Design an Implementation of Crypto based Water Marking Techniques for EHR Security

J. Guru Mohish Srivastava[1], R. Sheeja[2]

[1]Department of Computer Science and Engineering
Saveetha School of Engineering, Saveetha Institutions of Medical and Technical Sciences, Chennai, India
[2]Assistant professor, Department of Computer Science and Engineering,
Saveetha School of Engineering, Saveetha Institutions of Medical and Technical Sciences, Chennai, India

Article Info
Volume 82
Page Number: 10788 - 10792
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 19 February 2020*

Abstract

Secured communication in between person to person is more essential in daily life. The information passed in between them is lost as their security levels are less. By using steganography technique, we are going to hide the data from unauthorized user. By using the encryption key, we are going to hide the data and later it decrypts the data by entering the encrypted key. The cryptographic techniques are also used to hide the information and communicate with others. The input data is stored in the form of images, Data stores are used for storing images, so image compression has to be done. In order to use of statistics – hiding key to create a sparse space to accommodate some additional information. Having an encrypted photo contains additional statistics even though they does not understand the photographic content. With the help of encryption key the receiver can decrypt the received information. A photo just like a unique one, but cannot extract the additional information and recover the original contents. When the additional information is not too large then they can use spatial correlation in normal image.

Keywords: *Data security, DES, Encryption, Steganography,*

1. Introduction

In the present, world the communication between the person to person through computer network has more security requirements. Due to attack, there is the chance for data loss. So, more security level should be applied for protects the confidential information. Here we are going to implement new technique by the combination of steganography and cryptography. For security the information from intruders.

Cryptography

It is a type of technique that is used to hide the data which can be unreadable by others and secure more information. It means protects the user data. It involves two basic functions like Encryption and Decryption. Encryption means the process of making the plain text into cipher text. And Decryption means quite opposite to encryption technique. Cryptography mainly used to hide the data from others so that the authorized person can only see the data. There are lots of cryptography algorithms to encrypt the data like DES, AES, Blowfish, RSA etc. But blowfish is the strongest algorithm when comparative to another algorithm.

Steganography

It is used to hide information from the invisible communication between two authorized persons. It is used to cover media information. The embedded process is mainly used to hide the message by producing stego medium.

In steganography there are four different types: 1. Text 2. Image 3. Audio 4. Video

Text Steganography: They has a very less amount of redundant data; therefore, they are very rottenly used.

Audio/Video Steganography: They are very complex in use.

Image Steganography: It is primarily used for hiding procedure of data. It affords a secure and simple way to transfer the information over the internet. It is categorized in various types:

Transform Domain: It includes JPEG. Spread Spectrum: It includes patch work. Image Domain: It includes LSB and MSB in BMP and LSB in JPG.

2. Literature Review

In these paper they have used AEC-GCM and ECDSA. Two algorithms are proposed here and each consists of two procedures they are encryption and signature creation procedure. These algorithms are used for encryption, digital signatures and hashing which provides authenticity, integrity and confidentiality. The encrypted header data is using AES-GCM which consists of cipher pixel data and authentication tag simultaneously. The tag that signed by ECDSA for authentication. The signature creation and encryption procedure to decryption and signature verification. The algorithm is grouped into three classes watermarking–based, crypto-based and hybrid they are used for effectiveness of the proposed algorithms is evaluated and demonstrated through extensive techniques in benchmark set of DICOM images. [1]

In this paper they produced new techniques and methods in cryptography means to improve trustworthiness for making the strong link in between image and data on its integrity and authenticity without any compression of image quality to the end user. There are number of works done in here with the approach of two techniques they are meta data and watermarking. Anyhow there are some limitations in them they must be clearly addressed. The encryption key must be derived in the form of integrity and authenticity the user will be able correct the information if the security key will be tampered or deleted. For multiform of images it must be taken into accounts as their private data as the following conditions in them properly. A simple encryption key will be processed to generate two encrypted forms still similar to each other, the algorithm must perform different encryptions for each form. [2]

