# GIẢI PHÁP


WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

Sáng chế quốc tế 24 điểm bảo hộ, WIPO: **WO2022043756**

**HÀ NỘI 2022**

# CÁC TÍNH NĂNG CHÍNH



# CÁC TÍNH NĂNG NÂNG CAO

# I. GIỚI THIỆU

Xin gửi tới các đơn vị quan tâm, giới thiệu hàng rào điện tử công nghệ cao eFence, được phát triển trên các nền tảng kỹ thuật bảo mật tốt nhất thế giới hiện nay.

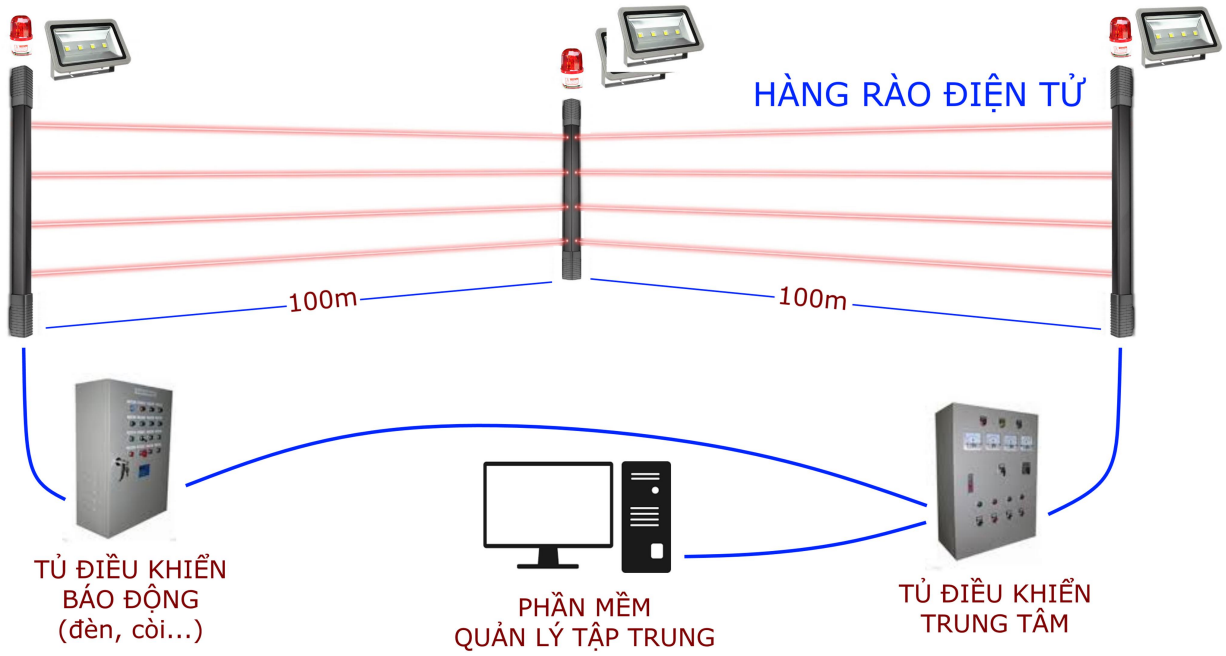
So với các hàng rào chống trộm dân dụng hiện nay sử dụng công nghệ chùm tia hồng ngoại, vốn không áp dụng các biện pháp bảo mật phòng chống tội phạm kỹ thuật cao, rất dễ bị xâm nhập bằng các phương pháp đơn giản; thì eFence đặc biệt ưu trội vì hàm chứa các biện pháp khắc chế hoàn toàn nhược điểm đó, đồng thời có những tính năng vượt trội khác.

Phạm vi ứng dụng:

- Hệ thống hàng rào và cảnh báo xâm nhập dành cho các đơn vị có chu vi cần bảo vệ rộng lớn, lực lượng bảo vệ không thể bao quát toàn diện và toàn bộ thời gian. Như:
  - Nhà máy, xí nghiệp, khu công nghiệp;
  - Cơ quan có nhu cầu an ninh bảo mật cao;
  - Kho hàng, bến đỗ cần được bảo vệ
- Hệ thống hàng và cảnh báo xâm nhập dành cho hộ gia đình

