(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0044459**

(51)[7] **H04L 29/06**; H04L 9/08

(13) **B**

(21) 1-2019-05416

(22) 02/10/2019

(45) 25/03/2025 444

(43) 26/04/2021 397A

(71) Trần Minh Sơn (VN)
Số 30 Hoàng Cầu, quận Đống Đa, thành phố Hà Nội

(72) Trần Minh Sơn (VN); Trần Quang Đức (VN); Trần Thu Hà (VN).

(74) CÔNG TY TRÁCH NHIỆM HỮU HẠN TƯ VẤN ĐẦU TƯ VÀ SỞ HỮU TRÍ TUỆ INTERFIVE (INTERFIVE CO., LTD)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG BẢO MẬT THÔNG TIN CHO CAMERA

(21) 1-2019-05416

(57) Sáng chế đề cập đến phương pháp và hệ thống bảo mật thông tin cho camera. Phương pháp bảo mật thông tin cho camera này bao gồm các bước: (a) kết nối khối chức năng bảo mật với ít nhất một camera, (b) tách ra ít nhất một luồng dữ liệu đa phương tiện từ camera, trong đó luồng dữ liệu đa phương tiện này được đóng gói ít nhất hai lần liên tiếp, lần đóng gói thứ nhất nén dữ liệu phù hợp với chuẩn nén để tạo ra các gói nén và lần đóng gói thứ hai tạo ra gói truyền dẫn theo định dạng của giao thức truyền dẫn, (c) tách các gói nén ra khỏi gói truyền dẫn và mã hóa các gói nén bằng ít nhất một khoá mã hoá, (d) tạo ra ít nhất một gói nén mới, được gọi là gói nén định danh mã hóa, theo chuẩn nén của camera, dùng để chứa ít nhất là thông tin định danh khóa của khóa mã hóa ở bước (c), (e) đóng gói gói nén định danh mã hóa được tạo ra ở bước (d) và các gói nén được mã hóa ở bước (c) vào gói truyền dẫn ở bước (b) theo đúng thứ tự và truyền dẫn gói này vào mạng internet.

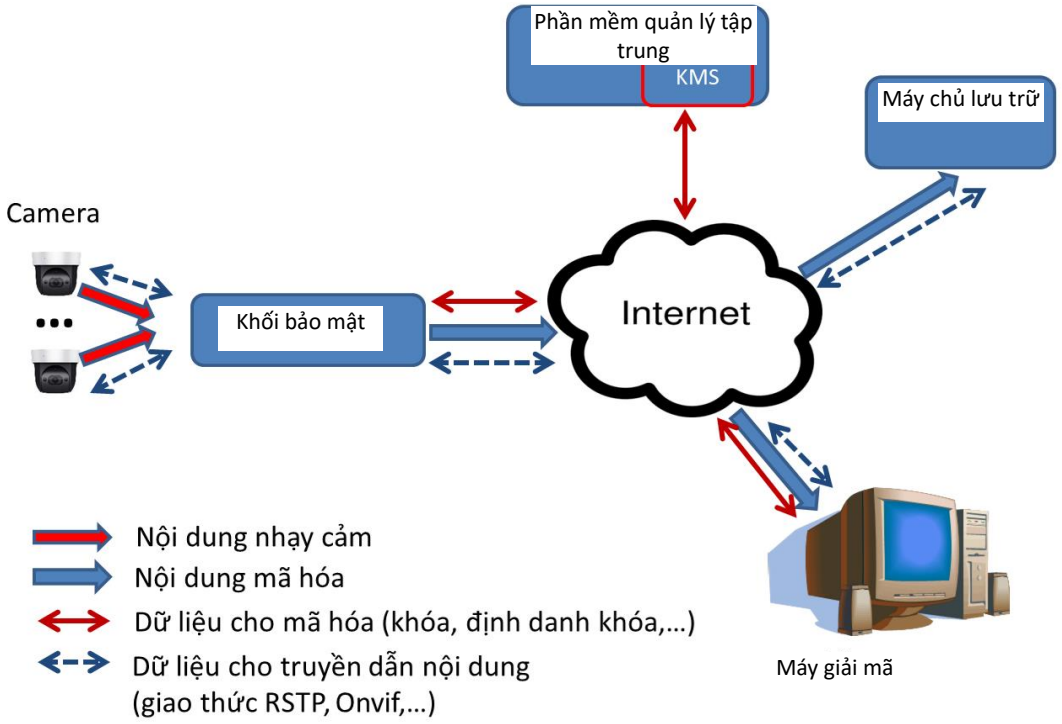


FIG.1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp và hệ thống bảo mật thông tin cho camera.

Tình trạng kỹ thuật của sáng chế

Hiện tại, các giải pháp mã hóa và bảo mật dữ liệu của camera theo giao thức internet (Internet Protocol camera, IP camera) tập trung vào ba hướng tiếp cận sử dụng các công nghệ (1) mạng riêng ảo (Virtual Private Network, VPN), (2) giao thức bảo mật và truyền siêu văn bản (Hyper Text Transfer Protocol Secure, HTTPS) và (3) giao thức bảo mật và vận chuyển thời gian thực (Secure Realtime Transport Protocol, SRTP).

Công nghệ VPN thường là khá phức tạp khi triển khai. Công nghệ này thiết lập mạng ảo nội bộ để bảo mật dựa trên cơ sở mạng chung internet. VPN thiết lập chế độ bảo mật cho tất cả các thông tin nói chung, do đó sẽ không hoạt động tốt đối với dữ liệu thời gian thực. Cấu hình của camera/máy chủ VPN phải thật sự tốt thì mới có thể bảo đảm hình ảnh được phát mượt mà thông qua VPN.

