Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 3, Pages 301-303, April 2017

Security Analysis of Medical Images Transmission over Wireless Network

D.Suguna[1] and G.Vallathan[2]

[1]*UG Scholar, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India.*
[2]*Associate Professor, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India.*

Article Received: 16 April 2017 *Article Accepted: 27 April 2017* *Article Published: 30 April 2017*

ABSTRACT

Booming telemedicine applications makes it regarded important to give security administrations to such applications. There are three algorithms proposed for this: they are watermarking-based algorithms, crypto-based algorithms and hybrid algorithms. In this paper, the proposed technique includes Elliptic Curve Cryptography algorithm (ECC) to maintain confidentiality, authenticity, and integrity. Mainly the Elliptic Curve Cryptography Algorithm is utilized for authenticity and integrity. This algorithm suits for the Digital Image and communication process in medical field (DICOM). This focuses on both the header data and the pixel data in DICOM images.

Keywords: ECC algorithm, DICOM image and Confidentiality.

1. INTRODUCTION

Telemedicine is a present day therapeutic care rehearse encouraged by the arrangement of correspondence and data frameworks into the human services foundation. Various advantages are picked up by telemedicine applications, for example, remote determination and counsel among doctors, access to concentrated restorative files and medicinal remote-remove learning. With these benefits, in any case, there are attendant dangers for medicinal information circling in open systems, and in this manner being effectively available by gatecrashers. In this manner experts working in the medicinal field have communicated their pressing requirement for secured plans and techniques fit for giving safe trade of restorative image what's more, records. The significance of a secured trade of therapeutic image has made ready for worldwide human services associations to distribute extraordinary principles that arrangement with restorative information security issues. One such standard is the computerized imaging and correspondence in pharmaceutical (DICOM) standard. The standard gives rules and instruments to human services experts and substances to accomplish three telemedicine security administrations: classification, realness and uprightness.

The classification administration is important to avoid illicit access to the transmitted image, while the respectability and credibility administrations are expected to confirm proprietorship and distinguish altering of the gotten image. Presently, cryptography and advanced watermarking innovations are utilized to actualize plans and calculations equipped for giving the required security administrations to telemedicine applications. The crypto-based approach for accomplishing security in the medicinal data trade frameworks depends on the utilization of cryptographic capacities, for example, symmetric encryption, hashing what's more, computerized marks. Symmetric encryption gives classification for the transmitted image utilizing square figures and stream figures, though hashing and computerized marks confirm legitimacy and strict trustworthiness of the got image. On the other hand, advanced picture watermarking is the act of concealing mystery information into advanced medicinal image.

Secrecy is accomplished by installing the patient's private information as hearty watermarks, while genuineness and respectability are accomplished by covering up strong and delicate watermarks into the therapeutic image. In spite of the fact that the installed watermarks are practically indistinct to the human eye, the general concept of installing, and in this way debasing the medicinal picture, may prompt serious imperviousness to its appropriation by therapeutic models and experts. In this paper, we propose two crypto-based calculations able to do giving classification and confirming genuineness and honesty of DICOM image. Not at all like the DICOM standard and other crypto-based plans, the proposed calculations give classification, legitimacy what's more, honesty for both constitutes of the DICOM image: the header information and the pixel information. Solid cryptographic capacities with remotely and inside produced symmetric keys and hash codes are utilized as a part of the usage of the calculations.

2. PROPOSED SYSTEM

The algorithms provide confidentiality, authenticity and integrity for the pixel data as well as for the header data of DICOM images.

ECC Algorithm

The elliptic bend advanced mark calculation (ECDSA) is a variation of the advanced mark calculation (DSA). Both calculations depend on open key cryptography, be that as it may, ECDSA utilizes elliptic bend cryptography (ECC) to create shorter marks than the first DSA, while keeping up a similar security levels. This property is of a specific significance for our proposed calculations since the 256 bits advanced marks delivered by ECDSA can be effortlessly put away in the DICOM header, as will be clarified in the proposed calculations segment. Besides, ECDSA lessens the computational necessities while keeping up a similar level of security managed by other open key plans with

correspondingly bigger keys. A 256 bits ECC gives a similar security level a 3072 bits Diffie–Hellman conspire offers, at much lower calculation cost.

Encryption and signature creation procedure

This procedure takes the pixel data and the confidential attributes of the header data as its inputs, and outputs fully encrypted pixel data and partially encrypted DICOM header.