This paper is presenting about the lossless watermarking scheme in the process of sensing the original image can be exactly recovered from the watermarked one, in the process of verifying the integrity and authentication of images. The capability of not introducing the any embedding distortion in the region of interest for images. The techniques are used in this paper are ROI and PACS. Through they are going to introduce the protection of data and converted images. Different expansion of adjacent pixel values are noted in them as they are different from each other as they are embedded in several bits. Each of them represented as they are vertex information of a polygon image and introducing embedded distortion in the ROI. Vertex information of a polygon is transmitted in embedding region to the decoder for construction, which improves the embedding capacity of considerable part. The digital signature of the image is embedded for verified integration image. EPR is embedded for verifying the integrity image and simultaneously processing the watermarked image. [3]

Steganography is a critical technique for statistics hiding in any virtual object. Steganography technique is the technology that includes speaking secret statistics in a suitable virtual multimedia cover objects which include audio, video and photograph files. The main goal of steganography is to cover the lifestyles of the embedded facts. Steganography method has progressed the safety of existing facts hiding techniques by using the outstanding improvement in computational power. Objectives of steganography are undetectability, robustness and capacity of the concealed statistics, these key elements that separate it from related strategies like cryptography and watermarking. This paper delivers a survey on virtual images steganography and masking its essential concepts. The development of photograph steganographic methods in spatial representation, in JPEG layout and the additional information recent development inside the subject of photograph steganography. Specific generally used approaches for growing steganographic security are summarized studies are additionally added to develop. [4]

Although human beings have hidden secrets in simple sight-now called steganography-at some stage in the ages, the recent boom in computational energy and technology has propelled it to the vanguard of modern protection techniques. Essentially, the information-hiding manner in a steganographic machine begins by means of identifying a cowl medium's redundant bits (those that may be changed without destroying that medium's integrity). The embedding technique in stego medium creates by changing those redundant bits with statistics from the hidden message. This article discusses existing steganographic systems and offers recent studies in detecting them via statistical steganalysis. Here, we present recent studies and speak the realistic application of detection algorithms and the mechanisms for getting around them. [5]

This academic paper opinion the principle and design of codes for hiding and embedding through signals information can be changed with images, video, audio, graphics, and text. Such codes have also been known as watermarking codes; they can be used in quite a few packages, which includes copyright safety for digital media, content material authentication, media forensics, records binding, and covert communications. Some of those programs imply the presence of an adversary trying to disrupt the transmission of facts to the receiver; other packages contain a noisy, generally unknown, verbal exchange channel. Our cognizance is at the mathematical models, essential principles, and code design techniques which are applicable to records hiding. The method attracts from primary principles in statistics idea, coding theory, game idea, and sign processing, and is illustrated with applications to the hassle of hiding information in images. [6]

Steganography is the artwork of hiding the fact communication is taking place, by means of hiding statistics in other statistics. Many distinct carrier report formats can be used, but digital images are the maximum popular because of their frequency at the internet. This paper introduces new methods wherein in cryptography and steganography are blended to encrypt the data as well as to cover the information in any other medium through photograph processing. This paper securing the image via encryption is done with the aid of DES algorithm using the key picture. The encrypted image can be covered in the another image by mean of using LSB techniques, so that the secret's very lifestyles is concealed. The decryption may be accomplished by means of the same key picture the usage of DES algorithm. [7]

With the advancement in data trade by electronic framework, the requirement of information security has become a necessity. We tend to conferred sight and sound data move by the use of cryptography calculation. The primary image was becoming squares and later on revised utilizing Blowfish calculation. This procedures execution is clearly superior to different cryptography calculation in sight of the use of sq. based mostly modification technique. [8]

The quick improvement of sight and sound and net takes under consideration wide dispersion of computerized media info. Mostly tons are bit easier than other, amendment and duplicate computerized knowledge. aside from that, computerized reports are in addition straightforward to duplicate and distribute, so it'll be looked by varied dangers. it's a significant security and security issue, it become necessary to get appropriate assurance as a result of the urgency, exactitude and affectability of the information. Steganography considers one in all the systems that accustomed make sure the vital knowledge. the first objectives for this paper, to understand the specialists for the principle basics of steganography. Provides a general review of the related to branches of knowledge: Steganography varieties, General Steganography framework, Characterization of Steganography Systems and Classification of Steganography Techniques. [9]