HTTPS là giải pháp được lựa chọn phổ biến, trong đó dòng dữ liệu theo giao thức vận chuyển thời gian thực (Realtime Transport Protocol, RTP) được đóng gói trong các bản tin theo giao thức truyền siêu văn bản (Hyper Text Transfer Protocol, HTTP) thông qua cơ chế HTTPS Tunneling (RTP Video Streaming over HTTPS) (xem tài liệu: Apple Computer Inc. RTSP over HTTP, Tunneling QuickTime RTSP and RTP over HTTP, *https://opensource.apple.com/source/QuickTimeStreamingServer/QuickTimeStreamingServer-412.42/Documentation/RTSP_Over_HTTP.pdf*). Đây là cơ chế bảo mật theo phiên giao dịch. Vì vậy, khi áp dụng quy trình truyền dẫn gồm ít nhất hai giai đoạn tách biệt theo thời gian là thu nhận thông tin từ camera và lưu trữ lại để xem về sau, thì cơ chế HTTPS không phát huy được tác dụng bởi vì cơ chế khóa theo phiên giao dịch không được thiết kế để trường tồn theo thời gian. Nội dung cần phải được giải mã và được mã hóa lại bằng một khóa khác, được cung cấp bởi các hệ thống DRM, để thuận tiện cho việc lưu trữ.

SRTP (RFC 3711) (xem tài liệu: Baugher, M., McGrew, D., Naslund, M., Carrara, E., and Norrman, K., *The Secure Real-time Transport Protocol (SRTP)*, RFC 3711, DOI

10.17487/RFC3711, March 2004, <https://www.rfc-editor.org/info/rfc3711>) là chuẩn mở rộng của giao thức vận chuyển thời gian thực (Realtime Transport Protocol, RTP), được bắt đầu nghiên cứu từ năm 2004 bởi các chuyên gia đến từ Cisco và Ericsson. SRTP hỗ trợ đồng thời mã hóa, xác thực, bảo đảm tính toàn vẹn dữ liệu, giúp giảm thiểu các nguy cơ như tấn công phát lại và tấn công từ chối dịch vụ (Denial of Service). Từ năm 2017, SRTP đã được tích hợp vào một số dòng IP camera cao cấp của Axis Communication AB (xem tài liệu: Genetec Inc. and Axis Communications Collaborate to Offer End-to-End Secure Real-time Transport Protocol (SRTP), *https://www.genetec.com/about-us/news/press-center/press-releases/genetec-inc-and-axis-communications-collaborate-to-offer-end-to-end-secure-real-time-transport-protocol-(srtp)-*). Giao thức này cũng trở thành tùy chọn trong sản phẩm của Hikvision, Dahua, nhưng được cài đặt với mục đích mã hóa dòng dữ liệu khi người dùng sử dụng dịch vụ điện toán đám mây (Cloud P2P) được cung cấp bởi nhà sản xuất (xem tài liệu: Hikvision, Network Camera Security Guide, *https://www.hikvision.com/ueditor/net/upload/2018-02-28/e8854c0d-0a40-40e8-9c79-2abffcea2e46.pdf*).

Trên thực tế, hầu hết các phiên bản tích hợp SRTP hiện tại đều dựa trên một khóa cố định cho nên có thể tiềm ẩn nhiều rủi ro dẫn đến mất an toàn thông tin, nếu khóa đó bị mất hoặc bị tin tặc khai thác, lợi dụng. Việc sử dụng một khóa duy nhất cũng gây khó khăn trong việc thu lại quyền truy cập của cá nhân đã được cấp quyền trước đó (xem tài liệu: Bảo mật dữ liệu đối với IP camera: Nguyên nhân và Giải pháp, *https://dascam.com.vn*). Ngoài ra, SRTP tương tự như HTTPS được phát triển theo nguyên lý mã hóa kênh truyền. Các giải pháp này không bảo đảm khả năng giữ bí mật nếu dữ liệu phải đi qua hệ thống đóng vai trò là trạm trung chuyển trung gian, như thiết bị đầu ghi hoặc hạ tầng dịch vụ điện toán đám mây. Nói cách khác, đơn vị cung cấp phần cứng cho hệ thống trung gian hoặc quản trị viên nếu cố ý vẫn có thể truy xuất trực tiếp hình ảnh được cung cấp từ IP camera.

Cần phải có phương pháp bảo mật được nhúng sâu vào nội dung cần bảo mật để bảo mật cho các thông tin đa phương tiện (hình ảnh, âm thanh), ví dụ bảo mật cho luồng viđeo phát ra từ các IP camera. Phương pháp như vậy bảo đảm tính hoàn toàn độc lập với

các giao thức truyền dẫn phổ biến hiện nay như TS, RTP, MP4. Nội dung đa phương tiện, sau khi được truyền dẫn qua các môi trường phức hợp, điển hình như từ luồng truyền trực tuyến chuyển sang ghi nhận để xem lại về sau, và được truyền dẫn tiếp trên mạng internet, sẽ không cần phải được giải mã và được mã hóa lại để cho phù hợp hơn với giao thức mới ở các vị trí chuyển tiếp giữa các giao thức truyền khác nhau. Việc loại bỏ quy trình giải mã và mã hóa lại lần nữa không những làm cho việc truyền dẫn thông tin được mạch lạc và nhanh chóng hơn mà còn nâng cao tính bảo mật trong toàn bộ quá trình truyền tải thông tin bảo mật. Trong suốt quá trình truyền tải thông tin như vậy sẽ không có bất cứ thời điểm nào mà nội dung bảo mật có thể được tiếp cận ở dạng thô không mã hóa.

