SURVEY ON SECURING MEDICAL RECORD USING DYNAMIC WATERMARK GENERATOR SEQUENCE AND SELECTIVE ACCESS CONTROL

[1]Megha Trivedi, [2]Dishant Soni,
[1]Student, [2]Assistant Professor
[2] Computer Department
[1] Sankalchand patel College of Engineering Gujrat,India
[2] Sankalchand patel College of Engineering Gujrat, India

Abstract— Information security is process to encrypt and decrypt the information. Patients supply information to medical application provider hoping that the information supplied will not be used anywhere. If these applications are compromised due to attack patient's medical information may be revealed.

Index Terms— health information, encryption, medical images, AES, random generator

I. INTRODUCTION

With advances in healthcare informatics, one can provide better means to process patient records and therefore speed up the treatment, which in turn reduces the overall cost. Many tools exist for facilitating patient record processing: from assisting data entry to manipulating records, from generating output in required form to transferring it to other physicians for further examination, or to save it digitally for future use. The significance of relies on the fact that we bring a software engineering oriented systematic approach to design and develop an electronic health record system (EHR). Our scheme is fundamentally a computer based patient record (CPR) system. In particular, this work extends a CPR system by incorporating a software engineering approach during development, and incorporates many aspects from database design, web deployment, and security.[1]Advancement in health information systems with emphasis on tele-medical procedures ,remote healthcare services and health cloud storage infrastcture with medical imaging data as key component in ensuring effective health delivery. The importance and urgency nature of health care services delivery has led to the creation of opportunities in the software development sector.[2] In encryption key sharing using AES key and ecc use for securing key its use in digital signature.[1] Cryptographic algorithm is the mathematical function used for encrypting and decrypting process, this mechanism leads to encrypt the original data using different combination of a key a word, number, or expression. The encrypted data security is completely reliant on two important aspects; the key confidentiality and the cryptographic algorithm strength. A cryptosystem is designate due to the presence of cryptographic algorithm, along with all the working protocols and all potential keys.[5] Medical image[2] information is a central part of the diagnostics in health information system. Health information[2]system is part of the information technology infrastructure due to nature of the data processed with treatment history, medical records etc.Digital watermarking [12] is the act of hiding information in multimedia data, for the purposes of content protection or authentication. In ordinary digital watermarking, the secret information is embedded into the multimedia data with minimum distortion of the cover data. Due to these watermarking techniques the watermark image is almost negligible visible.

II. RELATED WORK

At Present[11] Research work in digital watermarking can be categorized into two parts: Spatial-Domain and Frequency-Domain.(Toughi Shahriyar,Mohmmad H. Fathi,Yoones A. Sekhavat,2017**)** In this paper [3] use the three-technique to encrypt the image.in ecc parameter generate the random numbers.it generates the random curves.in image encryption hybrid AES algorithm used.In proposed method, ECC and AES using maskers with a created primary key.In encryption phase create the new color cipher image.

(Quist-Aphetsi Kester,et al ,2015)Medical Images Are Important [2] For Health Information Systems.Privacy, Security Is Important For Patients To .It Confidentiality And Authentication Methods To Authorship.In This Paper Author work Cryptographic And Watermarking Technique Combined.It Fully Recoverable.During The Watermark Process Changes The Image Pixels.

(Rafic Hamza,2016) In This Paper [4] Novel Algorithm For Pseudo-Random Sequence Generator.It Uses A Digital Image Cryptography Applications.In The Proposed Method [64*64] Bits It Is The Limit. PRNG Solves The Non-Uniform Distribution.Algorithm More Convenient For Encryption Images.Chaos-Based Cryptography Problem Is Select Chaotic System Generate The Pseudo-Random Bits.

(Rim Zahmoul,Ridha Ejabali,Mourad Zaied,2017) Beta Maps Are Based On [5] A Beta Function Which Is The Simple Mathematical Tool.The Proposed Algorithm Image Encryption Approach Adopts Permutation-Substitution Network Structure With Good Confusion And Diffusion Properties.

(Volodymyr Lynnyk,Nonoru sakamoto,Sergej Celikovsky,2015)An Approach [6] To Generate The Pseudo Random Number Sequences From A Single Generalized Lorenz System (GLS) Is Proposed In This Paper. New Algorithms Are Introduced For The Binary Sequence generation based on the GLS. Basic Statistical Tests And Security Analysis Of The Pseudo Random Number Generators (PRNG) Based On The GLS Are Also Provided.

