CHỮ KÝ SỐ VÀ ỨNG DỤNG TRÊN NỀN TẢNG VIDEO

Nguyễn Mậu Hân

Khoa Công nghệ Thông tin, Trường Đại học Khoa học, Đại học Huế

Email: nmhan@husc.edu.vn

Ngày nhận bài: 6/3/2024; ngày hoàn thành phản biện: 7/3/2024; ngày duyệt đăng: 7/3/2024

TÓM TẮT

Hiện nay, chữ ký số được ứng dụng rộng rãi trên nhiều lĩnh vực của xã hội, đặc biệt trên các nền tảng văn bản, hình ảnh, ... như khai thuế qua mạng, nộp thuế điện tử, khai báo hải quan điện tử, … Việc ứng dụng chữ ký số đem lại cho doanh nghiệp, tổ chức nhiều lợi ích như: tiết kiệm chi phí giấy tờ, thời gian luân chuyển trong hoạt động quản lý công văn, giấy tờ, thư điện tử; giúp đẩy nhanh các giao dịch qua mạng. Tuy nhiên, trên nền tảng video việc ứng dụng chữ ký số còn ít được bàn đến. Bài báo này đề xuất một phương pháp ứng dụng chữ ký số để kiểm duyệt các thước phim, video, ... trong khi vẫn đảm bảo độ an toàn và bảo mật thông tin.

Từ khóa: chữ ký số, video, phim

1. MỞ ĐẦU

Từ khi con người có nhu cầu trao đổi thông tin, thư từ cho nhau thì nhu cầu giữ bí mật và bảo vệ tính riêng tư của thông tin, thư từ được trao đổi đó cũng nảy sinh. Hình thức thông tin được trao đổi phổ biến và sớm nhất là dưới dạng các văn bản, để giữ bí mật của thông tin người ta đã sớm nghĩ đến cách che dấu nội dung các văn bản bằng cách biến dạng các văn bản đó để người ngoài đọc không hiểu được, đồng thời có cách khôi phục lại nguyên dạng ban đầu để người trong cuộc vẫn đọc hiểu được; theo cách gọi ngày nay thì dạng biến đổi của văn bản được gọi là mật mã của văn bản, cách lập mật mã cho một văn bản được gọi là phép lập mã, còn cách khôi phục lại nguyên dạng ban đầu của văn bản từ mật mã được gọi là phép giải mã [1].

Dịch vụ chứng thực chữ ký số là một loại hình dịch vụ chứng thực chữ ký điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cung cấp cho thuê bao để xác thực việc thuê bao là người đã ký số trên thông điệp dữ liệu. Giá trị pháp lý của chữ ký số được quy định theo Nghị định số 130/2018/NĐ-CP Quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số [3].

Ngày càng có nhiều doanh nghiệp và tổ chức sử dụng các dịch vụ này do những lợi ích mà nó mang lại. Đối với các đơn vị báo chí nói chung và đài truyền hình nói riêng, công tác kiểm duyệt nội dung video hết sức quan trọng, từ khâu sản xuất, trao đổi, kiểm duyệt, lưu trữ, phát sóng. Ở đây chúng ta đang bàn đến ứng dụng chữ ký số trong việc duyệt, chuyển tải các dữ liệu trên nền tảng video.

2. MỘT SỐ KHÁI NIỆM TOÁN HỌC LIÊN QUAN

2.1. Hàm băm

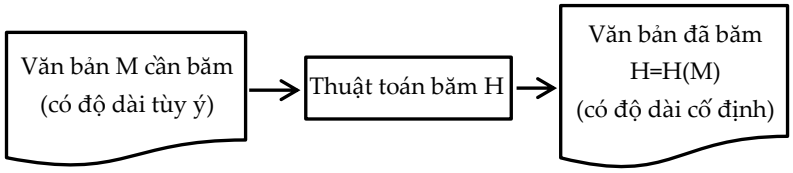
Hàm băm là hàm toán học dùng để chuyển đổi một văn bản có độ dài bất kì thành một chuỗi bit có độ dài cố định. Bất kỳ nỗ lực gian lận nào để thay đổi phần nào của văn bản sẽ bị phát hiện vì giá trị băm mới sẽ không phù hợp với thông tin cũ [5].

Hàm băm được định nghĩa bằng công thức: h = H(M), với M là văn bản cần băm, H là hàm băm và h là giá trị băm. Hàm băm H không có chức năng mã hóa vì khi giải mã không về được văn bản ban đầu. Giá trị băm h là một xâu bit còn được gọi là "đại diện thông điệp". Hàm băm H là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này "khó" có thể suy ngược lại được nội dung hay độ dài ban đầu của dữ liệu gốc. Hàm băm h không phải là một song ánh. Do đó với thông điệp x bất kỳ, tồn tại thông điệp x' ≠ x sao cho h(x) = h(x').