Operational steps of the procedure

1. Header information secrecy: To fit in with the essential application level secrecy profile depicted in DICOM PS 3.15, the technique peruses every single classified quality of the header, encodes their unique qualities utilizing AES-GCE and stores the outcome in the 'altered characteristics arrangement (0400, 0550)' while supplanting the values in the first areas with sham ones. An extra yield of AES-GCE is the verification tag of the header which will be utilized as a part of the following stride. The encryption key and initialisation vector utilized by AES-GCE to scramble the header information are taken from the hash code created by applying the whirlpool hash work on the pixel information. The hash code is then scrambled by AES and put away in the DICOM header for later use at the recipient's side. Producing the encryption key and initialisation vector from the hash code of the pixel information makes a solid connection between the pixel, header and security information. Therefore, the client will not have the capacity to see the right header qualities if the pixel information gets messed with or debased. Besides, unique DICOM records have diverse secret header qualities, and along these lines the encryption key and initialisation vector shift from one picture to another. This lessens security hazards and abstains from presenting a potential helplessness in the encryption procedure. 2. Header information realness and honesty: The verification tag created by AES-GCE in the past stride is marked with the private key of the sending substance utilizing ECDSA. The created computerized mark is put away in the DICOM header. Genuineness and respectability of the header information are not tended to some degree 15 of the DICOM standard. 3. Pixel information privacy: The pixel information is encoded with AES-GCE: a similar encryption calculation used to encode the header information. Notwithstanding, the encryption key and initialisation vector are the hash code delivered by applying the whirlpool hash work on the classified characteristics of the header. The hash code (encryption key and initialisation vector) is then encoded by AES what's more, put away in the DICOM header for later use at the recipient's side. An extra yield of AES-GCE is the confirmation tag of the pixel information which will be utilized as a part of the following stride. Encryption, what's more, along these lines secrecy, of the pixel information is not tended to a limited extent 15 of the DICOM standard. 4. Pixel information legitimacy and trustworthiness: The verification tag delivered by AES-GCE in the past stride is marked with the private key of the sending substance, creating a computerized mark of the pixel information. The mark is put away in the DICOM header as per the computerized marks profiles portrayed to some degree PS 3.15 of the DICOM standard.

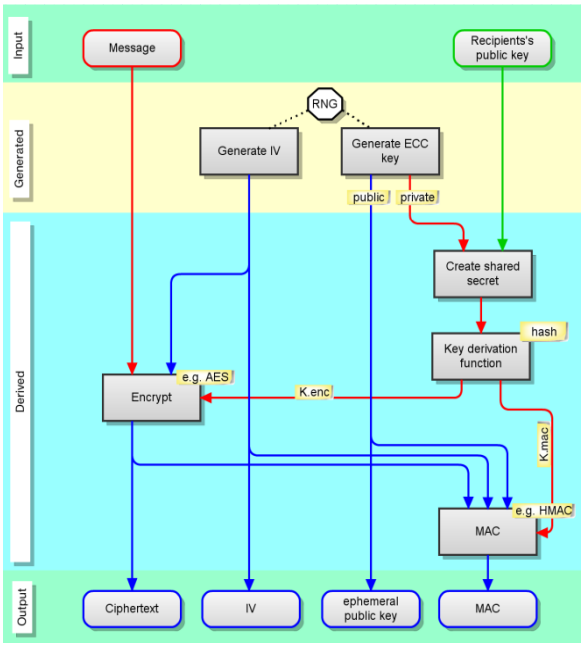

Fig.1. Encryption and signature creation procedure

Decryption and mark check methodology

This methodology decodes the in part scrambled DICOM header furthermore, the encoded pixel information, and confirms their genuineness and respectability as appeared in Figs. 3 and 4 and depicted from this point forward. 1. Pixel information privacy: Retrieve the encoded hash code of the header's private qualities from the DICOM header and unscramble it utilizing the AES standard. The 512 bits yield is utilized by AES-GCM as an unscrambling key and an initialisation vector to decode the pixel information. Other than the pixel information, AES-GCM produces a confirmation tag of the pixel information. 2. Pixel information legitimacy and uprightness: Retrieve the advanced mark of the pixel information from the header and concentrate its confirmation label utilizing people in general key of the sending substance. Contrast the removed tag and the validation tag produced by AES-GCE in the past stride. In the event that a match exists between the two labels, realness and respectability of the pixel information are checked. 3. Header information secrecy: Retrieve the encoded hash code of the pixel information and unscramble it utilizing the AES standard. The 512 bits yield is utilized by AES-GCM as an unscrambling key and initialisation vector to unscramble the private qualities of the header. Other than the unscrambled header's qualities, AES-GCM produces a validation tag of the qualities.

