International Journal of Advanced Technology and Engineering Exploration
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
Volume-2 Issue-12 November-2015

A review on Image Security through standard encryption techniques

Priyank Singhai[1*] and Amit Shrivastava[2]
Mtech Scholar Department of computer science, Sagar Institute of Research & Technology , Bhopal, India[1]
HOD Department of computer science, Sagar Institute of Research & Technology , Bhopal, India[2]

Abstract

Image encryption is an important area of today's research community as it is very important so that any data violation can be prevented. There are a few approaches to secure the information in which cryptography and steganography is the main. There are several techniques are available for text data but in case of image data all the techniques which are applied in text data may not fit in the image data. As there is not a solitary general system which can secure every one of the sorts of information. There is the need to change the encryption and execution with the goal that it can be connected to distinctive kind of potential outcomes. In this paper we have discussed about image cryptography and steganography so that we will able to secure the image data.

Keywords

Image Cryptography, Image Steganography, Data Security, Standard Encryption Techniques.

1. Introduction

In the current scenario we see that the use of a single stage data encryption algorithm is not very secure. To overcome this situation a combined encryption algorithm is proposed in this thesis. That is, the algorithm security is greatly enhanced, through researching several well-known data encryption algorithms, and improving some data encryption algorithms and arranging encryption algorithms in some sort of order. An improved concept is proposed by analyzing the principle of the cryptography technique based on the combination of symmetric key and translation of plain text into an image. Moreover, the safety measures, security and performance of the proposed concept will also estimate [1].

The experimental results depend upon combination of symmetric and conversion of plain text into an image and finally attaching key will endorse the effectiveness of the proposed concept. The resultant cipher text which is generated by this method will be unreadable as well as perplexing that the information transferred is text or image and will be appropriate for realistic use in the secure transmission of confidential information over the Internet [2].

Disregard cryptography is mindful here the confederation of keyed equivalent and ability in pretending to pay deception walk are including beneficial than those developed utilizing unadulterated" proportional or uneven systems alone [1]. Standard in the fundamental, this takes the vicinity of a deviated cryptosystem the world suitably of a non-specific keyed mirror-like cryptosystem with certain bolster properties as a sub-schedule. This empowers the plan of tricky in which a few of the computational inconvenience is hypothetical by the about productive in extent cryptosystems undiplomatic trading off the field of the general cryptosystem [2][12][13]. Generally, disregard cryptography is rummage to Rather initiate encryption information at the obvious encryption of the correspondence is given by a consistent encryption plot want under an arbitrarily produced symmetric key [3][4][5]. The uneven encryption wish is problematically second-hand to encode this arbitrarily produced symmetric key. This permits the encryption objective to squire sting messages, an obligation with some immaculate unbalanced encryption plans [6][7].

Contemporaneous cryptosystem gives the power to content stabilizer for recommend in point of interest transmitting it absence of restriction an unreliable channel [8]. The encryption plan is likewise recommended in [9]. Straightforwardly proof is transmitted over the web we get sanctuary letter, retreat, legitimacy and non-denial for it. In senior age encryption and computerized marks are concentrated on a significant obligation in end report privacy and information respectability yet autonomously [10].

*Author for correspondence

Generally the report is rummage to stages saucy premise computerized seal and slanted the message is not publishable to convey to an end both the secrecy and information trustworthiness [11]. The craving is over and over flaunted as signature then encryption longs. The plan having pair pressurize: Shoddy adequacy and high cost of such recreation [12]. There is several other image encryption techniques are also discussed in [13-17]. Some related standard encryption techniques are also suggested in [18-21]. The main objectives are to solve the key exchange dilemma, transfers single file together with data as well as key and to improve the conventional cryptographic algorithm and make it effective against brute force attack.

2. Literature Review

In 2011, Matalgah et al. [22] motivated by system coding hypothesis a productive half and half encryption-coding calculation that obliges utilizing customary encryption just for the first little measure of information. This measure of information, which we allude to as the first square, is controlled by the conventional encryption calculation to be connected on this first piece. In their proposed calculation, all whatever remains of the data will then be transmitted safely over the remote channel, utilizing system coding, without a requirement for utilizing customary encryption. The same with the distinctive methodology has been proposed in [23][24] .