# II. NGUYÊN LÝ KỸ THUẬT

## 1. Sơ đồ nguyên lý hệ thống cảnh báo hàng rào:



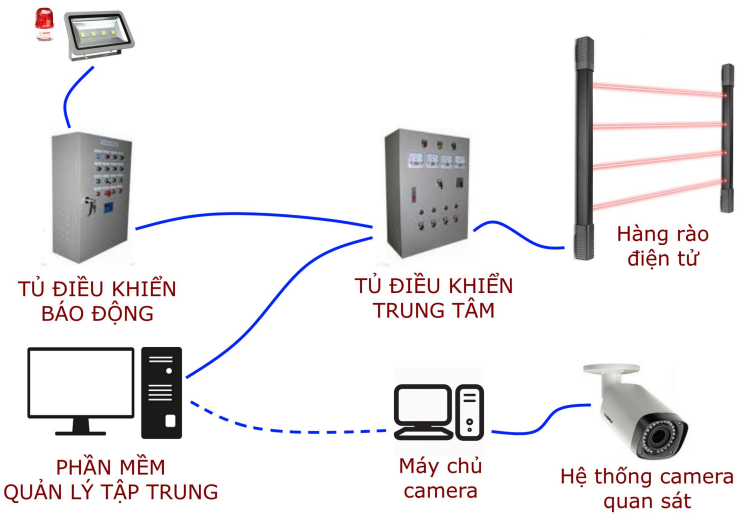

*Hình 1: Sơ đồ khối nguyên lý hệ thống hàng rào điện tử*

**Các thiết bị sử dụng trong hệ thống hàng rào điện tử bao gồm:**

- Các cột cảm biến: khoảng cách làm việc 100m; sử dụng công nghệ xung hồng ngoại đa tia
- Mỗi cột đều lắp đặt còi báo động, đèn pha rọi
- Hệ thống cáp nối, chuyển đổi tín hiệu
- Hệ thống điện dự phòng (UPS, chuyển nguồn ATS)
- Tủ điều khiển trung tâm: tiếp nhận thông tin cảnh báo từ cột cảm biến
- Tủ điều khiển cảnh báo: phát tín hiệu cảnh báo đến các thiết bị cảnh báo (còi, đèn…)
- Các thiết bị cảnh báo (Còi, đèn, …) được gắn trên mỗi đỉnh cột cảm biến
- Modem GSM (dùng để nhắn tin, gọi điện khi có báo động)
- Trung tâm báo động: máy tính cài phần mềm eFence
- Các phụ kiện hỗ trợ vận hành khác (khóa điện tử bằng thẻ / nhập mã PIN …)

**Hoạt động:**

- Các cột cảm biến khi phát hiện xâm nhập lập tức báo về tủ điều khiển trung tâm
- Tủ điều khiển trung tâm tự động kích hoạt báo động: gửi tín hiệu báo động sang tủ điều khiển báo động
- Tủ điều khiển trung tâm gửi thông tin báo động về phần mềm quản lý trung tâm: Hiển thị trên màn hình lớn, lưu trữ thông tin,
- ***Kết nối liên động tới các hệ thống khác (camera quan sát, Access Control)***



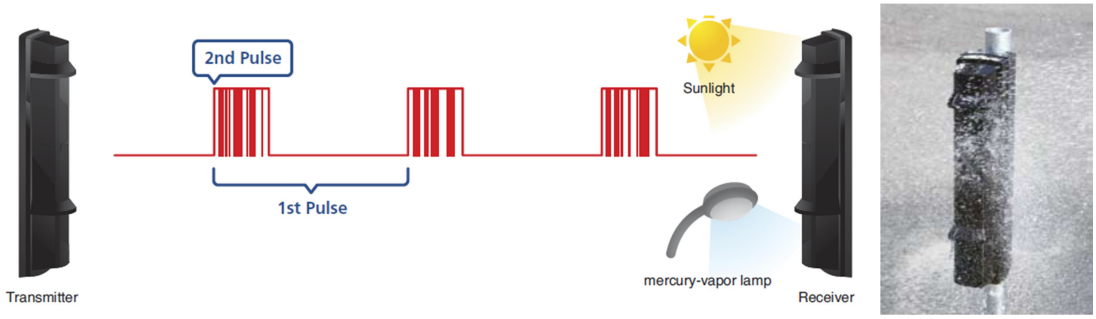

*Hình 2: Sơ đồ khối kết nối liên động hệ thống hàng rào điện tử với hệ thống camera giám sát*

## 2. Tính ưu việt của hệ thống

So với các giải pháp truyền thống, hệ thống báo động mới có các ưu điểm sau:

- Sàng lọc được sự xâm nhập của người và vật thể nhỏ:

- Hệ thống không bị ảnh hưởng bởi thời tiết khách nghiệt (mưa, sương mù, ánh sáng…)



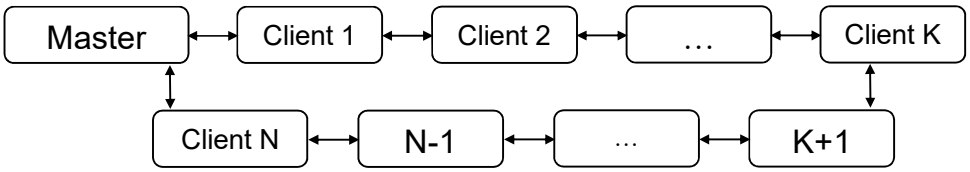

- Dễ dàng vận hành và thao tác, có thể nâng cấp với các hệ thống cũ chưa có hệ thống báo động.
- Chống xâm nhập điện tử. Với công nghệ mã hóa xung đã nêu ở trên. Các công nghệ cũ dễ dàng bị giả mạo chùm tia, với eFence, nguyên lý chùm tia mã hóa xung ngăn chặn hoàn toàn mọi khả năng giả mạo chùm tia
- Phạm vi bảo vệ rộng lớn: từ hộ gia đình, đến kho tàng, bến bãi, các khu vực trọng yếu, biên giới, hải đảo
- Chức năng báo cáo, thống kê các sự kiện báo động, cảnh báo theo thời gian, vị trí, loại cảnh báo…

## 3. Phần mềm cảnh báo trung tâm:

Trung tâm báo động là máy tính cài phần mềm eFence. Phần mềm eFence có nhiệm vụ thu nhận, xử lý các tín hiệu từ các cảm biến, điều khiển các đầu ra tương ứng. Các sự kiện cảnh báo, báo động được lưu giữ trên máy tính phục vụ cho công tác thống kê, hậu kiểm …