Bản chất kỹ thuật của sáng chế

Để tăng cường tính bảo mật cho hệ thống camera, sáng chế đề xuất giải pháp xây dựng một hệ thống bao gồm phần cứng và phần mềm phân tán để bảo đảm việc mã hóa, phân quyền và giải mã tín hiệu hình ảnh thu được từ các camera một cách hiệu quả và an toàn.

Sáng chế đề xuất giải pháp mã hóa được nhúng sâu vào nội dung cần mã hóa. Nhờ đó, khi tín hiệu hình ảnh của camera được truyền phát qua nhiều giao thức truyền dẫn khác nhau, tín hiệu hình ảnh được bảo mật tuyệt đối, không cần phải giải mã và mã hóa lại để cho phù hợp với giao thức truyền tải mới.

Theo khía cạnh thứ nhất của sáng chế, sáng chế đề xuất phương pháp bảo mật thông tin cho camera bao gồm các bước:

(a) kết nối khối chức năng bảo mật với ít nhất một camera,

(b) tách ra ít nhất một luồng dữ liệu đa phương tiện từ camera, trong đó luồng dữ liệu đa phương tiện này được đóng gói ít nhất hai lần liên tiếp, lần đóng gói thứ nhất nén dữ liệu phù hợp với chuẩn nén để tạo ra các gói nén và lần đóng gói thứ hai tạo ra gói truyền dẫn theo định dạng của giao thức truyền dẫn,

(c) tách các gói nén ra khỏi gói truyền dẫn và mã hóa các gói nén bằng ít nhất một khoá mã hoá,

(d) tạo ra ít nhất một gói nén mới, được gọi là gói nén định danh mã hóa, theo chuẩn nén của camera, dùng để chứa ít nhất là thông tin định danh khóa của khóa mã hóa ở

bước (c),

(e) đóng gói gói nén định danh mã hóa được tạo ra ở bước (d) và các gói nén được mã hóa ở bước (c) vào gói truyền dẫn ở bước (b) theo đúng thứ tự và truyền dẫn gói này vào mạng internet.

Theo khía cạnh thứ hai của sáng chế, sáng chế đề xuất hệ thống bảo mật thông tin cho camera bao gồm:

ít nhất một camera được tạo cấu hình để thu thông tin đa phương tiện, và

thiết bị vật lý có một hoặc nhiều mạch vi xử lý và bộ nhớ trong, được kết nối với ít nhất một camera, thiết bị vật lý này có khối chức năng bảo mật được tạo cấu hình để:

tách ra ít nhất một luồng dữ liệu đa phương tiện từ camera, trong đó luồng dữ liệu đa phương tiện này được đóng gói ít nhất hai lần liên tiếp, lần đóng gói thứ nhất nén dữ liệu phù hợp với chuẩn nén để tạo ra các gói nén và lần đóng gói thứ hai tạo ra gói truyền dẫn theo định dạng của giao thức truyền dẫn,

tách các gói nén ra khỏi gói truyền dẫn và mã hóa các gói nén bằng ít nhất một khoá mã hoá,

tạo ra ít nhất một gói nén mới, được gọi là gói nén định danh mã hóa, theo chuẩn nén của camera, dùng để chứa ít nhất là thông tin định danh khóa của khóa mã hóa,

đóng gói gói nén định danh mã hóa được tạo ra và các gói nén được mã hóa vào gói truyền dẫn theo đúng thứ tự và truyền dẫn gói này vào mạng internet.

Theo khía cạnh thứ ba của sáng chế, sáng chế đề xuất vật ghi đọc được bằng máy tính trên đó lưu trữ các câu lệnh để thực hiện phương pháp theo khía cạnh thứ nhất của sáng chế.

Theo đó, sáng chế đề xuất một giải pháp tổng thể tăng cường tính năng bảo mật cho hệ thống camera an ninh. Giải pháp này dựa trên cơ chế kết nối camera cần bảo mật với một khối chức năng bảo mật được nhúng vào trong thiết bị phần cứng chuyên dụng. Khối chức năng bảo mật này sẽ mã hóa các thông tin hình ảnh phát ra từ camera. Ngoài ra, khối chức năng bảo mật này sẽ chặn tất cả các cuộc trao đổi dữ liệu khác phát sinh do tin tặc tấn công camera hoặc do chính camera, được sản xuất bởi bên thứ ba không đáng tin

cậy, xuất ra thông tin một cách bất hợp pháp qua các "cửa hậu" thông tin. Phương pháp mã hóa của khối chức năng bảo mật này tác động sâu vào cú pháp nén của nội dung cần bảo mật. Vì vậy, khi giải mã nội dung mã hoá, không nhất thiết phải dùng chung cú pháp truyền tải giống như khi mã hóa. Ưu điểm này giúp loại bỏ quy trình giải mã và mã hóa lại để cho phù hợp với giao thức truyền tải mới mỗi khi có sự thay đổi giao thức truyền tải đối với nội dung cần bảo mật.

Mô tả vắn tắt hình vẽ

Hình 1 là sơ đồ thể hiện hệ thống bảo mật thông tin cho camera.

Mô tả chi tiết sáng chế

1. Phương pháp mã hóa được nhúng sâu vào trong nội dung viđeo nén theo chuẩn H264/H265

Phương pháp truyền thống để bảo mật thông tin là mã hóa thông tin đó bằng một cấu trúc dữ liệu bí mật, được gọi là khóa. Thông tin đã mã hóa được gắn kết với thông tin định dạng khóa để chỉ báo khóa nào được dùng để mã hóa thông tin. Ở phía giải mã, đã biết thông tin định dạng khóa, và nếu có đủ quyền truy cập, thì có thể truy cập thông tin của khóa này, từ đó thông tin sẽ được giải mã thành công. Có thể thấy rằng thông tin định dạng khóa đóng vai trò quan trọng trong việc giải mã.

