Tuy nhiên việc ứng dụng Watermarking vào một hệ thống thực sự vẫn chưa có nhiều nghiên cứu và thực nghiệm. Nghiên cứu này sẽ sử dụng Echo Hiding, một nhóm thuật toán của Watermarking Audio, để chứng minh tính khả thi của Echo Hiding nói riêng và Watermarking Audio nói chung vào một hệ thống phân phối âm nhạc thực tế. Sử dụng Hamming Code để tăng độ chính xác khi nhúng và trích xuất. Kết quả thu được cho thấy sự khả thi khi sử dụng thuật toán Echo Hiding. So sánh với nghiên cứu của Tekeli và Asliyan[3] cho thấy sự cải thiện rõ rệt trong BER. Nghiên cứu cũng đặt ra được đề xuất sử dụng fingerprint để phát triển hệ thống trong tương lai.**

**Keywords:** watermarking, echo hiding, audio steganography

**I GIỚI THIỆU**

Cùng với sự bùng nổ về công nghệ, đặc biệt là sự phát triển mạnh mẽ của Internet trong mọi mặt của cuộc sống, nhu cầu về giải trí của mọi người trở thành một nhu cầu thiết yếu. Âm nhạc, phim ảnh trở thành ngành công nghiệp tỷ đô. Song song với đó là các dịch vụ streaming hình ảnh, âm nhạc phát triển cực nhanh trên mọi lĩnh vực.

Tuy nhiên song song với dịch vụ streaming phát triển, việc bảo vệ tác quyền âm nhạc của nhà phát hành/tác giả/ca sĩ càng trở nên khó khăn hơn. Hiện tượng download nhạc, phim ảnh để xem, nghe offline trở nên vô cùng dễ dàng và là điều không thể tránh khỏi. Tuy nhiên vẫn có hiện tượng người dùng reupload nhạc, phim ảnh trở lại các platform streaming để kiếm tiền không chính đáng từ các dịch vụ đó. Theo ước tính của International Intellectual Property Alliance (IIPA), ngành công nghiệp điện ảnh của mỹ mất 1,3 tỷ đô la, âm nhạc và thu âm 1,7 tỷ đô la.[2]

**NHỮNG NGHIÊN CỨU LIÊN QUAN**

**Những vấn đề hiện tại của phân phối nhạc số**

Trong 1 thời gian ngắn, các công ty E-commerce đã trở thành những doanh nghiệp khổng lồ. Các dịch vụ phân phối phương tiện truyền thông đóng một vai trò quan trọng trong mô hình doanh nghiệp – khác hàng (Business-to-consumer – B2C). Nhạc số (Ví dụ như MP3 nén) đã trở nên vô cùng phổ biến. Ngoài ra với sự phát triển của các kết nối di động (như GPRS, 3G,…) giúp cho người sử dụng di động có thể kết nối mọi lúc mọi nơi.

Tuy nhiên ngoài những mặt tích cực của việc phân phối các phương tiện truyền thông kỹ thuật số cũng có nhiều bất cập. Một trong những vấn đề quan ngại lớn nhất chính là khả năng dễ sao chép, với chất lượng hoàn hảo.[2]

Vì thế, ta có thể thấy rõ rằng một hệ thống phân phối phương tiện truyền thông cần được bảo vệ. Điều này có thể đạt được nhờ một hệ thống DRM, được thiết kế để điều khiển và giới hạn quyền hạn truy cập dữ liệu đa phương tiện. Hệ thống này thường bao gồm mã hóa, giới hạn quyền truy cập và quản lý khóa. Nhiều hệ thống DRM cũng bao gồm thêm cơ chế điều khiển sao chép hệ thống thanh toán. Tuy nhiên việc điều khiển hay ngăn chặn việc sao chép là cực kỳ khó đạt được, nhất là một hệ sinh thái mở. Việc nhận dạng và truy ngược những bản copy của dữ liệu truyền thông đã được đề xuất làm bức tường cuối cùng. Tuy nó không thể ngăn chặn việc sao chép nhưng có thể định dạng được nguồn bị rò rĩ. Một kỹ thuật trong hệ thống DRM dùng để nhận dạng dữ liệu là watermarking. [2]

**Tính khả thi của watermarking vào phân phối nhạc số**

Watermarking không phải là một kỹ thuật độc lập. Nó chỉ có ích khi là một thành phần của hệ thống với ứng dụng chính là DRM và bảo vệ bản quyền. Tuy nhiên nó phải luôn được xem là mắt xích yếu nhất trong một hệ thống DRM. Một vấn đề khác của một hệ thống DRM là định danh người nhận thường là không biết hoặc không đáng tin cậy. Việc định danh từng cá nhân qua mỗi bản sao chép phân phối đa phương tiện chỉ có hiệu quả khi người nhận được định danh rõ rang.