Các hàm băm dòng MD: MD2, MD4, MD5 được Rivest đưa ra có kết quả đầu ra với độ dài là 128 bit. Hàm băm MD4 đưa ra vào năm 1990. Một năm sau, phiên bản mạnh MD5 cũng được đưa ra. Năm 1993, hàm băm SHA phức tạp hơn nhiều, kết quả đầu ra có độ dài 160 bit, cũng được xây dựng dựa trên các phương pháp tương tự.

Với văn bản đầu vào M thì chúng ta chỉ thu được giá trị băm duy nhất h=H(M).

- Nếu dữ liệu trong văn bản M bị thay đổi hay bị xóa để thành văn bản M', thì giá trị băm H(M') ≠ H(M) cho dù chỉ là một sự thay đổi nhỏ. Trong ***Hình 1*** chỉ ra rằng chỉ cần thay đổi 1 bit dữ liệu của văn bản gốc M, thì giá trị băm H(M) của nó cũng thay đổi theo. Điều này có nghĩa là hai thông điệp khác nhau, thì giá trị băm của chúng sẽ khác nhau.



Hình 1. Sơ đồ mô tả thuật toán băm

- Nội dung của bản tin gốc "khó" có thể suy ra từ giá trị hàm băm của nó. Nghĩa là: Với thông điệp M thì "dễ" xác định được h=H(M), nhưng lại "khó" xác định ngược lại được M nếu chỉ biết giá trị băm h=H(M) (kể cả khi biết hàm băm H).

2.2. Mã hóa (Encryption) - Giải mã (Decryption)

Mã hóa là quá trình chuyển thông tin có thể đọc được (gọi là bản rõ) thành thông tin khó có thể đọc được theo cách thông thường (gọi là bản mã). Đó là một trong những kỹ thuật để bảo mật thông tin. Giải mã là quá trình chuyển thông tin ngược lại từ bản mã thành bản rõ. Thuật toán mã hóa hay giải mã là thủ tục để thực hiện mã hóa hay giải mã. Khóa mã hóa là một giá trị làm cho thuật toán mã hóa thực hiện theo cách riêng biệt và sinh ra bản rõ riêng. Thông thường khóa càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khóa được gọi là không gian khóa. Hệ mã hóa là tập các thuật toán, các khóa nhằm che giấu thông tin, cũng như làm rõ nó. Một hệ mã hóa có các tính năng sau [4]:

- Tính bảo mật: Bảo đảm bí mật cho các thông báo và dữ liệu bằng việc che giấu thông tin nhờ các kỹ thuật mã hóa.
- Tính toàn vẹn: Bảo đảm với các bên rằng bản tin không bị thay đổi trên đường truyền tin.
- Chống chối bỏ: Có thể xác nhận rằng tài liệu đã đến từ ai đó, ngay cả khi họ cố gắng từ chối nó.
- Tính xác thực: Nhận dạng nguồn gốc của một thông báo, đảm bảo rằng nó là đúng sự thực và kiểm tra định danh của người đang đăng nhập hệ thống. Đồng thời kiểm tra đặc điểm của họ trong trọng hợp ai đó cố gắng kết nối và giả danh là người sử dụng hợp pháp.

2.3. Các phương pháp mã hóa:

2.3.1. Mã hóa đối xứng:

Mã hóa khóa đối xứng là hệ mã hóa mà biết được khóa lập mã thì có thể "dễ" xác định được khóa giải mã và ngược lại. Đặc biệt, một số hệ mã hóa có khóa lập mã và khóa giải mã trùng nhau (ke = kd), như hệ mã hóa "dịch chuyển"hay DES. Hệ mã hóa khóa đối xứng còn gọi là hệ mã hóa khóa bí mật, hay khóa riêng, vì phải giữ bí mật cả 2 khóa. Trước khi dùng hệ mã hóa khóa đối xứng, người gửi và người nhận phải thỏa thuận thuật toán mã hóa và khóa chung (lập mã hay giải mã), khóa phải được bí mật.