# III. WIPO WO2022043756

**TrainLoop PackTransfer**
Mạng chuyển mạch gói cấu trúc đoàn tàu

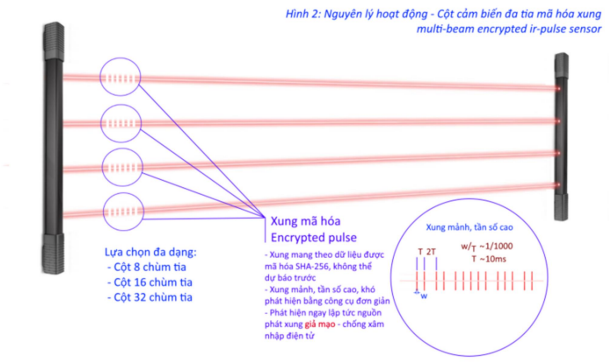



Đường truyền tin kết nối giữa các cột, có các tính năng:

- Tự động đánh địa chỉ các cột: các cột đánh địa chỉ, cho phép mở rộng đến $2^{16}$ cột – tương đương hàng ngàn kilomet hàng rào;
- Cấu trúc mạng đoàn tàu (TrainLoop): cho phép phát hiện đứt cáp giữa 2 cột bất kỳ để báo cho người sử dụng, phần còn lại của hệ thống vẫn hoạt động bình thường;
- Cột bất kỳ gặp sự cố mất điện, mất liên lạc: đều được phát hiện để báo cho người sử dụng, phần còn lại của hệ thống vẫn hoạt động bình thường;
- Thường xuyên cập nhật trạng thái hoạt động, cảnh báo xâm nhập, báo động;
- Các gói tin trên đường truyền được mã hóa bảo mật đường truyền; hệ thống sử dụng *giải thuật mã hóa được chính phủ Mỹ lựa chọn sử dụng làm mã chuẩn để mã hóa các tài liệu mật từ 2004*

**Sercured BeamTransfer**
Lưới hồng ngoại mã hóa

- Chùm phát xạ hồng ngoại sử dụng công nghệ xung mã hóa. Công nghệ xung mã thể hiện các ưu điểm
- Chống nhiễu trắng: không bị ảnh hưởng bởi thời tiết nắng nóng
- Công nghệ PWM: phát xạ xung mảnh 5% - 10%; tối ưu công suất phát đồng thời tiết kiệm năng lượng;
- Các cột trao đổi dữ liệu mã hóa qua các chùm xung mã hóa. Mã được sử dụng thuật toán mã hóa một chiều không thể dự đoán trước.




Kỹ thuật này vô hiệu các thiết bị xâm nhập: nghe lén lưu lại các đoạn mã, phát xung giả mạo đánh lừa hàng rào;

**SmartDetect**
Nhận diện xâm nhập

- Với khoảng thời gian phát hiện $T_{detect} \approx 5.5ms$, có thể phát hiện:

  ⇒ Vật thể có kích thước 5cm chuyển động nhanh với tốc độ 30km/h đi qua;

  ⇒ Máy bay không người lái kích thước 1.5m bay với tốc độ cận âm ≈900km/h;

- Giải thuật nhận diện thông minh cho phép nhận diện và cảnh báo:

  ⇒ Cùng lúc nhận diện 4 vật thể;

  ⇒ Nhận diện nhiễu, không cảnh báo, ghi nhận và đo đạc nhiễu.

  Ví dụ: lá cây rung rinh, bụi, nhiễu nền ánh sáng mặt trời;

  ⇒ Cảnh báo vật thể nhỏ. Ví dụ: động vật nhỏ, vật thể nhỏ bay qua;

  ⇒ Báo động xâm nhập. Ví dụ: động vật lớn, người xâm nhập vượt qua hàng rào;

  ⇒ Báo động xâm nhập điện tử. Ví dụ: Hacker đang tìm cách xâm nhập điện tử;

- Gửi cảnh báo, báo động về trung tâm xử lý;

  Phát cảnh báo lên Đèn & Còi trên cột;

  Kết nối liên động: gửi cảnh báo / báo động sang các hệ thống khác (Access Control, Camera)

**UltraRange**
Phạm vi bảo vệ rộng lớn

- Mỗi cột cảm biến hồng ngoại được trang bị 8 chùm tia (hoặc 16 chùm tia, 32 chùm tia, tùy chọn theo kích thước)
- Mỗi cột có khả năng phát xạ và thu nhận các chùm tia theo 2 hướng (trái, phải), mỗi cột được đánh địa chỉ 16 bits

  ⇒ Tạo ra kết cấu hàng rào nối tiếp liên tiếp, lên tới tối đa $2^{16}$ cột (65536 cột, tương đương 6500km)
- Phát xạ xung hồng ngoại qua thấu kính quang học: khoảng cách phát xạ lên tới 100m (trong tương lai có thể phát xạ xa hơn nữa);
  Cùng với khả năng xuyên thấu bụi bẩn, các điều kiện thời tiết khắc nghiệt: mưa rào, mưa phùn, mưa tuyết, sương mù, phơi nắng…

| MODEL | SEB08-100 | SEB16-100 | SEB32-100 |
|---|---|---|---|
| Số chùm tia | 08 | 16 | 32 |
| Khoảng cách làm việc | 100m | 100m | 100m |
| Mã hóa xung SHA-256 (256 bits) | Có | Có | Có |
| Kết nối mạch vòng | Có | Có | Có |
| Kết nối thiết bị cảnh báo (đèn, còi) | Có | Có | Có |
| Kết nối trung tâm | Có | Có | Có |

**CryptoDenfense**
Không thể bị hack

Hàng rào được trang bị thuật toán CryptoDefense hội tụ các công nghệ mật mã tối tân nhất thế giới hiện nay, CryptoDefense có tính chất: không thể bị tấn công mật mã, ngay cả với các siêu máy tính hiện đại nhất hiện nay, hay các phương pháp giải mã phân tán trên toàn mạng *internet of things*

Các phương pháp tấn công hàng rào đều phải tấn công CypherKey.