Việc giấu dữ liệu không phát hiện được vào âm thanh là một công việc khó khăn vì hệ thống cảm nhận âm thanh của người rất chính xác.[11] Tuy nhiên nó có nhiều đặc tính có thể khai thác được.

**Các thuật toán khả dụng để watermarking**

Một số lượng lớn bên trong nghiên cứu vào giấu dữ liệu đã và đang sử dụng hình ảnh làm trung gian. Về phần âm thanh, độ chính xác của cơ quan cảm nhận âm thanh của con người làm cho việc nhúng dữ liệu 1 cách bí mật vào trở nên khó khăn hơn, tuy nhiên nó vẫn có nhiều ưu điểm: độ lớn của tệp thường lớn hơn, cho phép khả năng nhúng cao hơn. Nó là một tệp tin vô hại để trao đổi, tệp MP3s có thể được gửi mail, mang đi rất dễ dàng.

Đã có nhiều phương pháp khác nhau dùng để nhúng dữ liệu vào audio file. Chúng ta sẽ bàn luận ở chương sau.

**Những vấn đề hiện tại đối với hệ thống DRM**

Trong các hệ thống phân phối nhạc số hiện tại thường có một hệ thống DRM. Tuy nhiên hệ thống này lại không được tự động/bán tự động, ngoài ra lại có nhiều lỗ hổng trong hệ thống. Vì trong một hệ thống DRM, độ mạnh mẽ của nó chính là mắt xích yếu nhất.[5]

Thứ nhất, yêu cầu cơ bản của một hệ thống DRM là đảm bảo rằng thông tin được đưa đến một đối tượng định sẵn. Vì sự giới hạn này phải luôn luôn được đi theo thông tin được gửi, vì thế DRM luôn phải có một sự “bảo vệ liên tục”.Thứ hai, người nhận thông tin cũng được xem là một kẻ tấn công tiềm năng. Không giống như giả định của một hệ thống mã hóa.

Thứ ba, việc mã hóa dữ liệu là không hiệu quả cho DRM. Vì để người dùng có thể sử dụng được dữ liệu thì người dùng phải có mã giải. Và việc này không phải là thiết kế của việc mã hóa.

Cuối cùng, phải luôn luôn ghi chú rằng luôn có một giới hạn mà một hệ thống DRM có thể sử dụng. Vì dữ liệu số cuối cùng cùng phải được trình bày và tại thời điểm đó có thể là mục tiêu tấn công. Ví dụ như một hệ thống DRM hoàn hảo đã được thiết lập, khi người dùng phát nhạc ra loa sau đó ghi âm lại, đó là một “lỗ hổng điện tín” (Analog Hole) (Doctorow 2002), điều mà tồn tại trong tất cả các hệ thống DRM. Tuy nhiên kiểu tấn công này tạo ra sự mất mán lớn về dữ liệu thu được. Vì thế nó không phải là một mốt quan tâm lớn của một hệ thống DRM. Mục đích của DRM là ngăn kẻ tấn công có được một bản gốc chất lượng cao và không được bảo vệ.

**Hướng giải quyết**

Sau khi phân tích các yêu cầu và vấn đề hiện tại. Hệ thống phân phối âm nhạc phải thỏa mãn các yêu cầu sau:

* Dữ liệu được bảo vệ, phát hiện ngay khi được upload lên hệ thống
* Dữ liệu âm thanh không thể bị nhận biết
* Dữ liệu phải mạnh mẽ trước các kiểu tấn công vô ý hoặc cố ý

Với những yêu cầu trên, kỹ thuật watermarking rất phù hợp với việc tạo ra một hệ thống phân phối âm nhạc số vì watermarking mang lại các lợi ích sau:

* Dữ liệu ẩn không thể hoặc rất khó bị nhận biết bằng tai thường.
* Dữ liệu ẩn đi kèm với tín hiệu âm thanh, vì thế được bảo vệ trong quá trình sao chép.