Khi truyền tải thông tin, thông tin được nén lại và lưu trữ trong những cấu trúc dữ liệu, được gọi là gói nén, tùy thuộc vào từng chuẩn nén. Ví dụ tín hiệu viđeo được nén theo chuẩn MPEG-2 sẽ tạo ra gói nén có định dạng dòng cơ bản dạng gói (Packetized Elementary Stream, PES). Còn tín hiệu viđeo được nén theo chuẩn H264/H265 sẽ tạo ra gói nén có định dạng tầng trừu tượng hoá mạng (Network Abstraction Layer, NAL).

Các gói nén này khi được truyền tải qua mạng thông tin sẽ được đóng gói một lần nữa vào cấu trúc dữ liệu, được gọi là gói truyền tải, phù hợp với giao thức truyền tải đã chọn. Ví dụ, khi truyền tải trên hệ thống theo chuẩn phát rộng dữ liệu viđeo kỹ thuật số (Digital Video Broadcasting, DVB), các gói nén PES hoặc NAL sẽ được đóng gói tiếp trong gói truyền tải có định dạng dòng truyền tải (Transport Stream, TS). Một dạng truyền tải khác thường dùng trong camera là RTP, trong đó cái gói nén PES, NAL sẽ được đưa vào gói có định dạng RTP. Một dạng truyền tải khác khá phổ biến hiện tại là

dạng lưu trữ MP4. Ở dạng này, cái gói nén sẽ được lưu trong những gói được gọi là đơn vị truy cập (Access Unit, AU). Đơn vị truy cập bao gồm một hoặc nhiều gói nén PES, NAL. Các đơn vị truy cập này được đưa vào cấu trúc dữ liệu mdat và được truy cập dễ dàng thông qua hệ thống xác đinh địa chỉ AU trong MP4.

Khi thực hiện quy trình mã hóa luồng thông tin, thông thường, gói truyền dẫn sẽ được mã hóa. Thông tin định danh khóa sẽ được lưu trữ riêng trong một cấu trúc dữ liệu đặc trưng cho phương pháp truyền dẫn. Ví dụ, trong phương pháp truyền dẫn DVB, các gói TS được mã hóa. Thông tin định danh khóa được truyền trong phần tiêu đề của gói truyền dẫn (2 bit thông tin chỉ báo khóa lẻ hoặc khóa chẵn). Trong phương pháp truyền dẫn RTP, cũng ở trong phần tiêu đề của gói truyền dẫn RTP, thông tin định danh khóa được thông báo để cho bộ phận giải mã có thể tìm đúng khóa để xử lý phần thân mã hóa của gói truyền dẫn RTP này.

Phương thức mã hóa hiện tại gắn chặt vào gói truyền tải dẫn đến việc khi nội dung cần bảo mật được truyền qua vài giao thức truyền tải khác nhau (ví dụ thu nhận luồng viđeo từ camera qua giao thức RTP để lưu trữ theo giao thức MP4, để sau này có thể xem trực tiếp hoặc tiếp tục chuyển phát qua giao thức DVB, ...), nhất thiết phải giải mã gói truyền dẫn, sau đó đóng gói các gói nén tạo thành kiểu gói truyền dẫn khác và mã hóa các gói truyền dẫn mới này. Quá trình nêu trên sẽ trở nên phức tạp, tốn nhiều tài nguyên và đặc biệt là tạo ra lỗ hổng cho tin tặc có thể truy cập vào các gói nén ở dạng không được bảo vệ trong quá trình chờ được chuyển sang gói truyền dẫn mới.

Sáng chế đề xuất phương pháp bảo mật thông tin cho camera bằng cách mã hóa sâu ở tầng các gói nén bao gồm các bước như sau:

(a) khối chức năng bảo mật được kết nối với ít nhất một camera,

(b) khối chức năng bảo mật tách ra ít nhất một luồng dữ liệu đa phương tiện từ camera, trong đó luồng dữ liệu đa phương tiện này được đóng gói ít nhất hai lần liên tiếp, lần đóng gói thứ nhất nén dữ liệu phù hợp với chuẩn nén để tạo ra các gói nén và lần đóng gói thứ hai tạo ra gói truyền dẫn theo định dạng của giao thức truyền dẫn,

(c) khối chức năng bảo mật tách các gói nén ra khỏi gói truyền dẫn và mã hóa các gói nén bằng ít nhất một khoá mã hoá,

(d) khối chức năng bảo mật tạo ra ít nhất một gói nén mới, được gọi là gói nén định danh mã hóa, theo chuẩn nén của camera, dùng để chứa ít nhất là thông tin định danh khóa của khóa mã hóa ở bước (c),

(e) khối chức năng bảo mật đóng gói gói nén định danh mã hóa được tạo ra ở bước (d) và các gói nén được mã hóa ở bước (c) vào gói truyền dẫn ở bước (b) theo đúng thứ tự và truyền dẫn gói này vào mạng internet.

Khối chức năng bảo mật trong các bước nêu trên là bộ phận lõi của sáng chế này. Cấu trúc của bộ phận lõi này sẽ được mô tả chi tiết dưới đây. Ở đây, các chức năng chính của khối chức năng bảo mật được mô tả chi tiết.