2.3.2. Mã hóa công khai (public-key):

Dùng để gửi dữ liệu một cách an toàn qua các mạng không an toàn như Internet. Mỗi người dùng đều có hai khoá, một khoá công khai, một khoá riêng. Khoá công khai được giữ trong một thư mục. Ai cũng có thể truy cập khoá này để mã hoá một thông điệp trước khi gửi tới người có khoá riêng tương ứng. Còn khoá riêng thì chỉ người nhận mới có thể truy cập được và dùng nó để giải mã thông điệp. Hệ mật mã công khai RSA được đưa ra năm 1977 là công trình nghiên cứu của ba đồng tác giả Ronald Linn Revest,

Adi Shamir, Leonard Aldeman. Hệ mật mã được xây dựng dựa trên tính khó giải của bài toán phân tích một số thành thừa số nguyên tố hay còn gọi là bài toán RSA [6].

2.4. Chữ ký số

2.4.1. Giới thiệu về chữ kí số

Chữ ký nói chung là bằng chứng thể hiện người ký có chủ định khi ký vào một văn bản, làm cho người nhận văn bản biết rằng ai là người đã ký văn bản đó. Về mặt nguyên tắc chữ ký không thể sử dụng lại được, không thể sao chép sang văn bản khác, văn bản đã ký không thể thay đổi, không thể giả mạo và cũng không thể chối bỏ khi đã ký. Chữ ký có nhiều ưu điểm như dễ kiểm tra, không sao chép được, chữ ký của một người là giống nhau trên nhiều tài liệu, nhưng chỉ có giá trị trên một tài liệu cụ thể [2].

Chữ ký số cũng có các tính chất của chữ ký, được tạo ra bằng cách biến đổi dữ liệu sử dụng hệ mã hóa khóa công khai, người có dữ liệu ban đầu và khóa công khai của người ký thì có thể xác thực được chữ ký số vừa ký. Theo đó, mỗi người dùng sẽ sở hữu một cặp khóa gồm khóa bí mật và khóa công khai. Khóa bí mật được lưu trữ bí mật và sử dụng để ký kết các giao dịch. Các giao dịch đã ký dùng chữ ký số được phát đi trên toàn bộ mạng. Bản chất của chữ ký số là một chuỗi số gắn kết với một văn bản với một (hoặc nhiều) thực thể nguồn nào đó. Nếu văn bản thay đổi thì chữ ký số phải thay đổi theo, do đó chữ ký số đảm bảo tính toàn vẹn của văn bản được ký. Chữ ký số không thể sử dụng lại và cũng không làm giả được. Chữ ký số đảm bảo tính xác thực vì chỉ có người ký mới xác thực được chữ ký. Chữ ký số cũng xác thực đảm bảo tính không thể chối bỏ của chữ ký. Người ký không thể chối bỏ rằng không ký vào tài liệu. Chữ ký số liên quan đến hai giai đoạn: Giai đoạn tạo chữ ký số và giai đoạn xác minh.

2.4.2. Cấu tạo của chữ ký số

Sơ đồ chữ ký số là một bộ năm thành phần gồm (P, A, K, S, V), Trong đó:

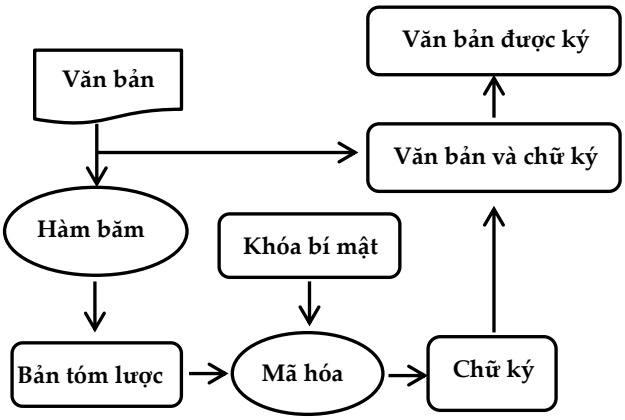
- P là tập hợp hữu hạn các văn bản.
- A là tập hợp hữu hạn các chữ ký có thể được sử dụng.
- Không gian khóa K là tập hợp hữu hạn các khóa có thể sử dụng. Trong đó không gian khóa K′ để tạo nên chữ ký, không gian khóa K′′ kiểm tra chữ ký. Thuật toán tạo nên khóa: K → K′ x K′′ (K′: không gian khóa bí mật, K′′: không gian khóa công khai)
- S là tập các thuật toán tạo chữ ký $\text{sig}_{K'} \in S$, $\text{sig}_{K'}: P \to A$
- V là tập các thuật toán kiểm tra chữ ký $\text{ver}_{K''} \in V$, $\text{ver}_{K''}: P \times A \to \{\text{đúng}, \text{sai}\}$, thỏa mãn điều kiện sau đây đối với bất kỳ bản tin x ∈ P và chữ ký y ∈ A.

$$\forall x \in P, \forall y \in A: \quad ver_{K''}(x, y) = \begin{cases} \text{Đúng}, nếu\ y = sig_{K'}(x) \\ Sai, nếu\ y \neq\ sig_{K'}(x) \end{cases} \quad (1)$$

Bởi vì văn bản cần ký thường có chiều dài khá dài. Một biện pháp để ký là chia văn bản ra các đoạn nhỏ và sau đó ký lên từng đoạn và ghép lại.