Tùy theo thuật toán được áp dụng mà độ mạnh mẽ sẽ khác nhau. Tuy nhiên các dạng tấn công phổ biến nhất là nén và resampling. Khóa luận này sẽ tập trung giải quyết vấn đề đó bằng thuật toán EH.

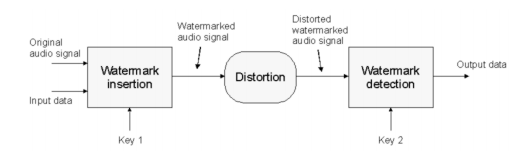
**II CƠ SỞ LÝ THUYẾT**

**ECHO HIDING**

Bảo vệ tác quyền âm nhạc không phải là một vấn đề mới. Ngành công nghiệp ghi âm đã chống lại việc vi phạm bản quyền từ khi ra đời. Tuy nhiên, sự phát triển của công nghệ kỹ thuật số càng làm cho cuộc chiến trở nên khó khăn hơn vì dữ liệu kỹ thuật số có thể được sao chép và phân phối dễ dàng. Watermarking đã được đề nghị để giải quyết vấn đề này. Bằng cách giấu watermark không thể nghe được vào bản nhạc.

Watermark khi được nhúng vào tín hiệu âm thanh, phải không làm ảnh hưởng đến chất lượng âm thanh, tuy nhiên nó phải có thể phát hiện được và không bị làm nhòa được.

Watermarking ban đầu được dùng trong các tài liệu in ấn để chống làm giả. Kiểu watermark thường bao gồm những hình vẽ ẩn chỉ có thể thấy được khi nhìn qua ánh sáng. Ví dụ như các tờ tiền hiện nay là minh chứng cho watermarking.

Những nghiên cứu đầu tiên về watermarking bắt đầu từ giữa những năm 90. Kỹ thuật đầu tiên được lấy cảm hứng từ những nghiên cứu về watermarking trong hình ảnh (Boney et al., 1996). Ý tưởng ban đầu bao gồm việc thêm một tín hiệu watermark vào tín hiệu gốc. Kết quả đạt được là tín hiệu mới phải được nghe giống như tín hiệu ban đầu. Thông tin có thể thu được có thể được dùng cho nhiều mục đích khác nhau.[4]  


Hình 1: Watermarking sử dụng như một kênh giao tiếp

Yêu cầu của một hệ thống watermarking âm thanh phải thỏa mãn là:

* **Inaudibility**: Watermarking phải không làm ảnh hưởng đến chất lượng âm thanh
* **Robustness**: Watermarking phải chống lại bất kỳ dạng tấn công vào tín hiệu âm thanh, trừ khi chất lượng âm thanh bị thay đổi đến mức không chấp nhận được
* **Capacity**: Bit rate của watermark phải đủ cao cho ứng dụng, tuy nhiên sẽ ảnh hưởng đến khả năng không thể nghe được và độ mạnh mẽ.
* **Reliability**: Dữ liệu chứa trong watermark phải được thu với tỉ lệ lỗi trong mức chấp nhận được
* **Low** **complexity**: Khi sử dụng cho các ứng dụng thời gian thực, thuật toán watermarking không được sử dụng quá nhiều thời gian.

**Cách hoạt động:**

Watermarking có thể được xem là một hệ thống giao tiếp. Watermark chính là tín hiệu để mang theo những thông tin cần thiết và tín hiệu âm thanh đóng vai là nhiễu kênh giao tiếp. Trong một kênh giao tiếp thông thường, tín hiệu gốc thường mạnh hơn tín hiệu nhiễu. Tuy nhiên điều này lại không phải trong watermarking.