In 2011, Wai Zin et al. [25] watch that because of expanding the advancements security frameworks are extremely well known in numerous territories. The security of data can be attained to by utilizing encryption and steganography. In cryptography, scrambled information is transmitted in the wake of changing the other frame rather than the first information. Contrast cryptography, data concealing procedure can be reached out for shielding from the intriguing of any assailant. They proposes the improve security framework by consolidating these two procedures. Their proposed framework means for information privacy, information validation and information trustworthiness.

In 2011, Sandeep Bhowmik et al. [26] recommend that the adequacy of the insurance through encryption relies on upon the calculation connected and in addition on the nature of the "key" utilized. On the off chance that a "key" is severely outlined or erratically chose, clearly the assurance neglects to give fitting security and dishonorable access can be picked up on the secured data. The principal calculation in cryptographic framework outline is the calculation to create 'key'. It determines the way in which the "key" is to be picked. This work concentrates on an absolutely new approach towards the "key" era for encryption algorithms.

In 2011, Rohollah Karimi et al. [27] explore shortcomings in existing Geoencryption frameworks and propose a few answers for increment the wellbeing and dependability in these frameworks. For this reason they show another geoencryption convention that will permit portable hubs to impart to one another securely by confine disentangling a message in the particular area and time period.

In 2012, Rajavel, D. et al. [28] proposed another cryptographic calculation in light of mix of hybridization and revolution of shapes. Hybridization was performed utilizing enchantment 3D shapes with m number of n request enchantment square for the creating crossover blocks. The got half breed solid shape was rearranged by means of pivot square, which thus created from haphazardly chose enchantment square. Cubic revolution was executed as same that of basic Rubik's shape rearranging.

In 2012, P. Fanfara et al. [29] recommend that Communication security is one of numerous informatics parts which have gigantic advancement. Delicate information is progressively utilized as a part of correspondence and that is the motivation behind why security prerequisite is all the more convenient and essential. The danger of getting information through different increments with upgrading the force of today's PCs. Their consideration is fundamentally given to sender validation in light of utilizing advanced signature and hilter kilter encryption by means of restricted hash capacity to figure open and private keys.

In 2012, Lili Yu et al. [30] recommend that calculation security is extraordinarily enhanced, through examining a few renowned information encryption calculations, and enhancing some information encryption calculations, and organizing encryption calculations in some request. At long last, the joined encryption calculation is effectively made by utilizing the starting encryption calculation, Micro Genard encryption calculation and the renowned

Base64 encryption calculation. That is, as per the request of the starting encryption calculation, the enhanced Micro Genard encryption calculation and the well-known Base64 encryption calculation, the client's data is bit by bit scrambled, and the calculation security is significantly improved.

In 2012, Seung-Hoon Cho et al. [31] proposes an ongoing information stockpiling framework that is made out of the pressure of the flight and voice information in view of DPCM, the encryption of the compacted information utilizing AES encryption calculation and the re-plan of the encoded information by rearranging system. The proposed framework is executed in equipment utilizing Verilog HDL and we tried the execution of the framework with the reproduction flight and voice information. Therefore, they found that the proposed framework pack the information proficiently and improves security qualities

3. Problem Domain

Most intriguing thing in this method is the mix of two distinct procedures. Basically this technique is a method of encryption that combines two or more encryption technique and usually includes a combination of substitution and symmetric key encryption algorithm like AES to take the benefits of the strengths of each type of cryptographic technique. The advantage of the symmetric encryption is the constant performance and the speed. On the other hand RGB substitution provides better security as it is changing the format of the plain text and confuses the intruder that weather transmitted data is a form of image or it is some other secure information. Another reason for choosing such architecture is that in the survey's we have seen that there are no key exchange method has been implemented. Every algorithm needs a secure mode of communication for key exchange. So for every set of data transfer they need one more file which contains key. Hence for sending single information minimum two data transfers and two communication channels are used. Further our proposed model sends only 2 integer space memory as a key which is very small these two integers are attached in the image obtained after RGB substitution. Our proposed model will solve the key exchange problem and only a single file will be transferred in the proposed methodology, this single file will contain data as well as key but only the legitimate user can only decrypt the file correctly. I will implement this concept using JAVA application on windows 7 operating system with MS-access database. The reason behind choosing JAVA and MS-access is that it is easily available and takes very less memory space.