2.4.3. Các giai đoạn tạo và kiểm tra chữ ký số

a. Giai đoạn tạo chữ ký số



Hình 2. Giai đoạn tạo chữ ký số

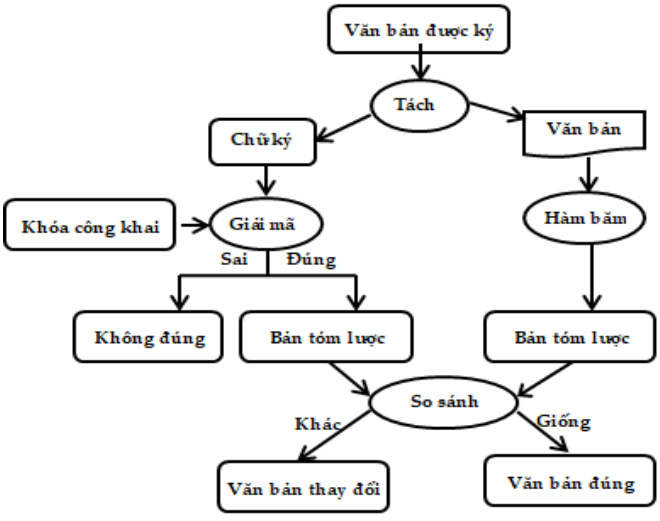
Dùng thuật toán băm cho văn bản cần truyền đi, kết quả được một bản tóm lược, sử dụng khóa bí mật của điểm gửi để mã hóa bản tóm lược. Bản tóm lược đảm bảo 2 tính chất sau:

(1) Tính duy nhất: mỗi bản khác nhau thì sẽ có một bit khác nhau, không trùng lặp và có độ dài không đổi;

(2) Tính một chiều: Từ bản tóm lược này không suy ngược lại được nội dung văn bản. Bản tóm lược này được mã hóa bằng khóa bí mật của điểm gửi và được kết hợp với văn bản, rồi gửi đến điểm nhận và bản tóm lược được mã hóa này chính là chữ ký số.

b. Giai đoạn kiểm tra chữ ký số

Điểm nhận sau khi nhận văn bản được ký số, quá trình tiến hành kiểm tra được thực hiện như sau (***Hình 3***):



Hình 3. *Giai đoạn kiểm tra chữ ký số*

Bước 1: Tiến hành tách văn bản và chữ ký số.

Bước 2: Lấy đoạn văn bản, đưa qua hàm băm thu được kết quả băm là bản tóm lược.

Bước 3: Giải mã chữ ký số (bản tóm lược được mã hóa bằng khóa bí mật), sử dụng khóa công khai của điểm gửi để giải mã nhận được bản tóm lược.

Bước 4: Tiến hành so sánh bản tóm lược vừa giải mã với bản tóm lược nhận được trong bước 2, nếu 2 bản này giống nhau và khóa công khai chắc chắn là do điểm gửi gửi thì kết luận: (1) văn bản nhận được là chính xác; (2) văn bản nhận được là do chính điểm

gửi gửi đi vì chỉ duy nhất điểm nhận được xác thực mới có khóa bí mật phù hợp với khóa công khai đã sử dụng để giải mã. Trường hợp 2 bản tóm lược khác nhau thì kết luận văn bản bị sửa đổi.

Chữ ký số được tạo ra bằng sự biến đổi một văn bản sử dụng hệ mã hóa khóa công khai, theo đó điểm nhận có văn bản ban đầu và khóa công khai của điểm gửi có thể xác định được.