Có rất nhiều cách watermark âm thanh đã được đề xuất, chúng ta có thể kể đến như:

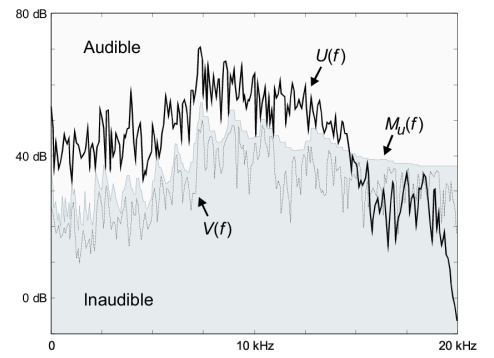
* **Spread-Spectrum watermarking**: Một hệ thống giao tiếp bằng spread-spectrum được đề xuất bởi (Dixon 1976) và (Haykin 1988) [4] bao gồm việc tách watermark ra các dãy tần số nhầm tăng tối đa cường độ mà vẫn giữ cho âm thanh không nghe được và chống lại tấn công (Boney et al.,1996) (Garcia, 1999).[4]
* **Echo-Hiding watermarking**: Giấu watermark vào tiếng vọng (Echo) nhằm khai thác lỗ hổng âm thanh trong tai người (Temporal masking properties) (Bender et al., 1996) (Neubauer, 2000)[4]
* **Bit stream watermarking**: Watermark sẽ được thêm trực tiếp vào dòng bit được tạo ra bởi coder tín hiệu âm thanh. Ví dụ như LSB hay MSB,…

**Khoa học âm thanh tâm lý (Psychoacoustic):**

Psychoacoustic là một môn khoa học nghiên cứu về sự nhận thức âm thanh. Qua nhiều thí nghiệm, những nhà khoa học đã thiết lập được nhiều giới hạn mà tai người đang có. Nếu như có 2 âm thanh gần tầng số với nhau và được chơi đồng thời, che khuất tần số có thể xảy ra khi một âm thanh to hơn âm thanh còn lại.

Các nhà khoa học đã tạo ra một khuôn mẫu về che khuất tần số cho các tín hiệu không theo âm điệu. Từ một tín hiệu âm thanh *u(t)*, các khuôn mẫu này tính được một đường cong Mu(f) được gọi là ngưỡng che khuất đông nhất với cường độ mật độ phổ âm (power spectral density – PSD) (Perreau, 1998)

Nếu như PSD V(f) của một tín hiệu v(t) thấp hơn Mu(f) cho mọi tần số. thì v(t) sẽ bị che khuất bởi u(t). Có nghĩa là người nghe sẽ không thể phân biệt được sự khác nhau giữa u(t) và u(t) + v(t) (Hình 2.1.1). Những mô hình này được dùng rộng rãi trong các phương thức nén mất âm như (MP3, MPEG-AAC (International Organization for Standardization, 1997) (Bosi et al., 1997)) để xóa những tín hiệu nhiễu không nghe được, cung cấp âm thanh chất lượng cao với tốt độ bits thấp.[4]



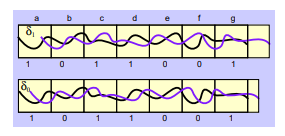
Hình 2: PSD của âm thanh che khuất và âm thanh bị che khuất ( U(f), đường nối liền và V(f), đường chấm mờ), cũng như ngưỡng che khuất Mu(f).

Trong việc watermarking âm thanh, các khuôn mẫu này được dùng để đảm bảo sự không thể nhận biết trong quá trình watermark. Dựa theo khuôn mẫu này, tín hiệu âm thanh có thể đạt tới 20dB.

Ngoài ra việc che khuất cũng có thể xảy ra trong vùng thời gian, nếu như 2 âm thanh gần nhau trong trường thời gian và to hơn rất nhiều thì nó sẽ che khuất âm thanh còn lại. Hiện tượng này được sử dụng trong những phương thức nén mất âm để tăng tỉ lệ nén (International Organization for Standardization, 1997). Che khuất hậu tố cũng được dùng trong phương thức EH. Watermark là một phiên bản làm trễ và nhỏ hơn của tín hiệu gốc. độ trễ giữa tín hiệu gốc và tiếng vọng chính là phương thức để mã hóa dữ liệu.

**Echo Hiding**

Phương thức EH được đề xuất ban đầu bởi Gruhl et al[9] bằng cách nhúng dữ liệu bit vào trường thời gian của tín hiệu âm thanh gốc bằng cách thêm vào một tiếng vọng.



