TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên luận án: **Nghiên cứu phương pháp bảo mật thông tin giấu trong ảnh số**

Chuyên ngành: **Kỹ thuật viễn thông**

Mã số: **9.52.02.08**

Họ và tên NCS: **Lê Hải Triều**

Người hướng dẫn khoa học: **GS.TSKH. Đỗ Trung Tá**

Cơ sở đào tạo: **Học viện Công nghệ Bưu chính Viễn thông**

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN

- Đóng góp thứ nhất: Đã đề xuất được thuật toán giấu tin mới sử dụng bộ mã 5 bít, với các ưu điểm sau đây. *Thứ nhất*, giảm tỷ lệ nhúng xuống khoảng 3,2% (≈1/31), đây là tỷ lệ cho phép chống lại các thuật toán tấn công thông kê cấp 1 và cấp 2. *Thứ hai là* thuật toán giấu tin trên có ưu điểm là đơn giản cho việc nhúng và trích chọn, ngoài ra lượng thông tin giấu được lớn nhưng các LSB thay đổi ít hơn. *Thứ ba* là tăng được khả năng giấu tin. *Thứ tư,* việc sử dụng từ mã 5 bít sẽ mã hết toàn bộ 26 ký tự Latinh. Kết quả đánh giá và so sánh thuật toán đề xuất mới và thuật toán cũ cho thấy lượng thông tin giấu được cao hơn 60% so với thuật toán cũ, tỷ số PSRN cao hơn tiêu chuẩn cho phép (>38dB) và cao hơn so với thuật toán cũ (ít nhất 64% cùng 1 lượng tin giấu), đồng thời tỷ lệ nhúng đạt dưới 2%.

- Đóng góp thứ hai: Ứng dụng thuật toán sinh bit giả ngẫu nhiên mới có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính, nhằm phục vụ trao đổi khóa bí mật cho việc giấu tin trong ảnh số. Ba ưu điểm trong thuật toán mới được thể hiện sau đây. *Thứ nhất,* chu kỳ R của dãy được kiểm soát nếu thực hiện đúng giả thiết của Định lý 2; *Thứ hai,* việc trao đổi khóa rất đơn giản, chỉ cần 4 tham số x_0,a,b,m. Tùy theo yêu cầu của ứng dụng để chọn m cho phù hợp. Đây là công thức truy hồi để tìm dãy $\{x_n\}$ với $n\geq 2$. *Thứ ba,* thuật toán này được sử dụng cho việc trao đổi khóa mật mã phục vụ đối với thuật toán 5 bít ở trên bằng hệ mật mã khóa công khai và ứng dụng trực tiếp cho nội dung trong chương 4 cũng như trong quốc phòng-an ninh.

- Đóng góp thứ ba: Từ các phương pháp đánh giá chất lượng giấu tin mật và sinh khóa giả ngẫu nhiên, đề xuất một số phương pháp đánh giá độ an toàn bảo mật. *Thứ nhất,* đánh giá chất lượng các dãy giả ngẫu nhiên được sinh từ hệ thống nào đó được coi là tốt nếu các thành phần của dãy đó là độc lập và có phân bố đều. Từ đó luận án giới thiệu thuật toán đánh giá an toàn đối với hệ thống sinh bít giả ngẫu nhiên tùy ý và thuật toán đánh giá an toàn đối với hệ thống dãy giả ngẫu nhiên chữ cái Latinh. *Thứ hai,* sử dụng phương pháp đánh giá độ an toàn hoàn hảo thông qua sai phân Kullback - Leibler giữa hàm mật độ xác xuất $D(P_s \,||P_c)$. Đã đề xuất được thuật toán đánh giá hàm D giải quyết theo hướng đơn giản và hiệu quả hơn với kết quả đánh giá sai phân $D(P_s \,||P_c) \leq 0{,}05$ với độ an toàn trên 98%.