CypherKey được cấu thành từ 3 thành phần: mã của nhà sản xuất (MasterKey), mã của người sử dụng (UserPIN), mã ngẫu nhiên thay đổi theo epoch không thể đoán trước (Seed) chỉ có hệ thống biết. Bất kỳ ai không nắm được đầy đủ 3 thành phần này của CypherKey đều không thể giải các câu đố mã hóa truyền giữa các cột.

Hãy cùng phân tích các phương án tấn công mật mã sau đây để thấy rõ năng lực phòng thủ mật mã của hệ thống:

**Tấn công cấp độ 1:**

***Điều kiện:***

- Không biết CypherKey,
- Không tiếp xúc trực tiếp với hàng rào, không thể nghe lén random_token

***Phương thức tấn công: giả mạo dữ liệu***

- Điều kiện tức là không có bảng mã, không có mã rõ

⇒ không thể giả mạo dữ liệu truyền qua các chùm tia trong mỗi session

- Nếu thu lại tín hiệu trên đường truyền, hòng tìm ra quy luật lặp lại:

⇒ Không thể, vì dữ liệu truyền trên đường truyền là khác nhau mỗi sesion, và trong mỗi session phân bố thông tin trong dữ liệu rất gần với phân bố đều (ngẫu nhiên)

***Kết quả:***

⇒ Không thể giả mạo dữ liệu truyền qua các chùm tia.

**Tấn công cấp độ 2:**

***Điều kiện:***

- Không biết CypherKey,
- Tiếp xúc trực tiếp với hàng rào ⇒ có thể nghe lén random_token vì random_token được truyền không mã hóa trên đường truyền PackTransfer

***Phương thức tấn công: giả mạo dữ liệu***

- Tấn công giả mạo dữ liệu truyền qua các chùm tia trong mỗi session
- Để thực hiện được tấn công này, hacker phải tấn công mã CypherKey dài 256 bits. Cách duy nhất hiệu quả là phương pháp BruteForce $2^{256}$ trường hợp trong vòng 1 epoch cỡ 1 ngày đến 1 tháng; tương đương cỡ $10^{70}$ phép thử trong 1 giây, sức mạnh tính toán này chưa tồn tại, ngay cả cộng gộp tất cả siêu máy tính và các thiết bị điện tử rời rạc cũng chưa đủ.

***Kết quả:***

⇒ Chưa có công cụ đủ sức mạnh để tấn công. Tức là không thể tấn công.

**Tấn công cấp độ 3:**

***Điều kiện:***

- Không biết CypherKey, nhưng bằng cách nào đó biết được UserPIN của User, đồng thời bằng cách nào đó biết được MasterKey của Coder và đã đọc toàn bộ tài liệu này; nhưng không biết Seed. *Lưu ý rằng điều kiện này rất khó đạt được, vì user cất rất kỹ UserPIN, nhưng giả định rằng có khả năng xảy ra.*
- Tiếp xúc trực tiếp với hàng rào, nghe lén random_token vì random_token được truyền không mã hóa trên đường truyền PackTransfer
- Đây là điều kiện được cho là tốt nhất, khi phe tấn công biết được rất nhiều thông tin về hệ thống đang vận hành (toàn bộ đặc tính kỹ thuật, thuật toán).

***Phương thức tấn công: tấn công hòng tìm ra CypherKey***

- Để thực hiện được tấn công này, hacker phải tấn công mã khi chưa biết Seed. Seed là 1 hoán vị ngẫu nghiên 32 phần tử do hệ thống sinh ra mỗi epoch.

  Cách duy nhất hiệu quả là phương pháp BruteForce cho 32! (32 giai thừa) trường hợp hoán vị Seed trong vòng 1 epoch cỡ 1 ngày đến 1 tháng; tương đương cỡ $10^{30}$ phép thử trong 1 giây, sức mạnh tính toán này chưa tồn tại, ngay cả cộng gộp tất cả siêu máy tính và các thiết bị điện tử rời rạc cũng chưa đủ.

***Kết quả:***

⇒ Chưa có công cụ đủ sức mạnh để tấn công.

Tức là không thể tấn công.

Điều này cũng hàm ý rằng, ngay cả coder hay người vận hành hệ thống cũng không có năng lực tấn công mật mã vào hệ thống này.