Hình 3: Chanel echo 0 và 1 màu tím và tín hiệu gốc màu đen

**Độ manh mẽ**

Trong quá trình thử nghiệm, phương thức EH không làm giảm chất lượng âm, hoặc nếu có cũng rất nhỏ nếu như chúng ta thay đổi âm thanh gốc với cường độ nhỏ. Thậm chí trong quá trình thử nghiệm có một số âm thanh trở nên “giàu” hơn. Giúp người nghe có trải nghiệm tốt hơn.[10]

Phương thức EH rất mạnh mẽ đối với các phương thức nén MPEG, các phương thức này không làm thay đổi lớn đối với tỉ lệ thu được ở mức 85%. Ngoài ra các phương thức nén MP3 với bitrate 56kb/s hoặc 128kb/s cho thấy mức độ lỗi bit nhỏ.[7]

Tuy nhiên EH giống như SS, vẫn khá yếu khi có sự thay đổi tần số.

Trong các phương pháp ẩn thông tin trong âm thanh, phương pháp ẩn âm thanh trong tiếng vọng (Echo Hiding) trở nên phù hợp nhất trong việc bảo vệ tác quyền âm nhạc số.

**ĐIỂM LỢI**

* Khó nhận ra, hoặc sự xuất hiện của tiếng vọng làm âm thanh trở nên hay hơn
* Khó bị thay đổi, khả năng chống tấn công tốt

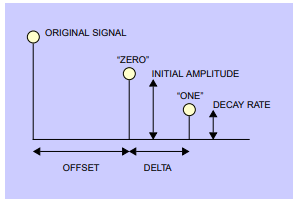
**ĐIỂM BẤT LỢI**

* Tỉ lệ nhúng thấp

Tuy nhiên, khi xét về nhu cầu trong hệ thống. Chúng ta chỉ cần lưu một lượng dữ liệu nhỏ để xác nhận tác quyền của tác giả/nhà phân phối, chứ không cần một file lớn. Vì thế phương pháp EH được chọn để tích hợp vào hệ thống phân phối nhạc số

**Cơ sở lý thuyết**

Thuật toán Echo Data Hiding rất được chú trọng trong công cuộc nghiên cứu watermarking. Tiếng vọng sẽ được thêm vào tín hiệu âm thanh để chèn dữ liệu vào bản nhạc. Dữ liệu được ẩn đi bằng việc thay đổi ba giá trị chính:[1]



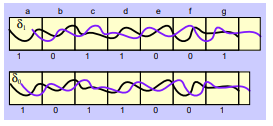
Hình 4: Các thông số trong thuật toán EH

Cho o0, o1, α lần lượt là offset cho bit 0, bit 1 và amptitute. Sau đó kernels tiếng vọng có thể được tính bằng phương trình 1 với δ [n] là hàm Kronecker delta như phương trình 2 để thể hiện cho xung của tín hiệu rời rạc.[3]

(1)

(2)

Tín hiệu tiếng vọng sau đó sẽ được tạo ra bằng cách tích chập tín hiệu âm thanh gốc và kernels tiếng vọng.



Hình 5: Tín hiệu âm thanh channel 0 và channel 1 và tín hiệu gốc đường đen

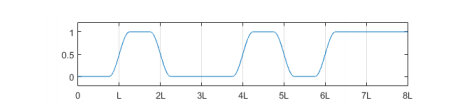
**Nhúng dữ liệu**

Bản âm gốc sẽ được chia thành nhiều phân khúc bằng với số bits sẽ được gắn vào. Sau đó mỗi phân khúc sẽ được thêm tiếng vọng với offset ứng với dữ liệu bit được gắn vào. Gọi N là số lượng bit cần gắn. L là độ dài của phân khúc. L được chọn sao cho N.L nhỏ hơn độ dài của tín hiệu âm thanh.

Tạo một tín hiệu trộn sẽ giúp tăng tính thuận lợi trong quá trình mã hóa, giúp giảm sự nhiễu âm trong quá trình gắn các phân khúc.

Các bước mã hóa dữ liệu vào đoạn âm thanh như sau:

* Tạo một chuỗi trong đó chứa chữ số không ở đầu.
* Tích chập bản nhạc gốc với để được bản tiếng vọng của tín hiệu âm thanh ứng với
* Tạo một tín hiệu trộn sử dụng những bits được mã hóa vào như hình:



