УДК 004.056.55
Д. Козарик; Ю. Лещишин, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ КОМП'ЮТЕРНОЇ СИСТЕМИ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ ТА ПЕРЕДАВАННЯ ФОТОГРАФІЧНИХ ЗОБРАЖЕНЬ

D. Kozaryk; Yu. Leshchyshyn, Ph.D.

METHODS AND MEANS FOR CONSTRUCTING A COMPUTER SYSTEM FOR STREAM ENCRYPTION AND TRANSMISSION OF PHOTOGRAPHIC IMAGES

Сучасне обладнання цифрового зв'язку для систем фото та відео нагляду активно використовуються у різноманітних сферах діяльності людини, від контролю якості виробництва до відео нагляду у охоронних системах та безпілотних літальних апаратів. Від цієї фото і відео інформації залежить якість виготовленої продукції, збереження майна та деколи і життя людини. Тобто така фото і відео інформація є цінною і має бути надійно захищеною від перехоплення та підміни зловмисниками.

Для захисту інформації від перехоплення використовують різноманітні методи та алгоритми шифрування, однак потоковий характер фото та і відео інформації зумовлює використання потокових алгоритмів шифрування з високим рівнем стійкості до зламу.

Специфіка використання фото і відео обладнання для таких задач потребує побудови портативних систем цифрового зв'язку, що використовують мікроконтролери з малим споживанням енергії та, як наслідок, невисокою обчислюваною потужністю. Тому для вирішення таких завдань використовують симетричні алгоритми шифрування, що ґрунтуються на єдиному ключі, який використовується для як шифрування, так і дешифрування [1]. У таких системах мікроконтролер, що відповідає за шифрування, діє як додатковий пристрій до цифрового модему, що усуває необхідність змінювати його конструкцію. Модулі шифрування повинні втілювати найбільш поширені методи апаратного шифрування, зокрема потоковий ARC4 та блочний AES-128. Ефективність цифрової системи зв'язку може бути оцінена за її стійкістю до завад, тобто за характеристиками прийому помилкового біта відповідно до виду модуляції при різних відношеннях сигнал-шум, як показано на рис. 1.

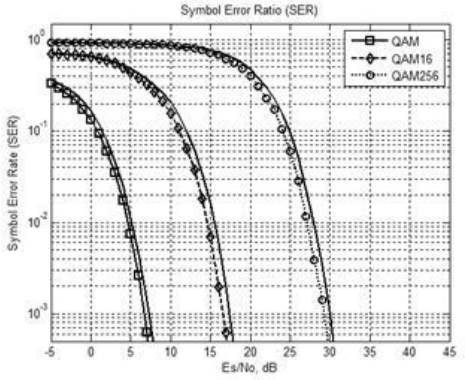

Рис.1. Залежність приймання помилкового біта від виду модуляції, при застосуванні QAM (N_s = 1, 4, 8).

Об'єднання зазначених технологій в одну цілісну комп'ютерну систему дозволяє надійно та ефективно передавати фото та відео інформацію засобами зв'язку. Подальше дослідження спрямоване на моделювання таких систем цифрового зв'язку, що уможливлює порівняння їх ефективності при застосування різних методів шифрування та передавання інформації, а отже розробити портативні пристрої з високим рівнем захисту інформації.

Література

1. Whitfield Diffie and Martin Hellman, «Multi-user cryptographic techniques» [Diffie and Hellman, AFIPS Proceedings 45,1976].