- Đóng góp thứ tư: Trên cơ sở nghiên cứu và đánh giá so sánh hiệu năng lỗi của ảnh JPEG/JPEG2000 đã đánh dấu bảo mật bằng watermar. *Thứ nhất,* cung cấp mô hình phân tích và kết quả số mô tả hiệu năng lỗi cho mô hình đề xuất trong quá trình xử lý ảnh theo chuẩn JPEG/JPEG2000 và quá trình đánh dấu bảo mật watermark vào dữ liệu cảm biến tương ứng. *Thứ hai,* xác suất này phụ thuộc vào các tham số thay đổi như độ lớn watermark trung bình, xác suất cảnh báo sai, hệ số nén và kích thước ảnh cho đến cách chia khối cho từng ảnh. *Thứ ba,* bảo mật đối với ảnh số bằng đánh dấu watermark theo phương pháp DWT là lựa chọn tốt nhất cho cả vấn đề hiệu năng lỗi cũng như xác suất tìm thấy dấu watermark.

- Đóng góp thứ năm: Dựa trên việc hiệu suất mạng bị hạ xuống trong các cuộc tấn công thông thường, luận án đề xuất mô hình trạng thái thuật toán Back-off, mô hình trạng thái kênh, 03 tham số hiệu suất. *Thứ nhất,* đã đề xuất được một mô hình phân tích mới đối với lớp MAC của IEEE 802.11 bằng việc sử dụng các thuật toán EIED đã bao gồm xử lý hiện tượng đóng băng back-off. *Thứ hai*, phân tích hiệu suất mạng theo các thuật toán back-off khác nhau dựa vào 3 tham số lưu lượng truyền tải, xác suất rớt gói tin và độ trễ truy cập đối với nút bình thường và nút lỗi. *Thứ ba* luận án đã đánh giá được thuật toán EIED back-off có hiệu suất tốt hơn so với thuật toán BEB trong điều kiện thông thường. Tuy nhiên, khi mạng tồn tại nút độc do ảnh hưởng của các tấn công thông thường, thì hiệu suất của mạng sử dụng thuật toán BEB back-off tốt hơn thuật toán EIED.

- Đóng góp thứ sáu: căn cứ vào yêu cầu thực tế công tác và nội dung nghiên cứu ở trên, luận án thiết kế hệ thống thông tin liên lạc bí mật nghiệp vụ thông qua truyền ảnh số có bảo mật dựa trên các nghiên cứu trên và mô-đun thu phát số FHSS.

CÁC ỨNG DỤNG, KHẢ NĂNG ỨNG DỤNG TRONG THỰC TIỄN HOẶC NHỮNG VẤN ĐỀ CÒN BỎ NGỎ CẦN TIẾP TỤC NGHIÊN CỨU

Hiện nay các phương pháp bảo mật thông tin trong ảnh số nói riêng và trong sản phẩm đa phương tiện số trong liên lạc công khai và bí mật luôn được các nước trên thế giới, nhất là các cơ quan đặc biệt về quốc phòng - an ninh quan tâm, đầu tư nghiên cứu và phát triển. Theo hướng này, trong thời gian tiếp theo nghiên cứu sinh sẽ tiếp tục phát triển các nội dung sau:

- Cải tiến thuật toán giấu tin mật nhằm đưa tỷ lệ giấu tin giảm xuống dưới 1%.

- Cứng hóa các tham số sinh số giả ngẫu nhiên nhằm tăng tốc độ xử lý cũng như độ an toàn cho khóa.

- Nghiên cứu về thuật toán đánh dấu bảo mật watermark trên đa phương tiện.

- Nâng cao hiệu suất mạng chống lại tấn công theo các phương thức đặc biệt.

- Tiếp tục hoàn thiện hệ thống thông tin liên lạc bí mật nghiệp vụ thông qua truyền ảnh số có bảo mật cũng như các thủ tục và hồ sơ công nhận liên quan để đưa vào sử dụng trong thực tế công tác.

Xác nhận của người hướng dẫn khoa học	**Nghiên cứu sinh**
GS.TSKH Đỗ Trung Tá	**Lê Hải Triều**