Table 1. Comparison between the Diffie-Hellman algorithm and the Elliptic curve Algorithm

RSA/DSA Key length	ECC Key Length for Equivalent Security
1024	160
2048	224
3072	256
7680	384
15360	512

3. CONCLUSION

The telemedicine is a modern medical care practice facilitated by the deployment of communication and information systems into the healthcare infrastructure. The proposed algorithm provides the confidentiality, authenticity, integrity (CIA) for both the header and the pixel data of DICOM images. The proposed algorithm consumes less time for both encryption and decryption process. The future work is mainly focused on the tamper localisation scheme to allow for content-based integrity rather than the strict-integrity functionality implemented by the current algorithms. The tamper localization is control integrity reduce the noise originating from the transmission process.

REFERENCES

[1] Craig, J., Patterson, V.: 'Introduction to the practice of telemedicine', *J. Telemed. Telecare*, 2005, 11, pp. 3–9.

[2] Raghupathi, W., Tan, J.: 'Strategic IT applications in health care', *Commun. ACM*, 2002, 45, (12), pp. 56–61.

[3] Ashley, R.: 'Telemedicine: legal, ethical and liability considerations', *J. Am. Diet. Assoc.*, 2002, 102, (2), pp. 267–269.

[4] McEvoy, F., Svalastoga, E.: 'Security of patient and study data associated with DICOM images when transferred using compact disc media', *J. Digit. Imaging*, 2009, 22, (1), pp. 65–70.

[5] Pianykh, O.: 'Digital imaging and communications in medicine (DICOM)' (*Springer-Verlag, Berlin Heidelberg*, 2012).

[6] 'Digital imaging and communications in medicine (DICOM) standard, *DICOM'*, 2006.

[7] 'Digital imaging and communications in medicine (DICOM), part 15: security profiles ed.', *National Electrical Manufacturers Association (NEMA)*, 2001, PS 3.15–2001.

[8] Buchmann, J.: 'Introduction to cryptography' (*Springer-Verlag, New York*, 2001).

[9] Cox, I.J., Miller, M.L., Bloom, J.A.: 'Digital watermarking' (*Morgan Kaufmann, San Francisco, CA*, 2002), pp. 26–36.

[10] Hartung, F., Kutter, M.: 'Multimedia watermarking techniques'. *Proc. of IEEE*, July 2006, vol. 87, no. 7, pp. 1069–1107.

[11] Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R.: 'Relevance of watermarking in medical imaging'. *Proc. of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, Arlington, USA*, November 2000, pp. 250–255.

[12] Coatrieux, G., Lecornu, L., Sankur, B., Roux, Ch.: 'A review of image watermarking applications in healthcare'. *Proc. of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, New York, USA*, 2006, pp. 4691–4694.

[13] Coatrieux, G., Maitre, H., Sankur, B.: 'Strict integrity control of biomedical images'. *Proc. of SPIE Security Watermarking Multimedia Contents III, SPIE 2001, San Jose, CA*, January 2001, vol. 4314, pp. 229–240.

[14] Giakoumaki, A., Pavlopoulos, S., Koutsouris, D.: 'Multiple image watermarking applied to health information management', *IEEE Trans. Inf. Technol. Biomed.*, 2006, 10, (4), pp. 722–732.

[15] Giakoumaki, A., Pavlopoulos, S., Koutsouris, D.: 'Secure and efficient health data management through multiple watermarking on medical images', *Med. Biol. Eng. Comput.*, 2006, 44, (8), pp. 619–631.

[16] Thodi, D., Rodríguez, J.: 'Expansion embedding techniques for reversible watermarking', *IEEE Trans. Image Process.*, 2007, 16, (3), pp. 721–730.

[17] Celik, M., Sharma, G., Tekalp, M., Saber, E.: 'Lossless generalized-LSB data embedding', *IEEE Trans. Image Process.*, 2005, 14, (2), pp. 253–266.

[18] Celik, M.U., Sharma, G., Tekalp, A.M.: 'Lossless watermarking for image authentication: a new framework and an implementation', *IEEE Trans. Image Process.*, 2006, 15, (4), pp. 1042–1049.

[19] Liew, S., Zain, J.: 'Tamper localization and lossless recovery watermarking scheme', *Commun. Comput. Inf. Sci.*, 2011, 179, (1), pp. 555–566.

[20] Guo, X., Zhuang, T.: 'Lossless watermarking for verifying the integrity of medical images with tamper localization', *J. Digit. Imaging*, 2009, 22, (6), pp. 620–628.