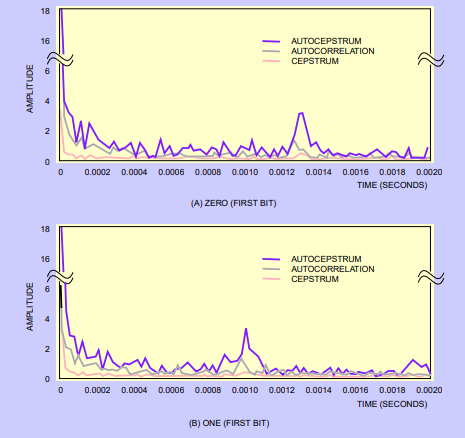
Hình 6: Mixer sử dụng để trộn 2s channel với tín hiệu gốc

* Thêm tiếng vọng vào tín hiệu âm thanh gốc bằng tín hiệu trộn trong phương trình

**Trích xuất dữ liệu**

Quá trình giải mã sử dụng việc phân tích tần số. Audio ẩn sẽ được chia thành những phân khúc bằng với số bit cùng với độ dài phân khúc đã được mã hóa. Sau đó lấy phần số thực của tần âm tại điểm có offset trùng với bit tương ứng như phương trình

Với:



Hình 7: Hình ảnh âm phổ trên thời gian

**HAMMING CODE**

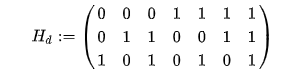
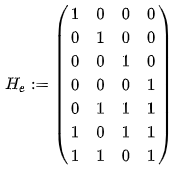
Hamming code là một tập các code tự sửa lỗi có thể dùng để phát hiện và tự sửa lỗi có thể xảy ra trong quá trình truyền và lưu dữ liệu từ người gửi đến người nhận. Kỹ thuật này được phát triển bởi R.W.Hamming.

Trong quá trình mã hóa/giải mã, có nhiều tác nhân gây sai lệch trong tần số của tiếng vọng, trong đó có thể là lỗi trong việc lưu tập tin, hoặc tấn công cả cố ý và vô ý. Vì vậy việc sửa lỗi bits sẽ tăng độ chính xác trong việc giải mã thông tin.

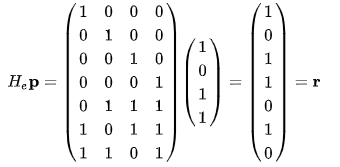
Ta sẽ sử dụng Haming(7,4) để mã hóa và giải mã đoạn bit truyền vào

**MA TRẬN HAMMING**

Chúng ta có 2 ma trận HAMMING đi liền với nhau:



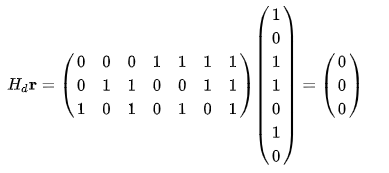
Chúng ta truyền một nhóm 4 bits dữ liệu : (1,0,1,1)   
Ta tính tích của và p



Sau đó mã hóa đoạn thông tin vào bản nhạc.

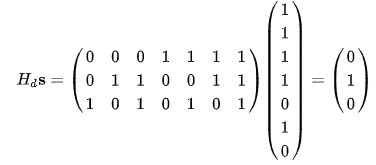
**Giải mã**

Khi giải mã, để kiểm tra có lỗi xảy ra hay không chúng ta sẽ nhân và r



**Sửa lỗi**

Nếu có lỗi xảy ra kết quả sẽ trả về vị trí lỗi của nó, ví dụ chúng ta sai ở bit thứ 2:



Kết quả trả về tương đương “010” là 2

**III THỰC NGHIỆM KẾT QUẢ**

**Thực nghiệm thuật toán**

So sánh giữa 32 mẫu nhạc gồm nhiều thể loại khác nhau Pop, Vpop, Rock, EDM,… Gồm nhiều độ dài khác nhau và sampled khác nhau.  
Sử dụng các thông số:

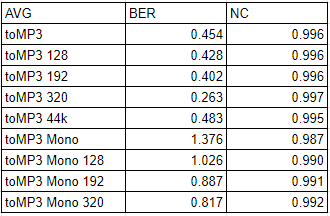
* L = Segment Bits Length = 8192 bit
* O = Offset = 0.04 ms
* D = Delta = 0.02 ms
* Amp = Echo Amplitude = 0.3

Sau đó sử dụng các kiểu tấn công nhằm thay đổi chất lượng như chuyển đổi định dạng, resampling, chuyển sang mono…  
Những file bị tấn công sau đó được giải mã và tính toán các thông số

* BER (Bit Error Rate)
* NC (Normalized Correlation)
* SNR (Sample-to-Noise Ration)

Để có thể đánh giá độ tin cậy của thuật toán.