**Tấn công cấp độ 4:**

***Điều kiện:***

- Tiếp xúc trực tiếp với hàng rào,

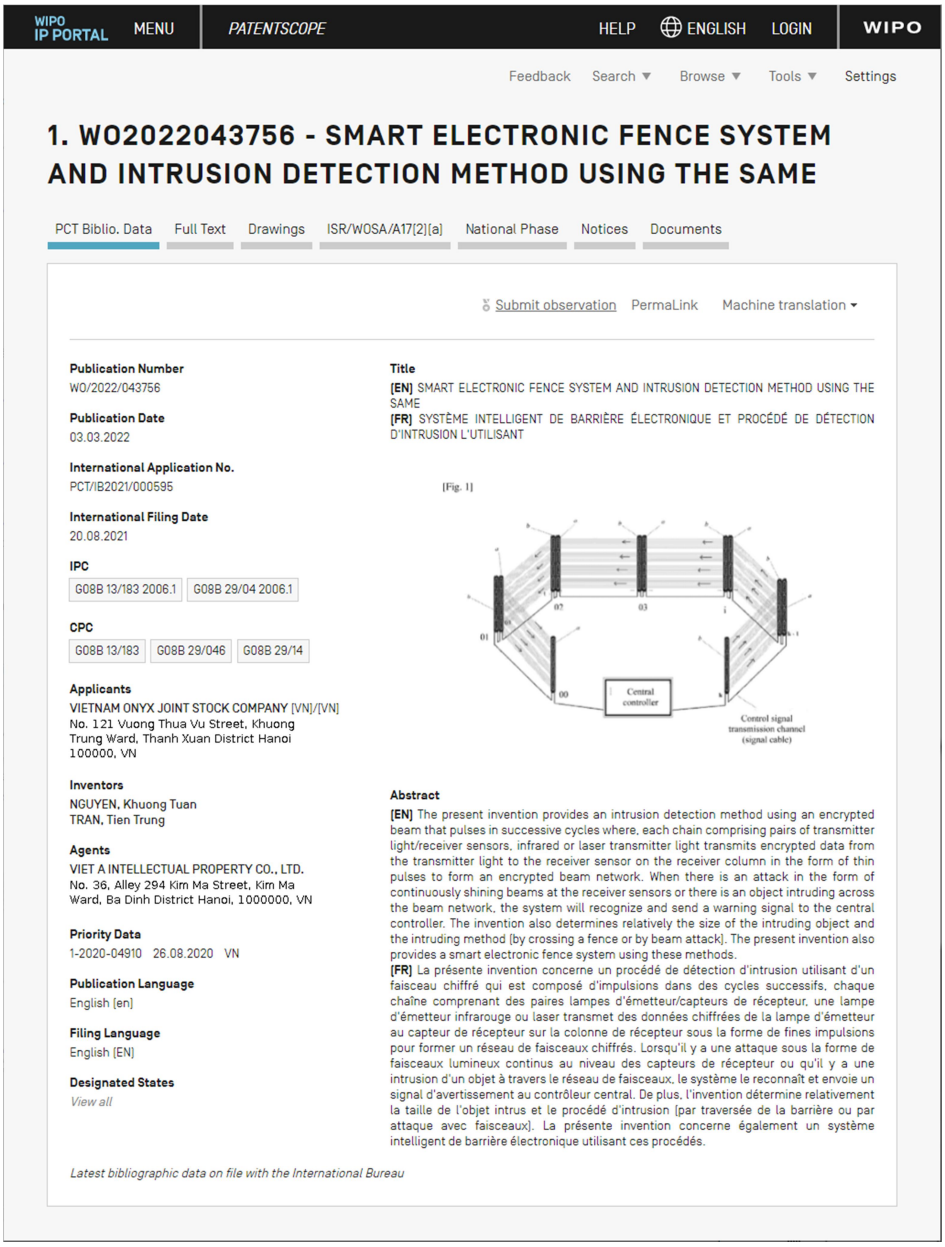
***Phương thức tấn công: giả mạo trạng thái các cột***

- Chặn các gói tin Alarm và giả mạo gói tin báo trạng thái bình ổn Status, hòng đánh lừa hàng rào
- Vì các gói tin Status là các gói tin có xác thực bằng mã CypherKey, cho nên giả mạo Status chính là tấn công CypherKey, các phân tích chi tiết quay về các cấp độ tấn công mật mã 1-3, tức là không thể thực hiện.

***Kết quả:*** không thể thực hiện.

Cả 4 cấp độ tấn công nêu trên đều không hiệu quả với hệ thống mật mã của hàng rào eFence.

## WO2022043756



WIPO IP PORTAL MENU PATENTSCOPE HELP ENGLISH LOGIN WIPO

Feedback Search Browse Tools Settings

**1. WO2022043756 - SMART ELECTRONIC FENCE SYSTEM AND INTRUSION DETECTION METHOD USING THE SAME**

PCT Biblio. Data | Full Text | Drawings | ISR/WOSA/A17[2][a] | National Phase | Notices | Documents

Submit observation PermaLink Machine translation

**Publication Number**
WO/2022/043756

**Publication Date**
03.03.2022

**International Application No.**
PCT/IB2021/000595

**International Filing Date**
20.08.2021

**IPC**
G08B 13/183 2006.1 | G08B 29/04 2006.1

**CPC**
G08B 13/183 | G08B 29/046 | G08B 29/14

**Applicants**
VIETNAM ONYX JOINT STOCK COMPANY [VN]/[VN]
No. 121 Vuong Thua Vu Street, Khuong Trung Ward, Thanh Xuan District Hanoi 100000, VN

**Inventors**
NGUYEN, Khuong Tuan
TRAN, Tien Trung

**Agents**
VIET A INTELLECTUAL PROPERTY CO., LTD.
No. 36, Alley 294 Kim Ma Street, Kim Ma Ward, Ba Dinh District Hanoi, 1000000, VN