Lấy một ví dụ cụ thể, khối chức năng bảo mật được kết nối trực tiếp với camera cần bảo mật, giữ vai trò là cổng trung chuyển giữa camera và các nguồn thu trên mạng internet được kết nối với camera này. Vì vậy, khối chức năng bảo mật sẽ truy cập vào luồng truyền dẫn RTP chứa các gói nén NAL theo chuẩn nén H264, là một cấu hình phổ biến của các hệ thống camera hiện nay.

Đối với mỗi gói RTP thu được từ camera, khối chức năng bảo mật sẽ tách ra một hoặc nhiều gói nén NAL. Có hai trường hợp có thể xảy ra:

1. Đối với các gói nén NAL không chứa thông tin hình ảnh (không phải NAL dạng tầng mã hoá tín hiệu viđeo (Video Coding Layer, VCL), chỉ chứa thông tin hệ thống của chuẩn nén, khối chức năng bảo mật sẽ khôi phục gói truyền dẫn RTP như không có gì xảy ra và truyền tiếp gói thông tin đến các nguồn thu trên mạng internet.

2. Đối với các gói nén chứa ít nhất một NAL dạng VCL, khối chức năng bảo mật sẽ truy cập khóa và thông tin định dạng khóa liên quan. Sau đó, khối chức năng bảo mật sẽ dùng khóa này để mã hóa phần thân của gói nén NAL dạng VCL. Đồng thời khối chức năng bảo mật sinh ra một gói nén NAL mới dạng SEI đối với dữ liệu riêng không đăng ký. Phần thân của gói nén này có cú pháp như sau:

user_data_unregistered(payloadSize) {	C	Descriptor
uuid_iso_iec_11578	5	u(128)
for(i = 16; i < payloadSize; i++)		
user_data_payload_byte	5	b(8)
}		

Trường user_data_payload_byte dùng để truyền tải thông tin định danh khóa theo sáng chế.

Gói nén mới này sẽ được chèn vào ngay trước gói nén NAL dạng VCL được mã hóa bằng khóa liên quan đến thông tin định danh có trong gói NAL dạng SEI. Các gói nén NAL sau đó sẽ được đóng gói vào gói RTP tương ứng. Trong trường hợp giao thức truyền dẫn sử dụng cấu hình một gói RTP chứa một gói nén NAL, gói nén mới NAL dạng SEI sẽ được đóng gói trong một RTP riêng, còn gói nén NAL dạng VLC (mã hóa) sẽ được đóng gói trong gói RTP tiếp theo. Số thứ tự của các gói RTP phải được cập nhật tương ứng (tăng thêm 1 vì có thêm một gói RTP cho gói nén NAL dạng SEI).

Trong trường hợp thứ hai nêu trên, có thể chỉ có một phần của gói nén NAL dạng VCL ở trong gói RTP. Trong trường hợp như vậy, khối chức năng bảo mật sẽ đợi để truy cập tất cả các gói RTP liền kề nhằm khôi phục trọn vẹn gói NAL dạng VCL. Sau đó, quy trình mã hóa mới được thực hiện. Gói NAL dạng VCL sau khi được mã hóa lại sẽ được phân mảnh vào một vài gói RTP như trước khi mã hóa.

Một ví dụ khác về phương pháp truyền tải thông tin định danh khóa trong gói nén NAL là sử dụng cấu trúc NAL dạng PPS. Phần thân của cấu trúc này có cú pháp như được thể hiện trong bảng dưới đây:

pic_parameter_set_rbsp( ) {
pic_parameter_set_id
seq_parameter_set_id
entropy_coding_mode_flag
bottom_field_pic_order_in_frame_present_flag
num_slice_groups_minus1
if(num_slice_groups_minus1 > 0) {
slice_group_map_type
if(slice_group_map_type == 0)
for(iGroup = 0; iGroup <= num_slice_groups_minus1; iGroup++)
run_length_minus1[iGroup]
else if(slice_group_map_type == 2)
for(iGroup = 0; iGroup < num_slice_groups_minus1; iGroup++) {
top_left[iGroup]
bottom_right[iGroup]
}

```
    else if(  slice_group_map_type  ==  3  ||
              slice_group_map_type  ==  4  ||
              slice_group_map_type  ==  5 ) {
      slice_group_change_direction_flag
      slice_group_change_rate_minus1
    } else if( slice_group_map_type  ==  6 ) {
      pic_size_in_map_units_minus1
      for( i = 0; i <= pic_size_in_map_units_minus1; i++ )
        slice_group_id[ i ]
    }
  }
  num_ref_idx_l0_default_active_minus1
  num_ref_idx_l1_default_active_minus1
  weighted_pred_flag
  weighted_bipred_idc
  pic_init_qp_minus26    /* relative to 26 */
  pic_init_qs_minus26    /* relative to 26 */
  chroma_qp_index_offset
  deblocking_filter_control_present_flag
  constrained_intra_pred_flag
  redundant_pic_cnt_present_flag
  if( more_rbsp_data( ) ) {
    transform_8x8_mode_flag
    pic_scaling_matrix_present_flag
    if( pic_scaling_matrix_present_flag )
      for( i = 0; i < 6 +
           ( (chroma_format_idc  !=  3 ) ? 2 : 6 ) * transform_8x8_mode_flag;
           i++ ) {
        pic_scaling_list_present_flag[ i ]
        if( pic_scaling_list_present_flag[ i ] )
          if( i < 6 )
            scaling_list( ScalingList4x4[ i ], 16,
                          UseDefaultScalingMatrix4x4Flag[ i ] )
          else
            scaling_list( ScalingList8x8[ i − 6 ], 64,
                          UseDefaultScalingMatrix8x8Flag[ i − 6 ] )
      }
    second_chroma_qp_index_offset
  }
  rbsp_trailing_bits( )
```

}

NAL dạng PPS cung cấp thông tin cần thiết cho quy trình giải nén các gói NAL dạng VCL có cùng giá trị pic_parameter_set_id và seq_parameter_set_id. Hai trường thông tin này (các giá trị được ghép đuôi với nhau) có thể được sử dụng để truyền thông tin định danh khóa theo sáng chế. Trong trường hợp được sử dụng để lưu trữ thông tin định danh khóa, các trường này sẽ chứa các giá trị có độ lớn 64 bit (xem đơn đăng ký sáng chế quốc tế số PCT/EP2018/086402). Như vậy, bộ phận giải nén sẽ không lầm lẫn các trường này với các cấu trúc PPS thật sự (các trường này có giá trị nhỏ hơn 10).