**Kết quả thực nghiệm**



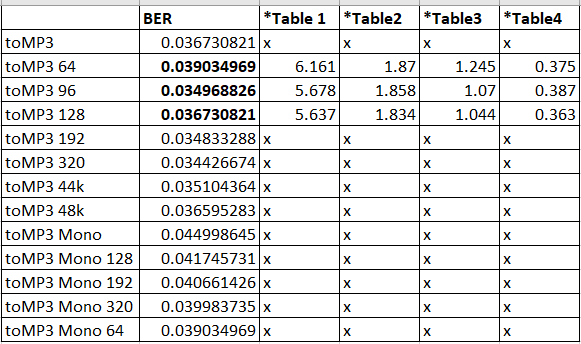
Bảng 1: Kết quả thu được thực nghiệm Bit Error Rate và Normalize Correlation

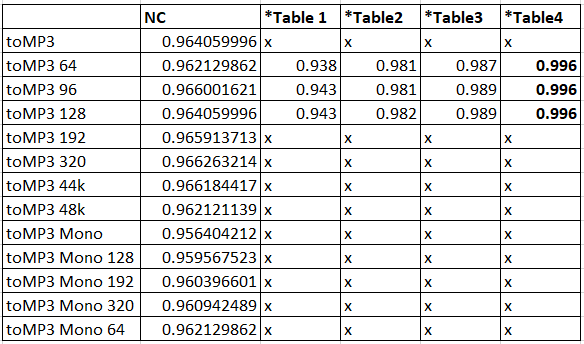


Kết quả cho thấy thuật toán hoàn toàn có thể chống các kiểu tấn công thay đổi định dạng rất tốt, với tỉ lệ BER thấp, hệ thống có thể đảm bảo tính mạnh mẽ trong việc bảo vệ tác quyền âm nhạc.

Với SNR cao trên 13.0, kết quả cho thấy khả năng nhận ra sự thay đổi file nhạc rất thấp, ngoài ra với việc sử dụng một mixer tốt làm cho đoạn thông điệp gần như không thể nghe được.

Dựa theo quyển A COMPARISON OF ECHO HIDING METHODS - Kadir Tekeli ,Rifat Asliyan - Adnan Menderes University – ISRES phát hành[3]





Bảng 7.2.1.2. Kết quả dùng làm đối sánh

Ta có thể thấy khi watermark chỉ một đoạn âm thanh, cộng với tỉ lệ nhúng thấp do thông tin cần đánh dấu nhỏ, tỉ lệ SNR rất cao việc phát hiện ra dữ liệu bị ẩn thấp. Tỉ lệ BER cũng thấp trong ngưỡng cho phép có thể tự sửa lỗi bằng mã sửa lỗi Hamming

Kết quả cũng cho thấy khả năng chống tấn công dạng thay đổi định dạng file rất tốt khi tất cả các file đều bị phát hiện tồn tại watermark với tỉ lệ BER rất thấp

**Thực nghiệm ứng dụng**

Ứng dụng đã đạt được những yêu cầu ban đầu đặt ra:

* Thực nghiệm trên 32 file và 4 người nghe khác nhau cho thấy người nghe không nhận ra được sự khác nhau giữa file đã watermarked và file gốc. Nếu có nhận ra thì người nghe có cảm giác hay hơn.
* Ứng dụng đã có đầy đủ những tính năng của một hệ thống phân phối âm nhạc bao gồm nghe, upload, download,…
* File gốc được bảo vệ và không thể truy cập được.
* Upload nhiều files thì các files được xử lý bất đồng bộ, vì thế tốc độ watermark cao tuy nhiên vẫn bị giới hạn để không ảnh hưởng tới hoạt động của hệ thống
* File download được bảo vệ dưới các kiểu tấn công. Bị phát hiện ngay lập tức khi reupload lên hệ thống.
* Ứng dụng có độ tin cậy cao. Tỉ lệ phát hiện sai là 0%

Sau khi thực nghiệm ứng dụng. Ứng dụng đã cho thấy được sự khả thi của việc ứng dụng watermarking vào hệ thống phân phối âm nhạc. Tuy nhiên vẫn có nhiều vấn đề nảy sinh sau khi đánh giá hệ thống như.