3. ỨNG DỤNG CHỮ KÝ SỐ TRONG HOẠT ĐỘNG KIỂM DUYỆT VIDEO

3.1. Giới thiệu

Hiện nay công tác kiểm duyệt nội dung file video được thực hiện chủ yếu qua chức năng kiểm duyệt của hệ thống quản lý thư viện (MAM - Media Asset System) hoặc kiểm duyệt trực tiếp trên file video cần kiểm duyệt. Các hệ thống MAM chủ yếu sử dụng các sản phẩm của nước ngoài, đôi khi không phù hợp với quy trình thực tế trong nước và giá thành khá đắt. Đối với cách kiểm duyệt trực tiếp file video: thường được thực hiện bằng cách trao đổi file video sử dụng các thiết bị lưu trữ di động hoặc gửi qua mạng. Việc xác nhận sau kiểm duyệt chủ yếu dựa trên thông tin metadata của file, đôi khi xảy ra tình trạng nhầm lẫn nội dung file, nhầm lẫn các phiên bản của cùng file, ... Để khắc phục tình trạng này cần gắng trách nhiệm của từng người, ở từng khâu kiểm duyệt, với từng file bằng cách ký số lên nội dung từng file video. Việc này được thực hiện tương tự việc ký số vào văn bản đang được sử dụng rộng rãi hiện nay. Mỗi khi có bất kỳ sự thay đổi nào của file video: có thể do đường truyền, lỗi file, cố ý thay đổi,…hệ thống sẽ xác minh lại chữ ký của từng người để xác thực file video là chính xác hay không. Thông tin chữ ký số được lưu kèm với file video nhưng không làm thay đổi file video ban đầu.

3.2. Các định dạng file video thông dụng

- *Định dạng AVI:* Định dạng AVI (Audio Video Interle) do Microsoft giới thiệu năm 1992 như một chuẩn video dành cho Windows. File AVI có thể chứa cả dữ liệu hình ảnh và âm thanh trong một tệp, cho phép phát lại đồng bộ hình ảnh và âm thanh.

- *Định dạng MP4:* MP4 (MPEG-4 Part 14) là định dạng video phổ biến và được hỗ trợ rộng rãi trên nhiều thiết bị và nền tảng. MP4 sử dụng các thuật toán nén dữ liệu như MPEG-4 AVC (Advanced Video Coding) để giảm kích thước file video mà vẫn giữ được chất lượng hình ảnh tốt. Nó cân bằng giữa chất lượng và kích thước file, cho phép truyền tải và lưu trữ video một cách hiệu quả.

- *Định dạng MXF:* Định dạng MXF (Material Exchange Format) là một định dạng tập tin video chuyên dụng được sử dụng trong các lĩnh vực sản xuất và trao đổi nội dung chuyên nghiệp, như truyền hình, phim ảnh và công nghệ thông tin.

- *Định dạng MOV:* Định dạng MOV (QuickTime Movie) là một định dạng tập tin video phát triển bởi Apple và thường được sử dụng trên các thiết bị Apple như iPhone, iPad và Mac. MOV có khả năng hỗ trợ nhiều codec khác nhau cho việc nén video và âm thanh. Một số codec phổ biến được sử dụng trong MOV bao gồm H.264, HEVC (H.265), MPEG-4, AAC và MP3.

- *Định dạng WEBM:* Định dạng video WEBM là một định dạng tập tin video được phát triển bởi Google và thuộc về dự án mã nguồn mở WebM. WEBM sử dụng codec nén dữ liệu VP9 hoặc AV1 để giảm kích thước file mà vẫn giữ được chất lượng hình ảnh tốt. WEBM được thiết kế để tương thích với các trình duyệt web phổ biến như Google Chrome, Mozilla Firefox và Opera. Định dạng này cung cấp âm thành hình ảnh chất lượng cao, kích thước file nhỏ và tính tương thích đa nền tảng, làm cho WEBM trở thành lựa chọn hữu ích trong việc làm việc với video trên Internet.

Kiểm duyệt video là một công việc phức tạp và tốn khá nhiều thời gian, công sức. Các hãng chuyên về video trên thế giới thường sử dụng kết hợp nhiều phương pháp khác nhau để thực hiện công việc này như:

- Sử dụng các công cụ tự động dựa trên máy học và trí tuệ nhân tạo.
- Kiểm duyệt cộng đồng.
- Phối hợp với các đối tác kiểm duyệt nội dung.
- Đưa ra các chính sách và hướng dẫn người dùng thực hiện.

Youtube sử dụng các thuật toán máy học và trí tuệ nhân tạo để tự động phát hiện và kiểm duyệt nội dung không phù hợp. Các thuật toán này được huấn luyện để nhận dạng và phân loại các yếu tố khác nhau như ngôn ngữ xúc phạm, hành vi bạo lực, nội dung người lớn, vi phạm bản quyền, ... sau đó đội ngũ kiểm duyệt sẽ xem xét và xử lý.