Một ví dụ khác về phương pháp truyền tải thông tin định danh khóa là sử dụng đúng gói NAL dạng VCL. Ba dạng chính của gói NAL dạng VCL là Slice I, Slice P và Slice B đều có thể sử dụng được. Để giúp phân biệt giữa gói NAL dạng VCL chứa thông tin định danh khóa và gói NAL dạng VCL thật đã được mã hóa, sáng chế đề xuất cách sao chép nguyên bản phần tiêu đề của gói NAL dạng VLC thật cho gói NAL dạng VCL chứa thông tin định danh khóa. Như vậy, trong dòng chứa các gói nén NAL thỉnh thoảng sẽ có hai gói NAL dạng VCL có cùng vị trí trong một khung hình video (do sao chép nguyên bản phần tiêu đề, cụ thể là trường first_mb_in_slice sẽ giống nhau, xác định vị trí của đoạn hình ảnh trên hình ảnh). Sáng chế quy ước là gói NAL dạng VCL đầu tiên trong những trường hợp như vậy sẽ chứa thông tin định danh khóa trong phần thân của gói NAL dạng VCL. Các gói NAL dạng VCL này cần phải được loại bỏ sau khi giải mã các gói NAL dạng VCL khác để tránh gây nhiễu cho bộ phận giải nén khi xử lý các gói NAL ngay sau đó.

2. Hệ thống bảo mật thông tin cho camera sử dụng phương pháp mã hóa sâu

Để bảo mật tín hiệu hình ảnh của camera, sáng chế đề xuất hệ thống bảo mật thông tin cho camera bao gồm các bộ phận chức năng như sau:

- Thiết bị phần cứng đóng vai trò là khối chức năng bảo mật (Protector): là thiết bị phần cứng chuyên dụng, hỗ trợ việc mã hóa dòng RTP theo thời gian thực. Thiết bị phần cứng này sử dụng phương pháp bảo mật bảo mật thông tin cho camera theo sáng chế: thực hiện các tính năng của khối chức năng bảo mật như đã được mô tả trên đây cùng với cơ chế phân phối khóa/đảo khóa để bảo vệ quyền riêng tư của người dùng trong môi

trường internet theo sáng chế.

- Phần mềm quản lý tập trung (Central Monitor): cung cấp giao diện quản trị tập trung đối với quyền truy cập, thiết bị phần cứng đóng vai trò là khối chức năng bảo mật, máy chủ lưu trữ (Storage) và các máy giải mã (Viewer). Trong phần mềm quản lý tập trung này có tích hợp chức năng quản lý khóa để bảo đảm việc cung cấp khóa cho thiết bị mã hoá và giải mã theo cơ chế đảo khóa nhanh. Mỗi khi khối chức năng bảo mật cần sử dụng một khóa để mã hóa, thì chức năng quản lý khóa sẽ cung cấp khóa và thông tin định danh khóa cho khối chức năng bảo mật. Khi muốn xem nội dung đã mã hóa ở máy giải mã (Viewer), nếu người xem có đủ quyền, với thông tin định danh khóa được tách ra từ các gói nén định danh mã hóa, chức năng quản lý khóa sẽ cung cấp các khóa tương ứng để cho máy giải mã (Viewer) có thể giải mã nội dung.

- Máy chủ lưu trữ (Storage): là thiết bị có chức năng lưu trữ có thể được triển khai cả trên máy ảo lẫn trên nền tảng điện toán đám mây của bên thứ ba. Mục đích của máy chủ lưu trữ là để lưu trữ dữ liệu hình ảnh của các camera ở trạng thái bảo mật và xem lại về sau trên máy giải mã (Viewer).

- Các máy giải mã (Viewer): thực hiện chức năng giải mã để có thể xem được nội dung hình ảnh của các camera.

- Khối chức năng bảo mật được lắp đặt trong một thiết bị vật lý có một hoặc nhiều mạch vi xử lý và bộ nhớ trong để thực hiện các câu lệnh của khối chức năng bảo mật. Khối chức năng bảo mật là các thiết bị phần cứng đóng vai trò Protector / Viewer, đồng thời cũng là các thiết bị vật lý / ảo hóa được trang bị bộ nhớ và khả năng xử lý thông tin để thực hiện các câu lệnh mã hóa và giải mã của yêu cầu bảo hộ. Máy chủ, máy tính các nhân, các tính năng tính toán ảo hóa trên nền tảng đám mây, các thiết bị vi mạch có trang bị các bộ vi xử lý cùng bộ nhớ trong như Rasberry Pi, FPGA,... là các ví dụ cụ thể của các thiết bị có thể đóng vai trò Protector và Viewer này.