**Priority Data**
1-2020-04910 26.08.2020 VN

**Publication Language**
English (en)

**Filing Language**
English (EN)

**Designated States**
*View all*

**Title**
**(EN)** SMART ELECTRONIC FENCE SYSTEM AND INTRUSION DETECTION METHOD USING THE SAME
**(FR)** SYSTÈME INTELLIGENT DE BARRIÈRE ÉLECTRONIQUE ET PROCÉDÉ DE DÉTECTION D'INTRUSION L'UTILISANT

[Fig. 1]



**Abstract**
**(EN)** The present invention provides an intrusion detection method using an encrypted beam that pulses in successive cycles where, each chain comprising pairs of transmitter light/receiver sensors, infrared or laser transmitter light transmits encrypted data from the transmitter light to the receiver sensor on the receiver column in the form of thin pulses to form an encrypted beam network. When there is an attack in the form of continuously shining beams at the receiver sensors or there is an object intruding across the beam network, the system will recognize and send a warning signal to the central controller. The invention also determines relatively the size of the intruding object and the intruding method (by crossing a fence or by beam attack). The present invention also provides a smart electronic fence system using these methods.
**(FR)** La présente invention concerne un procédé de détection d'intrusion utilisant d'un faisceau chiffré qui est composé d'impulsions dans des cycles successifs, chaque chaîne comprenant des paires lampes d'émetteur/capteurs de récepteur, une lampe d'émetteur infrarouge ou laser transmet des données chiffrées de la lampe d'émetteur au capteur de récepteur sur la colonne de récepteur sous la forme de fines impulsions pour former un réseau de faisceaux chiffrés. Lorsqu'il y a une attaque sous la forme de faisceaux lumineux continus au niveau des capteurs de récepteur ou qu'il y a une intrusion d'un objet à travers le réseau de faisceaux, le système le reconnaît et envoie un signal d'avertissement au contrôleur central. De plus, l'invention détermine relativement la taille de l'objet intrus et le procédé d'intrusion [par traversée de la barrière ou par attaque avec faisceaux]. La présente invention concerne également un système intelligent de barrière électronique utilisant ces procédés.

*Latest bibliographic data on file with the International Bureau*

Sáng chế quốc tế WIPO số WO2022043756
Công bố quốc tế ngày 03/03/2022

# IV. KẾT NỐI LIÊN ĐỘNG

## TrustFaceID

### 1. TrustFaceID là gì:

TrustFaceID = iSeal + FaceID

Là một hệ thống xác thực sinh trắc học 2 yếu tố,

Trong đó yếu tố thứ 2 là Thẻ an ninh, được sử dụng công nghệ iSeal với chữ ký số thay đổi liên tục chống giả mạo (chống sao chép thẻ); là một sáng chế quốc tế wipo số WO2022094635 khai thác đặc tính xác thực ưu việt của thuật toán Blockchain.

Với công nghệ này, xác thực sinh trắc học 2 yếu tố trở nên chính xác hơn đạt mức cao nhất.

Khi so sánh với các phương thức xác thực sinh trắc học 2 yếu tố khác, như Khuôn mặt + Vân tay, hoặc Khuôn mặt + Giọng nói, hoặc Khuôn mặt + Dáng đi, thì các phương thức khác đều khiến cho độ phức tạp tính toán **tăng lên theo cấp số nhân.** Cũng đồng nghĩa với chi phí để giải quyết tăng theo cấp số nhân, khiến cho tính khả thi giảm xuống.

### 2. Mục đích kết nối liên động eFence tới TrustFaceID:

Trong một số phương án triển khai eFence, lưới hồng ngoại mã hóa có thể cần phải bao phủ một số khu vực / giao lộ, là nơi vẫn cần có truy nhập được phân quyền.

Truy nhập được phân quyền tức là một số cán bộ chuyên trách, hoặc các chủ thể được cấp quyền truy nhập (vào/ra) các khu vực này. Hệ thống kiểm soát truy nhập được phân quyền gọi là Access Control (kiểm soát vào ra)

Để việc truy nhập phân quyền không gây ra báo động, sự kết nối liên động giữa eFence và Access Control là cần thiết. Và TrustFaceID là giải pháp kiểm soát vào ra tối ưu khi xét trên 2 yếu tố Xác thực an toàn và chi phí.

### 3. Sơ đồ nguyên lý kết nối liên động TrustFaceID:

Hình 3 mô tả sơ đồ nguyên lý kết nối liên động giữa eFence và TrustFaceID

**Hệ thống cần được trang bị thêm:**

- Hạ tầng thiết bị: máy chủ Sinh trắc học 2 yếu tố TrustFaceID, camera nhận diện khuôn mặt, đầu đọc thẻ công nghệ xác thực thẻ iSeal, thẻ iSeal được cấp cho người sử dụng
- Hạ tầng thông tin: Hệ thống AI nhận diện khuôn mặt, kết nối thông tin tới phần mềm eFence