4. Analysis

Our paper main motivation is ensure correctness, security and efficiency. For a good encryption scheme it should be correctly verifiable. The computational scrimp and notice on costs of an encryption longing should be smaller than those of the best known signature-then-encryption schemes with the same provided functionalities. An encryption long ought to at the same time fulfill the security attributes of an encryption scheme and those of a digital signature. Such helper properties mainly include: Confidentiality, Unforgeability, Integrity, and Non-repudiation. Varied encryption technique adjust abet attributes such as Public verifiability and Forward secrecy of message confidentiality while the others do not provide them [13][14].

The point of cryptography is to guarantee security of information in correspondence furthermore capacity methods, for example, the capacity to delegate processing to untrusted parties. On the off chance that a client could take an issue characterized in one mathematical framework and encode it into an issue in an alternate logarithmic framework in a manner that unraveling again to the unique logarithmic framework is hard, then the client could encode lavish calculations furthermore send them to the untrusted party[15]. This untrusted gathering then performs the relating reckoning in the second logarithmic framework, giving back where it's due to the client. After getting the result, the client can unravel it into an answer in the first logarithmic framework, while the untrusted party adapts nothing of which reckoning was really performed.

Cryptography is the art of securing information, which gives implies and routines for changing over information into unintelligible structure (encryption strategy), so that just substantial client can get to information decoding system. Cryptography is the practice and investigation of procedures for secure correspondence in the vicinity of outsiders (called foes). All the more by and large, it is about developing and breaking down conventions that defeat the impact of enemies and which are identified

with different perspectives in data security, for example, information classification, information uprightness, confirmation, and non-renouncement. Cryptography proceeding the advanced age was successfully synonymous with encryption, the change of data from a decipherable state to evident rubbish. The originator of a scrambled message shared the disentangling system expected to recuperate the first data just with proposed beneficiaries, subsequently blocking undesirable persons to do likewise. Encryption at the source and unscrambling at the beneficiary guarantee secure transmission of message through the channel. Be that as it may, a few assaults like capture and alteration of data substance by an unapproved individual or a gatecrasher can make the channel frail for secret information exchange.

5. Conclusion and Future Suggestions

This paper provides the analysis on Image encryption based on the previous related research. In this paper we have first investigates the past exploration with their preferences and drawbacks. At that point we recommend the crevices and the outcomes. We have likewise examined the parameters for the input. Taking into account the observations we can suggest standard encryption system with data correlation and entropy assessment which will be better security alternative.

References

[1] Ahmad Abusukhon Mohammad Talib "A Novel Network Security Algorithm Based on Private Key Encryption" IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 2012, pp. 33-37.

[2] M. Kiran Kumar, S. Mukthyar Azam, and S. Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique", International Journal of Network Security and its Applications, 2010, pp. 30-41.

[3] Komal D Patel, Sonal Belani "Image Encryption using different Techniques" International Journal of Emerging Technology and Advanced Engineering Volume: 1, Issue: 1, 2011, pp. 30-34.

[4] P.Karthigaikumar Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on Computational Science - New Dimensions & Perspectives", 2011.pp. 166-172.

[5] Manoj.B, Manula N Harihar "Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology, Volume: 1, Issue: 5, June 2012.pp. 290-294.

[6] Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security Volume: 12, Number: 04, pp. 18-31.

[7] P. Radhadevi, P. Kalpana "Secure Image Encryption Using AES" International Journal of Research in Engineering and Technology Volume: 1 Issue: 2, pp. 115-117.

[8] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm" International Journal of Computer Science Issues Volume: 9, Issue: 4, 2012, pp. 51-57.