(Laiphrakpam Dolendro Singh And Khumanthem Manglem Singh,2015) The Exponentially [7] Hard problem to solve an elliptic curve discrete logarithm problem with respect to key size of elliptic curve cryptography, helps in providing a high level of security with smaller key size compared to other cryptographic technique which depends on integer factorization or discrete logarithmic problem. in this paper, we implement the elliptic curve cryptography to encrypt, decrypt and digitally sign the cipher image to provide authenticity and integrity.

(Mohammad Masdari,Safiyyeh Ahmadzadeh,2017)"In This Paper Tele Medical Information System[8]is a medical center.TMIS is a remote care.In survey paper presents the different type uses the technique.This techniques secure the data and protect to the attacks.Authentication have different type process.one is one to one authentication second is a mutual authentication and third is many to many authentication."

III. COMPARISION

Table 1:Comperision for Paper

Paper Title	Domain	Technologies	Limitations	Future Scope
An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System	Image Encryption	ECC,AES,Random Generator	Random coordinates technique is unique way to the generate method.	Generate the new key method combining multiple encryption methods with the proposed method.
A Cryptographic Technique for Security of Medical Images in Health Information Systems	Health Information	Cryptographic and Watermarking Technique	There was a change in pixel value during the watermarking process	
A Novel pseudo random sequence generator for image-cryptogrphic applications	Pseudo random sequence	Cryptographic	[64*64] bits required to proposed method	PRNG Combined with the Proposed method with image encryption
Pseudo random number generator based on the generalized Lorenz chaotic system	Pseudo random sequence	Chaos,Random number Generator	In this proposed attacks on the cryptosystems based on weakness of the binary sequence which are generated by PRNG	
A Survey and taxonomy of the authentication schemes in Telecare Medicine Information System	Medical Information	Password ,Smart card, Biometric	Patients privacy over insecure communications and control the access remote medical databecome a critical challenges.	
Color image encryption based on hybrid hyper-chaotic system and cellular automata	Image Encryption	Chen system,Logistic map,	cellular automata in cryptography include limited number of reversal rules and inability to produce long sequences of states by these rules	the effect of hybrid clustering-based image encryption and hyper chaotic functions on the encryption performance.

IV. CONCLUSION

In recent era medical domain use the various advanced technology. In medical images, authentication and authorized is required. There for, we need batter technique that can provide batter security of medical data such as medical images and its information .We in this paper survived various thechniques to secure the medical information.We objerved that image watermarking with information found to be a batter solution for the problem.This technique its having some limitations like reproduciability of watermark imag. Hence research has to be made in this direction to secure the watermark information and other information.

REFRENCES

[1]. Ebru Celikel Cankaya1 Than Kywe2" A Secure Healthcare System: From Design to Implementation "SCSE:2015

[2]. Quist-Aphetsi Kester, Laurent Nana,Anca Christine Pascu,Sophie Gire,Jojo M.Eghan,Nii Narku Quaynor "A Cryptographic Technique for Security of Medical Images in Health Information Systems"Procedea Computer Science 58(2015)538-543

[3]. Toughi Shahriyar,Mohmmad H. Fathi,Yoones A. Sekhavat,An"Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System"Signal Processing june(2017)

[4]. Rafic Hamza "A novel pseudo random sequence generator for image –cryptographic applications"/ http://dx.doi.org/10.2016/jisa.2017.06.005

[5]. Rim Zahmoul,Ridha Ejabali,Mourad Zaied "Image encryption based on new Beta chaotic maps" optics and lasers in engineering 96(2017)39-49

[6]. Volodymyr Lynnyk,Nonoru sakamoto,Sergej Celikovsky"Pseudo Random number generator based on the generalized Lorenz chaotic system"/IFAC-PapersOnLine 48-18(2015)257-261

[7]. Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh Procedia Computer Science 54 (2015) 472 – 481

[8]. Mohmmad Masdari,Safiyyeh Ahmadzadeh "A Survey and taxomany of the authentication schemes in Telecare Medicine Information System"/ http://dx.doi.org/10.1016/j.jnca.2017.03.003

[9]. K. Shankar, P. Eswaran, An efficient image encryption technique based on optimized key generation in ecc using genetic algorithm, in: Artificial Intelligence and Evolutionary Computations in Engineering Systems, Springer, 2016, pp. 705–714.

[10]. Y. Niyat, M. H. Moattar, M. N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata, Optics and Lasers in Engineering 90 (2017) 225–237

[11]. Amit Mehto,Neelesh Mehra"Adaptive Lossless Medical Image Watermarking Alorithm based on DCT&DWT "(ICISP2015)

[12]. Tanmoy Sarkar sugata Sanyal."Digital Watermarking Techniques in Spatial and Frequency Domain",Arixiv.org/Ftp/Arxiv/Papers/1406/1406.2146