*Hình 3: Sơ đồ nguyên lý kết nối liên động eFence với TrustFaceID*

- Luồng thông tin: Khi người sử dụng "tít" thẻ, (1) ID định danh người dùng được xác minh ⇨ (2) tương ứng với ID đó là hình ảnh mẫu S được trích xuất từ cơ sở dữ liệu ⇨ (3) ảnh tức thời T được chụp từ camera nhận diện khuôn mặt được AI đối sánh với ảnh mẫu S ⇨ (4) Xác minh T có đúng là S đã được lưu hay không ⇨ (5) thông báo liên động tới eFence về truy cập của ID ⇨ (6) eFence kiểm tra quyền truy cập ⇨ (7) từ chối nếu ID không có quyền truy cập, hoặc mở rào nếu có quyền truy cập
- Theo luồng thông tin mô tả ở trên, hoạt động của AI xác thực trở thành đối sánh 1-1, tức là tiêu tốn ít năng lực tính toán hơn (và thực tế là sử dụng cùng năng lực tính toán đó để đạt hiệu suất xác minh cao nhất)

**4. Các tính năng nâng cao có thể triển khai trên nền tảng:**

***Chống fake ảnh.*** Trong tình huống giả định:
- Bằng cách nào đó, Bình "mượn" được thẻ của An trong thời gian ngắn
- Trước đó, Bình có thể đã chụp hình được An

Lúc này, mặc dù thẻ của An là không thể sao chép, nhưng Bình đã có đủ điều kiện để vượt qua các điều kiện kiểm tra: thẻ + nhận diện hình ảnh
Lúc này, hệ thống cần nâng cấp tính năng chống fake bằng ảnh,

Chức năng này đã được chúng tôi phát triển, dựa trên phương pháp nhận diện ảnh 3D, với 02 camera đồng thời kiểm tra hình ảnh và độ sâu 3D của vật thể, khiến cho các phương pháp fake bằng ảnh bị vô hiệu

**Hệ thống cần được trang bị thêm:**

- Hạ tầng thiết bị: camera 3D, là hệ thống camera bao gồm 2 camera 2D đặt cạnh nhau, nhờ đó hình ảnh có độ sâu 3D và phân biệt được đối tượng là hình ảnh phẳng với vật thể 3 chiều, và loại bỏ được các bức ảnh fake
- Hạ tầng thông tin: Hệ thống AI nhận diện khuôn mặt, được trang bị module chống fake ảnh từ hình ảnh 3D

# V. KẾT NỐI LIÊN ĐỘNG Surveillance Camera

**1. Mục đích kết nối liên động eFence tới Hệ thống camera giám sát:**

Các hệ thống camera giám sát có chức năng phát hiện chuyển động đã có trên thị trường cũng là một lựa chọn cho việc phát hiện xâm nhập, tuy nhiên có nhiều hạn chế như là:

Triển khai với mật độ cao trong không gian rộng có chi phí cao

Khó triển khai tại các địa hình không gian hẹp

Quá nhiều chuyển động trong môi trường kích hoạt cảnh báo khiến tổ bảo vệ phải thường xuyên và liên kiểm tra camera

Trong khi ưu điểm của eFence lưới hồng ngoại mã hóa cho phép triển khai dễ dàng trong nhiều điều kiện thực tiễn, với năng lực phát hiện vật thể xâm nhập nhanh và chính xác, tuy nhiên nhược điểm là không lưu hình ảnh của vật thể

Do đó, việc kết hợp giữa eFence và camera giám sát tại các điểm quan sát được bố trí trước cho phép tối ưu công năng sử dụng của hệ thống. Khai thác ưu điểm của cả hai công nghệ, với mức chi phí phù hợp.