Camera sẽ được bảo mật nhờ thiết bị hỗ trợ kết nối sau camera. Khối chức năng bảo mật mã hóa nội dung cần bảo mật được nhúng sâu vào trong phần cú pháp nén của nội dung. Vì vậy, phương pháp mã hóa sẽ độc lập với các cú pháp truyền dẫn, thay đổi tùy theo giao thức truyền dẫn mà nội dung được bảo mật phải đi qua. Nhờ đó, việc giải mã và mã hóa lại để cho phù hợp với giao thức truyền dẫn sẽ không còn cần thiết nữa. Quy trình

bảo mật nội dung sẽ thực sự an toàn trong suốt quá trình truyền tải, không có bất cứ thời điểm nào mà nội dung được giải mã (để mã hóa lại), trở thành lỗ hổng cho tin tặc chiếm dụng.

Sáng chế cũng đề xuất vật ghi đọc được bằng máy tính chứa chương trình máy tính gồm các câu lệnh để thực hiện phương pháp bảo mật thông tin nêu trên. Ví dụ về vật ghi như vậy là ổ cứng, thẻ nhớ,…

Các thuật ngữ viết tắt

AU: Access Unit	Cấu trúc dữ liệu số (nhị phân) tương đương với một đơn vị dữ liệu có thể xử lý / hiển thị một cách độc lập / có ý nghĩa.
DVB: Digital Video Broadcasting	Giao thức truyền dẫn tín hiệu truyền hình dùng trong truyền hình số
FPGA: Field Programmable Gate Array	Thiết bị bao gồm nhiều cổng bán dẫn có thể lập trình lại được.
HTTPS: Hyper Text Transfer Protocol Secure	Giao thức bảo mật để truyền dẫn nội dung văn bản đa phương tiện
IP: Internet Protocol	Giao thức cơ bản của hệ thống mạng Internet
MP4	Định dạng tập tin chứa các video nén theo chuẩn của MPEG
MPEG, MPEG-2: Moving Picture Experts Group	Tổ chức quốc tế nghiên cứu và thiết lập ra các chuẩn nén cho video. MPEG-2 đã từng là chuẩn nén video dùng rộng rãi trong truyền hình số.
NAL: Network Abstraction Layer	Dữ liệu số ở tầng độc lập với phương thức truyền dẫn tín hiệu
PES: Packetized Elementary Stream	Dòng của các gói dữ liệu cơ bản (hình, tiếng, văn bản,…)
PPS: Picture Parameter Set	Tập hợp các tính chất của các khung ảnh trong video

RTP: Realtime Transport Protocol	Giao thức truyền dẫn thông tin theo thời gian thực
SEI: Supplemental Enhancement Information	Gói tin chứa các thông tin bổ trợ
SRTP: Secure Realtime Transport Protocol	Phiên bản bảo mật của RTP
TS: Transport Stream	Dòng các thông tin truyền dẫn theo chuẩn của MPEG-2
VLC: Video Coding Layer	Các thông tin số liên quan đến nội dung nén của video
VPN: Virtual Private Network	Không gian ảo của mạng nội bộ

Yêu cầu bảo hộ

1. Phương pháp bảo mật thông tin cho camera bao gồm các bước:

(a) kết nối khối chức năng bảo mật với ít nhất một camera,

(b) tách ra ít nhất một luồng dữ liệu đa phương tiện từ camera, trong đó luồng dữ liệu đa phương tiện này được đóng gói ít nhất hai lần liên tiếp:

- lần đóng gói thứ nhất nén dữ liệu phù hợp với chuẩn nén để tạo ra các gói nén có định dạng NAL (Network Abstraction Layer: dữ liệu số ở tầng độc lập với phương thức truyền dẫn tín hiệu) theo chuẩn nén H264/H265, và

- lần đóng gói thứ hai tạo ra gói truyền dẫn theo định dạng của giao thức truyền dẫn,

(c) tách các gói nén ra khỏi gói truyền dẫn và mã hóa các gói nén bằng ít nhất một khoá mã hoá,

(d) tạo ra ít nhất một gói nén mới, được gọi là gói nén định danh mã hóa, trong đó gói nén định danh mã hóa có định dạng NAL dạng PPS (Picture Parameter Set: tập hợp các tính chất của các khung ảnh trong video), dùng để chứa ít nhất là thông tin định danh khóa của khóa mã hóa ở bước (c),

(e) đóng gói gói nén định danh mã hóa được tạo ra ở bước (d) và các gói nén được mã hóa ở bước (c) vào gói truyền dẫn ở bước (b) theo đúng thứ tự và truyền dẫn gói này vào mạng internet.

2. Phương pháp theo điểm 1, trong đó gói nén định danh mã hóa có định dạng NAL dạng VLC (Video Coding Layer: các thông tin số liên quan đến nội dung nén của video)

3. Phương pháp theo điểm 1 hoặc 2, trong đó luồng dữ liệu đa phương tiện là luồng hình ảnh thu được từ camera.

4. Phương pháp theo điểm 1 hoặc 2, trong đó gói truyền dẫn được tạo ra trong lần đóng gói thứ hai có định dạng RTP (Realtime Transport Protocol: giao thức truyền dẫn thông tin theo thời gian thực).

5. Phương pháp theo điểm bất kỳ trong số các điểm 1, 3 hoặc 4, trong đó gói nén định danh

mã hóa có định dạng NAL dạng PPS, và trong đó thông tin định danh khóa được nhúng vào trong dạng liên kết của hai trường pic_parameter_set_id và seq_parameter_set_id.

6. Phương pháp theo điểm bất kỳ trong số các điểm 2, 3 hoặc 4, trong đó gói nén định danh mã hóa có định dạng NAL dạng VLC dùng để chứa thông tin của SliceI, phần thân của gói NAL dạng VLC này chứa mã định danh riêng để phân biệt với các gói NAL dạng VLC Slice I (Supplemental Enhancement Information: Gói tin chứa các thông tin bổ trợ) khác.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó khối chức năng bảo mật được lắp đặt trong một thiết bị vật lý có một hoặc nhiều mạch vi xử lý và bộ nhớ trong để thực hiện các câu lệnh của khối chức năng bảo mật.