3.3. Triển khai chữ ký số trên file video

3.3.1. Mục đích, yêu cầu của việc bảo mật file video

Trong các hệ thống kiểm duyệt video nội bộ, bảo mật hệ thống là một yếu tố quan trọng để đảm bảo tính chính xác, đáng tin cậy của quá trình kiểm duyệt nội dung với những lý do sau đây:

a. Tránh việc can thiệp bất hợp pháp: Mỗi thành viên được cấp một tài khoản với quyền và nghĩa vụ nhất định trên hệ thống. Nếu hệ thống không bảo mật, kẻ xấu dễ dàng chiếm tài khoản và thực hiện các thao tác với ý đồ xấu, làm sai lệch quá trình kiểm duyệt.

b. Đảm bảo tính công bằng và chính xác: Bảo mật hệ thống kiểm duyệt giúp đảm bảo người kiểm duyệt chỉ có thể đưa ra các nhận xét về chương trình, không thay đổi nội dung file video gốc. Điều này giúp duy trì độ tin cậy của quá trình kiểm duyệt.

c. Đối phó với việc đưa các nội dung không phù hợp lên hệ thống: Một hệ thống kiểm duyệt có bảo mật có thể giúp ngăn chặn các nội dung không phù hợp, độc hại, vi phạm bản quyền xuất hiện trên hệ thống. Điều này làm tăng tính an toàn cho hệ thống.

d. Chống thoái thác trách nhiệm: Hệ thống với độ bảo mật cao giúp người dùng chịu trách nhiệm với các hành động của mình, chống thoái thác trách nhiệm, gây các hậu quả pháp lý không mong muốn.

3.3.2. Cách tạo chữ ký số trên file video

File video cần kiểm duyệt sẽ được gửi lên video server, đồng thời người gửi cũng ký số lên file video này để xác nhận mình là người gửi file này. Dữ liệu trong file video được xác định qua hàm băm, thu được giá trị băm. Người dùng sử dụng mã PIN để mở khóa bí mật của mình, và dùng khóa này thực hiện ký số lên giá trị băm thu được chuỗi giá trị ký số. Chuỗi này được lưu trên database cùng với các thông tin khác về tài khoản người dùng, … Phương pháp tạo chữ ký số lên file video được sử dụng cho cả người gửi video và người kiểm duyệt video.

3.3.3. Cách xác thực chữ ký số

Khi người dùng mở file video đã được ký số và lưu trên video server, hệ thống sẽ thực hiện tính giá trị băm của file này. Đồng thời sử dụng khóa công khai của người đã ký số để giải mã chuỗi giá trị ký số đã lưu trên database. So sánh giá trị này với giá trị băm đã tính được, nếu trùng khớp thì chữ ký số là hợp lệ và ngược lại.

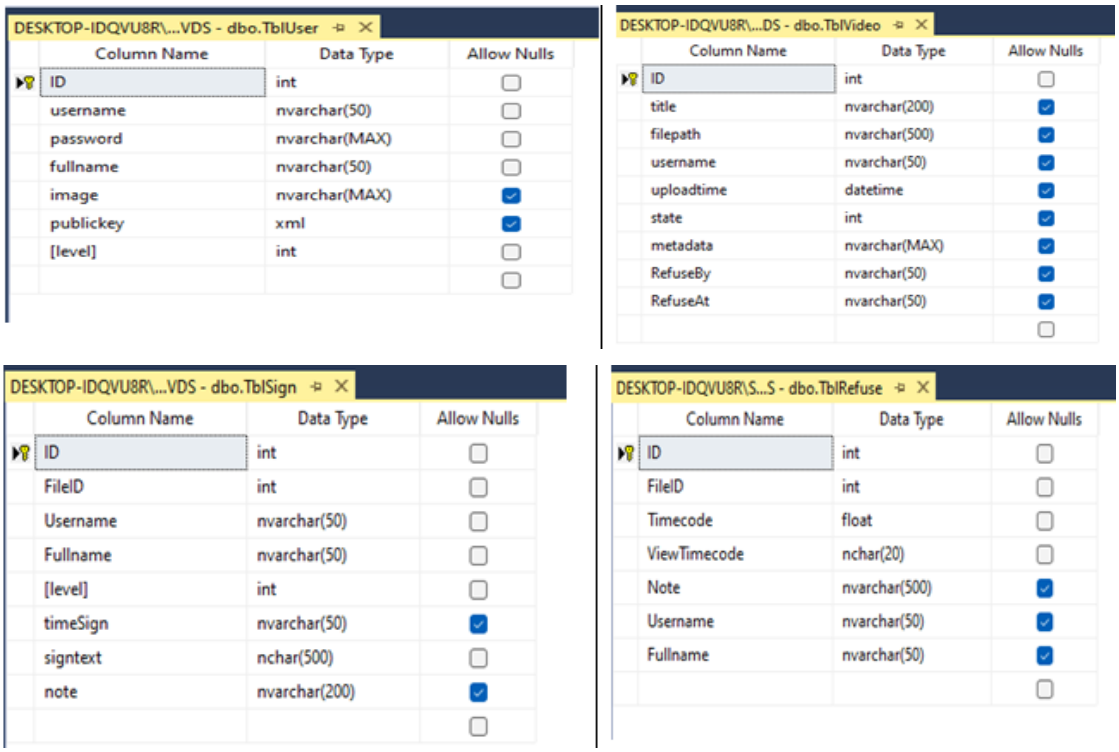
3.3.4. Hiển thị chữ ký số trên file video