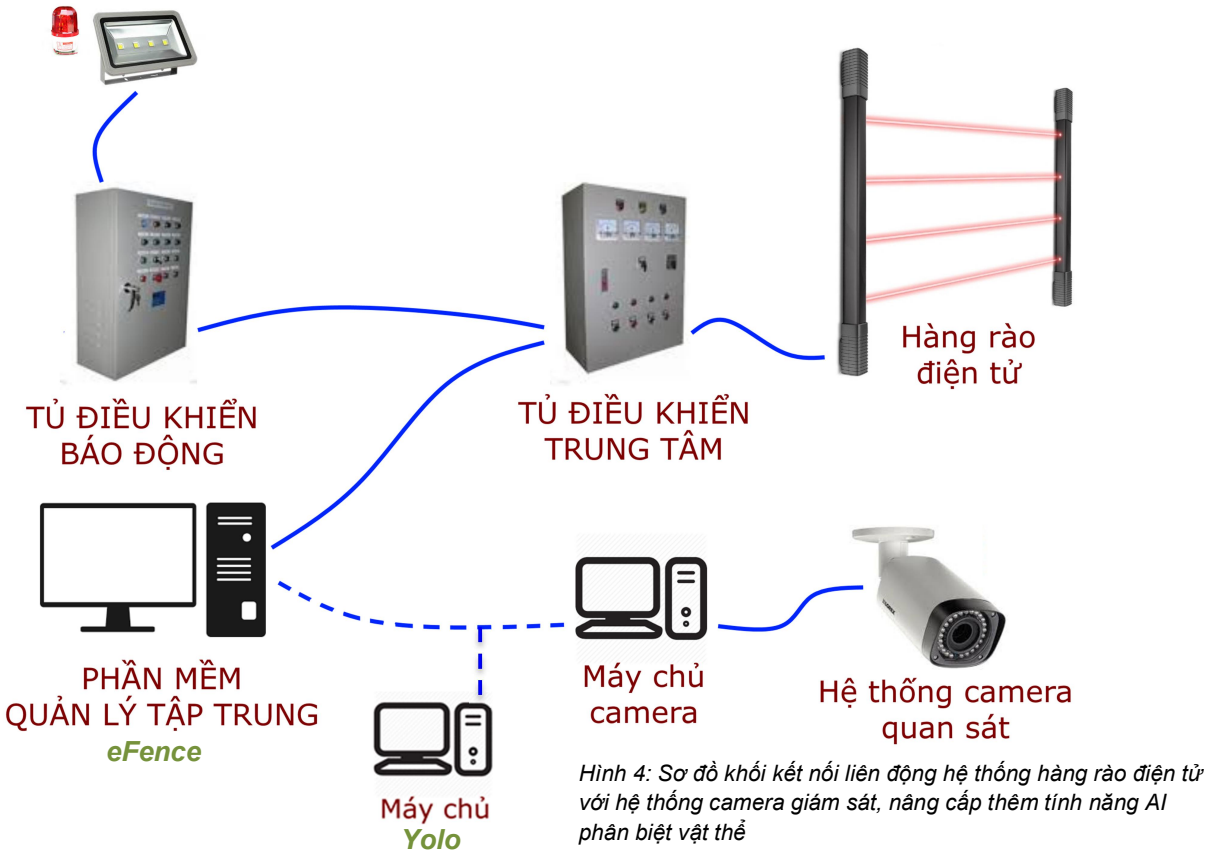
***Phương án kết nối liên động:***

- Lắp đặt thêm camera tại một số điểm quan sát được thiết kế trước
- Không nhất thiết mọi vị trí của hàng rào đều phải gắn camera
- Hệ thống lưới hồng ngoại mã hóa được thiết lập định vị theo logic: ghép cột node_id với camera_id tương ứng kiểm soát khu vực của cột đó

Khi hàng rào eFence phát hiện xâm nhập hoặc có vật thể nhỏ băng qua, eFence báo tín hiệu liên động sang hệ thống camera tương ứng, tính hiệu này là một thông tin ghi chú sự kiện giúp cho việc truy xuất thông tin từ camera dễ dàng hơn;

Đồng thời eFence hiển thị video-stream từ camera tương ứng lên màn hình điều khiển, cho phép tổ đội bảo vệ quan sát chi tiết hình ảnh từ camera báo về.

**2. Sơ đồ nguyên lý kết nối liên động tới Hệ thống camera giám sát:**




*Hình 4: Sơ đồ khối kết nối liên động hệ thống hàng rào điện tử với hệ thống camera giám sát, nâng cấp thêm tính năng AI phân biệt vật thể*

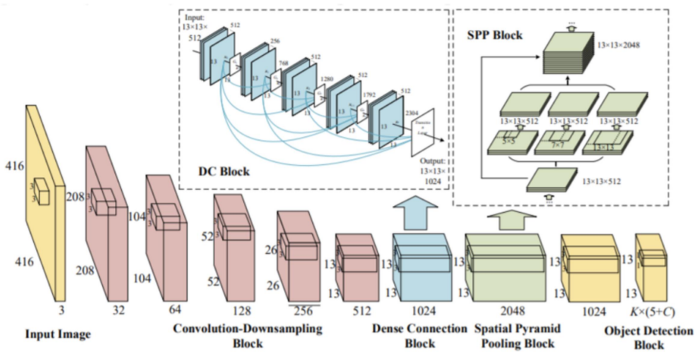
**3. Các tính năng nâng cao có thể triển khai trên nền tảng:**

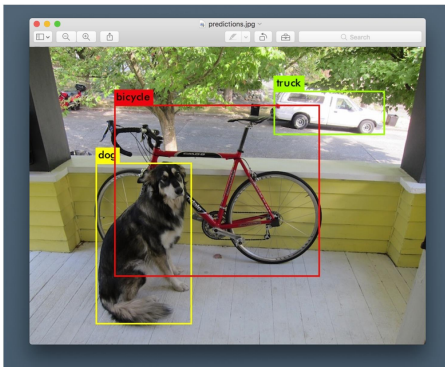
Triển khai trí tuệ nhân tạo phân biệt người và các vật thể khác. Nhằm hỗ trợ công tác giám sát của tổ bảo vệ.

Phương pháp nâng cấp:

- Trên nền tảng phần cứng hiện có
- Hạ tầng thiết bị: Bổ sung thêm máy chủ trí tuệ nhân tạo
- Hạ tầng thông tin: Triển khai phần mềm trí tuệ nhân tạo phân biệt người và các vật thể khác (Yolo), kết nối với phần mềm eFence
- Luồng thông tin: (1) Khi eFence phát hiện được vật thể xâm nhập, có thể là vật thể lớn hoặc vật thể nhỏ ⇨ (2) eFence gửi yêu cầu xác minh tới Yolo ⇨ (3) Yolo tiến hành chụp ảnh và phân tích vật thể, phân loại ⇨ (4) Yolo gửi thông tin gợi ý vật thể này là loại gì (người, động vật, xe cộ ...) sang eFence

⇨ (5) eFence bổ sung vào báo cáo cảnh báo, giúp cho bảo vệ có thêm thông tin hữu ích cho công việc bảo an




**TRÂN TRỌNG CẢM ƠN!**

Onyx

64/97 Văn Cao,
Liễu Giai, Ba Đình, Hà Nội
Website: https://onyx.vn
Hotline: +84.934.441.196

**Các giải pháp an ninh của Onyx**

Onyx Cypher

CyLock

eFence electronic security fence

TrueOrigin KEEP BELIEVING

WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION

Số sáng chế:
WO2022094635
WO2021174264
WO2022043756
PCT/VN2022/000001