* Watermark không được giấu pseudorandom generated. Giả sử ta có user-case như sau: Người dùng A upload file nhạc -> Người dùng B download file đã watermarked rồi reupload. Mối liên kết duy nhất giữa A và B là file watermarked. Để có thể pseudorandom generated chúng ta phải giải quyết 2 bài toán:
* Một thuật toán sinh ra một số mà khi cho tín hiệu gốc, và tín hiệu đã watermark vào đều sinh ra một số.
* Một thuật toán mà muốn thay đổi số sinh ra phải thay đổi rất nhiều tín hiệu đến mức làm ảnh hưởng đến chất lượng âm thanh

Sau khi nghiên cứu và giải quyết bài toán, nhóm cho rằng kỹ thuật Audio Fingerprint sẽ phù hợp để giải quyết bài toán này.

**KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

Hệ thống NKMusic đã được hoàn thiện với các tiêu chí sau:

* Áp dụng thuật toán watermarking vào một ứng dụng có tính thực tiễn. Chứng minh tính khả thi của thuật toán watermarking nói chung và EH nói riêng.
* Tạo nên một hệ thống nghe nhạc có thể hoạt động theo hướng thương mại, tạo nên lợi nhuận cho người phát triển nhờ sự bảo vệ bản quyền âm nhạc rất cạnh tranh.
* Giúp bảo vệ tác quyền cho các nhà phân phối âm nhạc/nhạc sĩ tự do. Chống gian lận bản quyền, kiếm tiền bất chính từ trí tuệ của các nhạc sĩ.
* Chống lại các kiểu tấn công vô ý cũng như cố ý như nén, resample, merge channels,…

**Hướng phát triển**

* Watermark không được giấu pseudorandom generated. Giả sử ta có user-case như sau: Người dùng A upload file nhạc -> Người dùng B download file đã watermarked rồi reupload. Mối liên kết duy nhất giữa A và B là file watermarked. Để có thể pseudorandom generated chúng ta phải giải quyết 2 bài toán:
* Một thuật toán sinh ra một số mà khi cho tín hiệu gốc, và tín hiệu đã watermark vào đều sinh ra một số.
* Một thuật toán mà muốn thay đổi số sinh ra phải thay đổi rất nhiều tín hiệu đến mức làm ảnh hưởng đến chất lượng âm thanh

Sau khi nghiên cứu và giải quyết bài toán, nhóm cho rằng kỹ thuật Audio Fingerprint sẽ phù hợp để giải quyết bài toán này.

**TÀI LIỆU THAM KHẢO**

1. Deepali Brahmbhatt, Mark Stamp - Digital Rights Management for Streaming Media chapter II - San Jose State University, USA
2. Frank Hartung and Friedhelm Ramme - Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications - [IEEE](https://www.researchgate.net/journal/0163-6804_IEEE_Communications_Magazine),2000
3. Kadir Tekeli & Rifat Asliyan - A COMPARISON OF ECHO HIDING METHODS - EPSTEM, 2017
4. Leandro de C.T. Gomes , Pedro Cano , Emilia Gómez , Madeleine Bonnet , Eloi Batlle - Audio Watermarking and Fingerprinting: For Which Applications? -  Journal of New Music Research, 2003
5. Michael Arnold - AUDIO WATERMARKING: FEATURES, APPLICATIONS AND ALGORITHMS – IEEE, 2000
6. I. J. Cox, J. Kilian, F. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical report 95-10, NEC Research Institute, Princeton, NJ, USA, 1995.
7. Stephan Wiefling - Comparison of Audio Watermarking-Techniques - Master Hauptseminar Medientechnologie WS 15/16
8. Namita Verma, Vinay Kumar Jain - Audio Steganography – A Review, ISSN: 2278 – 909X, IJARECE, 2013
9. D. Gruhl, A. Lu, and W. Bender. Echo hiding. In R. J. Anderson, editor, Information Hiding, First International Workshop, Cambridge, U.K., May 30 - June 1, 1996, Proceedings, volume 1174 of Lecture Notes in Computer Science, pages 293–315. Springer, 1996.
10. W. Bender, D. Gruhl, N. Morimoto, A. Lu - Techniques for data hiding -  Ibm Systems Journal · January 1996
11. Neil Jenkins1 , Jean Everson Martina - Steganography in Audio - University of Cambridge - 2003