8. Phương pháp theo điểm 1, trong đó gói nén định danh mã hóa có định dạng NAL dạng VLC.

9. Hệ thống bảo mật thông tin cho camera bao gồm:

ít nhất một camera được tạo cấu hình để thu thông tin đa phương tiện, và

thiết bị vật lý có một hoặc nhiều mạch vi xử lý và bộ nhớ trong, được kết nối với ít nhất một camera, thiết bị vật lý này có khối chức năng bảo mật được tạo cấu hình để:

tách ra ít nhất một luồng dữ liệu đa phương tiện từ camera, trong đó luồng dữ liệu đa phương tiện này được đóng gói ít nhất hai lần liên tiếp:

- lần đóng gói thứ nhất nén dữ liệu phù hợp để tạo ra các gói nén có định dạng NAL theo chuẩn nén H264/H265, và

- lần đóng gói thứ hai tạo ra gói truyền dẫn theo định dạng của giao thức truyền dẫn,

tách các gói nén ra khỏi gói truyền dẫn và mã hóa các gói nén bằng ít nhất một khoá mã hoá,

tạo ra ít nhất một gói nén mới, được gọi là gói nén định danh mã hóa, theo chuẩn nén của camera, trong đó gói nén định danh mã hóa có định dạng NAL dạng PPS, dùng để chứa ít nhất là thông tin định danh khóa của khóa mã hóa,

đóng gói gói nén định danh mã hóa được tạo ra và các gói nén được mã hóa vào gói truyền dẫn theo đúng thứ tự và truyền dẫn gói này vào mạng internet.

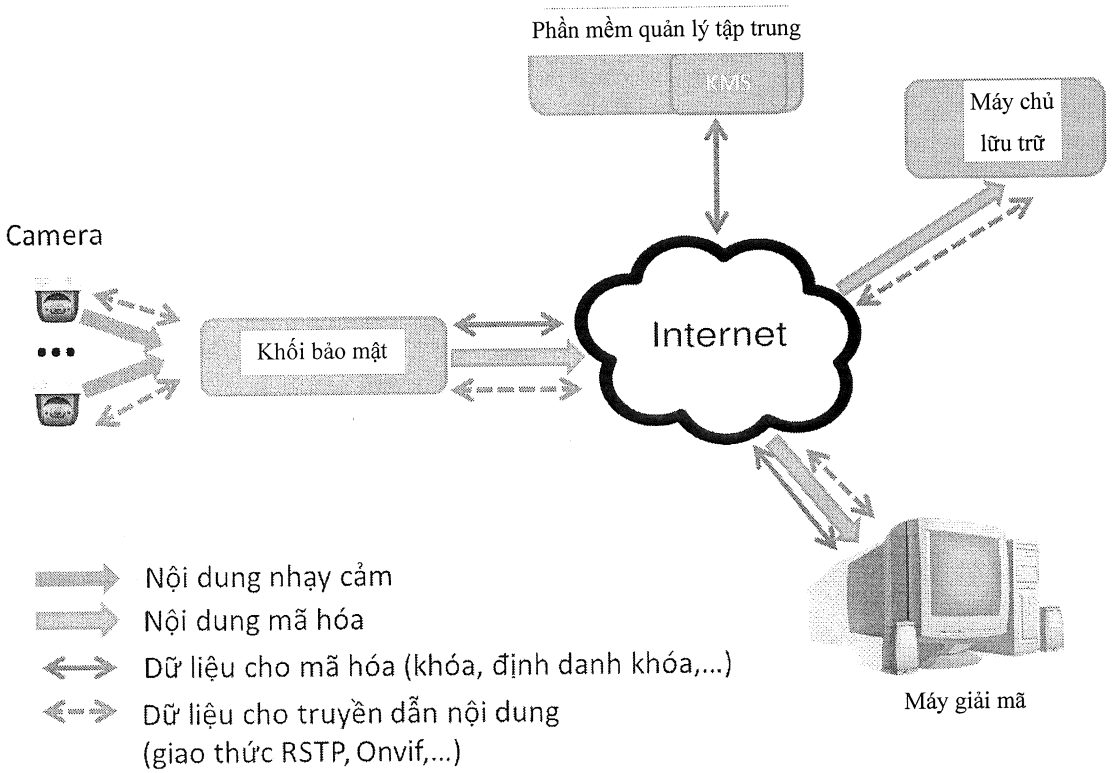
10. Hệ thống theo điểm 9, trong đó luồng dữ liệu đa phương tiện là luồng hình ảnh thu được từ camera.

11. Hệ thống theo điểm 10, trong đó gói truyền dẫn được tạo ra trong lần đóng gói thứ hai có định dạng RTP.

12. Hệ thống theo điểm 9, 10 hoặc 11, trong đó gói nén định danh mã hóa có định dạng NAL dạng PPS, và trong đó thông tin định danh khóa được nhúng vào trong dạng liên kết của hai trường pic_parameter_set_id và seq_parameter_set_id.

13. Hệ thống theo điểm 8, 10 hoặc 11, trong đó gói nén định danh mã hóa có định dạng NAL dạng VLC dùng để chứa thông tin của SliceI, phần thân của gói NAL dạng VLC này chứa mã định danh riêng để phân biệt với các gói NAL dạng VLC Slice I khác.

14. Vật ghi đọc được bằng máy tính trên đó lưu trữ các câu lệnh để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 8.



Hình 1: Hệ thống bảo mật thông tin cho camera