The inventers have given another technique for concealing any disorganized mystery message within a diffusion record. For scrambling mystery message, the inventers have used new calculation projected by Nath etal. For concealing mystery message we've used a technique projected by Nath et al. In MSA technique we've altered Play cheap strategy into another stage wherever we are able to scramble or unscramble any document. We've given another organization technique for manufacturing the irregular key framework to scramble plain content record and to rewrite figure content document. We have similarly taken another calculation for coding the plain content on totally different occasions. Our strategy is totally subject to the whimsical content key that is to be provided by the shopper. The foremost extreme length of the content key will be of sixteen characters long and it would contain any character (ASCII code zero to 255). We've designed up a calculation to work the organization variety and therefore the encoding number from the given content key. the dimensions of the encoding key lattice is sixteenx16 and therefore the all-out variety of networks will be formed from 16 x 16 is 256 that is incredibly immense and so on the off probability best power technique will be applied by someone, at that time they has to provide path for 256 times that is incredibly crazy. Besides, the various encoding technique makes the framework more verified. For concealing mystery message within the unfold document, we've embedded the eight bits of every character of encoded message record in 8 back to back bytes of the unfold document. We've given secret key for concealing data within the unfold document. we have a tendency to backer that our new technique might be typically fitting for concealing any record in any normal unfold document, as an example, picture, sound, video documents. When the message is hided then it will be encoded much thinkable for the trespasser to unhide the real mystery message from the deep-seated unfold document. This strategy can be the foremost verified technique in processed water stamping. [10].

With the progression of innovation internet and completely different correspondence structures that bear it is developed in clear quality daily. Anyway, aboard this progression has likewise developed the danger of programmers and vindictive gatherings. There are a couple of inactive and dynamic assaults creating the duty of knowledge security actually vital. Additional typically than no longer the facts elapsed means that of internet could contain classified or individual data that various people would want to be secured against assaults. completely different information coding calculations are created to confirm that the data transmitted through internet is secure from any quite hacking or assaults. a couple of science calculations in addition are made for coding and with all having a few focal points and impediments. This paper introduces some extent by this point investigation of regular encryption/decoding calculations and its favorable circumstances and burdens. [11]

Security of facts is continually needed whenever communication is accomplished and to obtain that motive different strategies are used so that statistics should no longer be attacked by using the 0.33 party. Different data concealing techniques like cryptography, watermarking etc. are used. But if we want the intruder now not to even realize about the presence of secret information we should use the Steganography Technique. And this technique can be carried out by means of the usage of different documents like text, audio, video etc. One of the steganography sorts as video steganography used to cover the secret facts in a smooth manner because of the complexity of its structure. We have different forms of methods primarily based upon Format, Cover, and Frequency in video steganography. This paper affords an evaluation and evaluation of the video steganography technique carried out to AVI video report with LSB technique and the evaluation of frames within the video record is analyzed with the help of different parameters to discover how similar the cover video frame after embedding the secret information. The analysis is based at the PSNR, MSE, and the end result is given. [12]

In the gift state of affairs, any communication of web and networks application needs safety. Immeasurable statistics protection and records concealing algorithms had been developed within the remaining decade. Cryptography and steganography are the two major techniques for mystery communication. During this paper, the mystery image is initial encrypted by mistreatment BLOWFISH algorithmic rule that has glorious performance and could be a most powerful technique compared to alternative Algorithms. Currently this encrypted image is embedded with video by mistreatment LSB Approach of steganography. Our planned model offers layers of protection for secret facts, that utterly fulfill the straightforward key factors of data safety system that includes: Confidentiality, believability, Integrity and Non – Repudiation. [13]

Blowfish, a new secret-key block cipher, is proposed. It is a Feistel network, iterating a easy encryption characteristic 16 times. The block size is sixty four bits, and the key may be any length up to 448 bits. Although there is a complex initialization segment required before any encryption can take place, the actual encryption of data may be very efficient on huge microprocessors.