Khi đã xác minh chữ ký số là hợp lệ, hệ thống tự tạo thêm 1 lớp video để hiển thị thông tin chữ ký số. Thông tin này sẽ hiển thị đè lên video gốc nhưng có độ trong suốt nhất định để không che nội dung video gốc. Người dùng có thể lưu lại thành video mới có kèm chữ kí số để sử dụng cho các mục đích khác nhau.

3.4. Cài đặt và thực nghiệm

3.4.1. Thiết kế cơ sở dữ liệu trên SQL Server

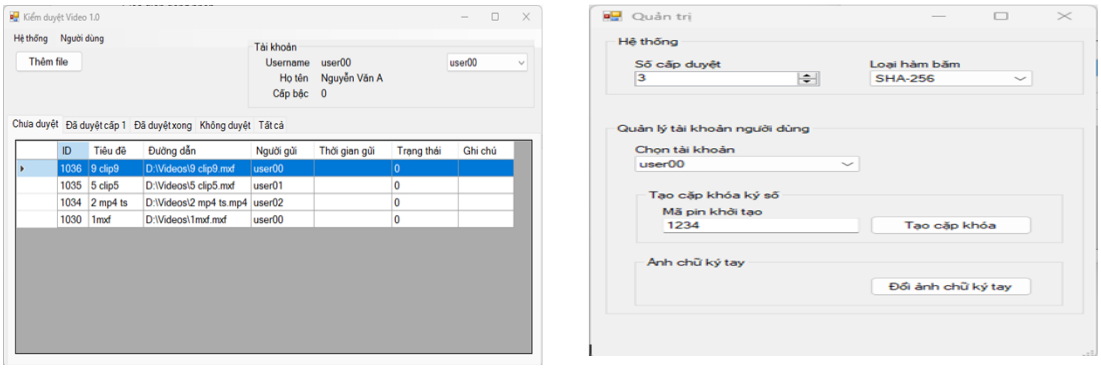
Ảnh chữ ký tay và khóa công khai của người dùng được lưu cùng với thông tin tài khoản trong bảng TblUser. Thông tin metadata, trạng thái duyệt được lưu trong bảng TblVideo. Thông tin chữ ký số được lưu trong bảng TblSign. Thông tin nhận xét/từ chối được lưu trong bảng TblRefuse.



Hình 4. Chi tiết cấu trúc các bảng dữ liệu được sử dụng trong chữ ký số

3.4.2. *Quản trị người dùng*

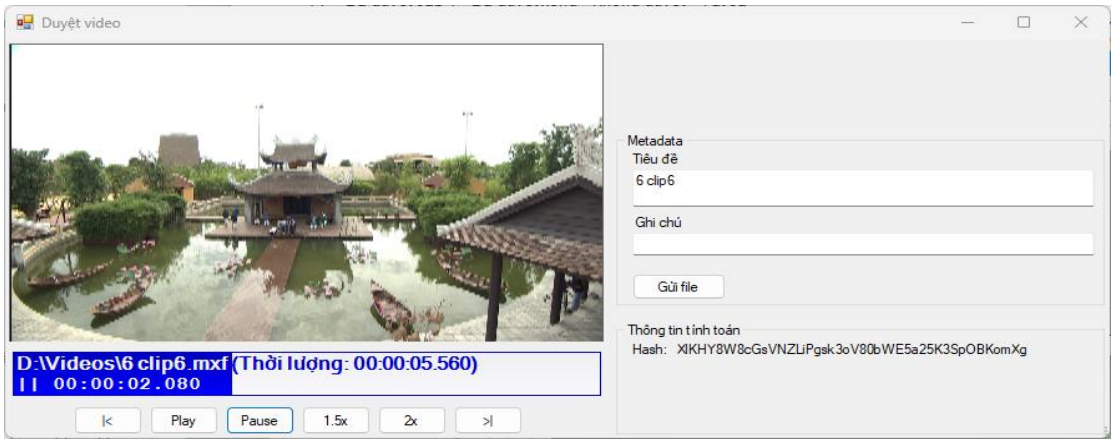
Mật khẩu người dùng được mã hóa AES và lưu vào cơ sở dữ liệu SQL. Người dùng cần nhập mật khẩu mỗi khi sử dụng ứng dụng.