[9] Praveen.H.L , H.S Jayaramu, M.Z.Kurian "Satellite Image Encryption Using AES" International Journal of Computer Science and Electrical Engineering (IJCSEE), Volume:1, Issue: 2, 2012, pp. 56-60.

[10] Whitfield Diffie, "The First Ten Years of Public Key Cryptography", Proceedings of the IEEE Volume 76, 1988 pp. 560-577.

[11] W.E. Burr, "IEEE Security and Privacy Volume: 1, Issue: 2", 2003, pp. 43-52.

[12] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal Volume: 6, Issue: 2, 2010, pp. 1-14.

[13] Nazmudeen, Naida H., and F. J. Farsana. "Satellite Image Security Improvement by Combining DWT-DCT Watermarking and AES Encryption." International Journal of Advanced Computer Research 4, no. 2 (2014): 645.

[14] Sandhya Rani M.H., K.L. Sudha, "Design and Implementation of Image Encryption Algorithm Using Chaos", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.660-664.

[15] Arunabha Sengupta, "Dynamic fragmentation and query translation based security framework for distributed databases", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-20, September-2015, pp.249-263.

[16] Ketki P. Kshirsagar, " Key Frame Selection for One-Two Hand Gesture Recognition with HMM " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015 ,pp.192-197.

[17] Nanda Hanamant Khanapur and Arun Patro, " Design and Implementation of Enhanced version of MRC6 algorithm for data security " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015 ,pp.225-232.

[18] Dubey, A.K., Dubey, A.K., Namdev, M. and Shrivastava, S.S., 2012, September. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In Software Engineering (CONSEG), 2012 CSI Sixth International Conference on (pp. 1-8). IEEE.

[19] Manju Kaushik, Gazal Ojha , " Attack Penetration System for SQL Injection " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.724-732.

[20] Urmi Chhajed, Ajay Kumar, "Detecting Cross-Site Scripting Vulnerability and performance comparison using C-Time and E-Time", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.733-740.

[21] Bhavesh Joshi and Anil Khandelwal, "Rivest Cipher based Data Encryption and Clustering in Wireless Communication", International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-2, January-2015, pp.17-24.

[22] Matalgah, Mustafa M. ,Magableh, A.M., "Simple encryption algorithm with improved performance in wireless communications",IEEE 2011.

[23] Asoke Nath, Debdeep Basu, Surajit Bhowmik, Ankita Bose, Saptarshi Chatterjee, " Multi Way Feedback Encryption Standard Ver-2(MWFES-2) " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-13, December-2013 ,pp.28-34.

[24] Sagar Chouksey, Rashi Agrawal, Dushyant Verma,Tarun Metta, " Data Authentication Using Cryptography " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-10, June-2013 ,pp.183-186.

[25] Wai Wai Zin and Than Naing Soe ," Implementation and Analysis of Three Steganographic Approaches", IEEE 2011.

[26] Sandeep Bhowmik and Sriyankar Acharyya," Image Cryptography: The Genetic Algorithm Approach",IEEE 2011.

[27] Rohollah Karimi and Mohammad Kalantari, "Enhancing security and confidentiality in location-based data encryption algorithms", IEEE 2011.

[28] Rajavel, D., Shantharajah, S.P., "Cubical key generation and encryption algorithm based on hybrid cube's rotation",IEEE 2012.

[29] P. Fanfara, E. Danková and M. Dufala, "Usage of Asymmetric Encryption Algorithms to Enhance the Security of Sensitive Data in Secure Communication", 10th IEEE Jubilee International Symposium on Applied Machine Intelligence and Informatics, SAMI 2012.

[30] Lili Yu, Zhijuan Wang and Weifeng Wang, "The Application of Hybrid Encryption Algorithm in Software Security", 2012 Fourth International Conference on Computational Intelligence and Communication Networks.

[31] Seung-Hoon Cho, Chan-Bok Jeong, Seok-Wun Ha, Yong Ho Moon," A Flight Data Storage System with Efficient Compression and Enhanced Security", IEEE 2012.