The cryptographic network desires to offer the sector with a new encryption standard. DES, the workhorse encryption set of rules for the past fifteen years, is nearing the stop of its useful life. Its 56-bit key size is prone to a brute-pressure attack, and latest advances in differential cryptanalysis and linear cryptanalysis imply that DES is liable to other assaults as well. [14]

3. Existing System

The lossy compression method in compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. The user gets loss of images and data. To if the restriction of information is final touch then it is finally getting into un authorized massive of consumption only user has more information in secure but loss of facts is more inside the existing proposed systems. The algorithm previously used are having some low significant values through these the performance varies and make them high confidential in use of them.

Crypto-based Algorithm Services

Table 1: Security Services in crypto based algoritm

Algorithm	Confidentiality	Authenticity	Integrity
AES Algorithm	Header data	Pixcel data	Pixcel data only
RSA Algorithm	Pixcel data	Pixcel data	Pixcel data only
Blow fish Algorithm	Header and pixcel data	Header and pixcel data	PIxcel and header data

Security analysis is an important feature in encryption and decryption algorithm. The algorithm which was used in would be fast and not secure then we will be avoided to use them. Then we are automatically move to the accurate on and secured one. The encryption will be hide the data in particular time span and automatically from different algorithms the speed will be varies.

4. Conclusion

In this study, security is needed more to make communication in between the persons through network. So, we are going to use cryptography and steganography in building the project. The data will be converted into the image files for not to loss of information then also to compress the data from limited storage. The new strategy is going to us in projected synchronization techniques between the sender and collector are learned for hide the information from unauthorized person to be confused in understanding the communicated information.

5. Future Scope

Further work can specialize in up the on- board registering skills with the goal that the overwhelming majority of the calculation bother is expelled from the bottom station thus decreasing the large live of remote traffic at the present caused. To securely move image and video data, the quad rotor engineering is furnished associate degree on-board secure advanced camera (SDC). In such a circumstance, the quad rotor may be sent to catch and transmit touchy information faithfully mistreatment it's on-board SDC. This is often be} particularly vital in specific applications during which associate degree outsider can alter the knowledge transmitted from the quad rotor.

References

[1] Ali Al-Haj, Gheith Abandah, and Noor Hussein, "Crypto-based algorithms for secured medical image transmission", IET Information Security, 9(6), pp. 365-373, Nov. 2015.

[2] L. Kobayashi, S. Furuie and P. Barreto, "Providing integrity and authenticity in DICOM images: A novel approach. IEEE Transactions on Information Technology in Biomedicine, vol. 13, issue: 4. (2009) 582-589

[3] X. Guo, T. Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data," Journal of Digital Imaging 22(1): (2009) 53-64.

[4] J.C. Judge, Steganography: past, present, future. SANS Institute publication, /http://www.sans.org/reading_room/whitepapers/stenganography/552.phpS, 2001.

[5] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Security and Privacy 1 (3) (2003) 32–44.

[6] P. Moulin, R. Koetter, Data-hiding codes, Proceedings of the IEEE 93 (12) (2005) 2083–2126.

[7] S.B. Sadkhan, Cryptography: current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19–23, 2004, pp. 417–418

[8] Ratinder Kaur, V.K. Banga "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP 2012) July 15-16,2012 Singapore.

[9] Zaidoon kh.AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan. O. Alanazi "Overview: Main Fundamentals for Steganography" Journal of computing, Volume 2,Issue 3,March 2010 ISSN 2151-9617

[10] Advanced Steganography Algorithm using encrypted secret message, Joyshree Nath and Asoke Nath, International Journal of Advanced Computer Science and Application (IJACSA) Vol-2 No.3, Page 19-24, March 2011

[11] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis", in International Journal of Emerging Technology and Advanced Engineering Volume1, Issue 2, December 2011.

[12] Mritha Ramalingam, "Stego Machine – Video Steganography using Modified LSB Algorithm" ,World Academy of Science, Engineering and Technology 50 2011.

[13] Prof. DP Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak "Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithm in Video Steganography" International Journal of Engineering Research and Application (IJERA) Volume 1, Issue2, pp.102-108.

[14] B.Schneier, Description of a new Variable-Length Key, 64-bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp.191-204.