Hình 5. Giao diện quản trị người dùng và giao diện cài đặt quản trị

3.4.3. Xem lại file video:

Hệ thống cho phép cập nhật thông tin metadata của video, ở đây minh họa 2 giá trị thường dùng là Tiêu đề và Ghi chú. Các phím chức năng phục vụ việc xem nội dung video như phát, tạm dừng, về đầu, về cuối, thay đổi tốc độ phát, hiển thị timecode.

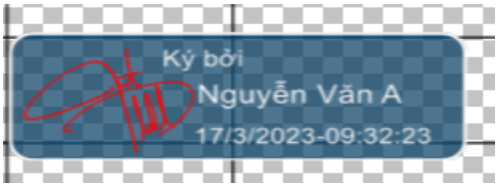


Hình 6. Giao diện gửi file

Sau khi xem lại nội dung video đã chính xác, người gửi nhấn nút Gửi file. Ứng dụng yêu cầu xác thực mã pin nhằm bảo đảm tính bảo mật. Nếu mã PIN hợp lệ hệ thống sẽ tiến hành ký số, cập nhật dữ liệu lên database, sao chép file video vào video server.

3.4.4. Thiết kế chữ ký số

Chữ ký được cài đặt dạng XML để có thể thay đổi thiết kế, thay đổi các thông tin cần hiển thị, vị trí hiển thị theo nhu cầu. Chữ ký số sẽ được hiển thị chữ ký tay của người ký; hiển thị thông tin người ký; hiển thị thời điểm ký. Nội dung hiển thị không che khuất nội dung video gốc.



Hình 7. Thiết kế chữ ký mẫu

4. KẾT LUẬN

Trong bài báo này chúng tôi đã áp dụng lý thuyết mật mã, hệ mã hóa công khai và chữ kí số trong việc kiểm duyệt video để phục vụ công tác duyệt phim, video. Việc kí lên video và xác thực thông tin đã đáp ứng tốt các yêu cầu về bảo mật, chống lại các hình thức giả mạo và tấn công hiện nay.

TÀI LIỆU THAM KHẢO

[1] Phan Đình Diệu (2002). Lý thuyết mật mã và an toàn thông tin, Đại học Quốc gia Hà Nội.

[2] Phạm Thị Tâm, Đoàn Văn Ban (2017). Một số thuật toán chữ ký số và ứng dụng trong bảo mật dữ liệu điện tử, NXB Đại học Thái Nguyên.

[3] Nghị định số 130/2018/NĐ-CP của Chính phủ (2018): Quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.

[4] Secure Hash Standard (2018), Federal Information Processing Standards Publication (FIPS PUBS).

[5] Bart Van Rompay (2014). Analysis and Design of Cryptographic Hash Functions, MAC Algorithms and Block Ciphers, Juni, tr. 27-28

[6] Burt Kaliski (2021), RSA Laboratories, The Mathematics of the RSA Public-Key Cryptosystem

DIGITAL SIGNATURES AND APPLICATE ON VIDEO-BASED

Nguyen Mau Han

Faculty of Information Technology, Hue University of Sciences, Hue University

Email: nmhan@husc.edu.vn

ABSTRACT

Currently, digital signatures are widely applied in many areas of society, especially on text and image platforms, etc. such as online tax declaration, electronic tax payment, electronic customs declaration, electronic social insurance, etc. The application of digital signatures brings many benefits to businesses and organizations such as: Saving paper costs, turnover time in managing official dispatches, documents, and emails and helping speed up online transactions. However, on video platforms, the application of digital signatures is rarely discussed. This article proposes a method of applying digital signatures to censor movies, videos, etc. while still ensuring safety and information security.

Keywords: digital signature, video, movie.

Nguyễn Mậu Hân sinh năm 1957 tại Thừa thiên Huế. Năm 1981, ông tốt nghiệp cử nhân toán tại Trường Đại học Tổng hợp Huế. Năm 1998, ông nhận bằng thạc sĩ Khoa học máy tính tại Trường Đại học Bách khoa Hà Nội. Năm 2003, ông nhận bằng tiến sĩ Khoa học Máy tính tại Viện Công nghệ Thông tin Hà Nội. Hiện ông là Phó Giáo sư, Giảng viên cao cấp tại Trường Đại học Khoa học, Đại học Huế.

Lĩnh vực nghiên cứu: Công nghệ phần mềm, Cơ sở dữ liệu, Xử lý song song và phân tán.