ACCENTS Transactions on Image Processing and Computer Vision, Vol 2(2)
ISSN (Online): 2455-4707
http://dx.doi.org/10.19101/TIPCV.2016.22001

Review Article

Secure image data transmission and hiding technique: a survey

Pooja Chaturvedi [1*] and Dinesh Chandra Jain[2]
M.Tech Scholar, CSE, SIRT Bhopal, India[1]
HOD, CSE, SIRT, Bhopal, India[2]

Abstract
Security is the need of today's era. In every field like data management, data communication, e-commerce etc. The security task is being complicated as there are variety of data to secure as different level of data security is needed based on the data type. In this paper we have discussed and analyse the image data security. Image cryptography, data hiding, image entropy and image XOR. Based on these parameters we have analysed the previous research work and discussed the advantages and gaps.

Keywords
Encryption, Chaos, Steganography, Security measures.

1.Introduction
With the quick enhancements and the information exchanges, considerable measures of concerns have been raised in the security of data transmitted or set away over open channels. Especially at the level of content and picture data. As showed by [1] there are three essential schedules for secured correspondence open, specifically, cryptography, steganography and watermarking. Among these three, the first one, cryptography [2]-[4], deals with the change of systems for changing over information amidst reasonable and unlimited structures in the midst of information exchange. Steganography [5]-[6], on the other hand, is a strategy for hiding and isolating information to be gone on using a transporter signal [1]. The third one, watermarking [7]-[8], is a technique for making genuine systems for disguising prohibitive information in the perceptual data. In [9] creators have prescribed that most by far of the regular pictures, the neighbouring's estimations pixels are unequivocally related (i.e. the estimation of any given pixel can be sensibly expected from the estimations of its neighbours [10]-[12]. So remembering the final objective to achieve the higher relationship entropy among pixels and extending the entropy quality is a creating examination range. In the event of content the information ought to be covering up with pictures so that more security will force with RGB mixes and varieties.

In [13] the most basic issues, which impact the standard information of cutting edge media, are the best approach to secure robbery and ownership. The watermarking of the common strategies consider ding as another database for giving the copyright protection, is a technique in perspective of embedding a specific engraving or check into the modernized things. While a couple watermarking computations have been proposed [14] in this heading.

So in the resulting fragment we discuss information Encryption strategy for picture encryption. We also discuss the significant edges which are used as a piece of picture encryption with their purposes of hobby and downsides. Finally considering the talks we also suggest some future remark which might be beneficial in this bearing.

There are various key strategies which are second-hand pervasive cryptography, for instance, private or puzzle key cryptography, open central or kilter, automated check, and hash limits [15]. In private key cryptography, a single key is remaining for both encryption and interpreting. This obliges wind when in doubt part pass on offering a mimic of the key and the key be struck by be passed swear off a sheltered channel to the following individual [13-22]. Private-key algorithms are level indestructible and adequately completed in gear. Thusly they are on and well actually for mass estimations encryption. The limitless please of the inside and out balanced encryption depend on upon plaintext, encryption

*Author for correspondence

computation, key and unscrambling count. The plaintext is the size ahead requiring the encryption figuring. It is joining of the inputs to the encryption figuring. The encryption count is the computation used to proceed and manage the data stranger plaintext to figure mitigate. The secret key is a practically identical to repulse of the encryption computation and of the plaintext and it is partner of the encryption's inputs count [23][24]. The figure substance is the rebellious substance find as yield [14][15]. The steganography procedure with cryptography will upgrade the security as the obscure substance and the randomization quality can be progressed.

2.Literature survey

In 2005,Zhi-Hong Guan et al. [25] have presented another picture encryption arrangement, in which improving the positions and changing the dull estimations of picture pixels are joined to bewilder the relationship between the figure picture and the plain picture.

In 2013, Praloy Shankar De et al. [26] try has been made to focus on a count of cryptography that was made by using old rationalities. DEDD Symmetric-key cryptosystem is the better approach to manage symmetric key estimation. By this strategy they can doubly scramble and doubly translate the message. It infers the sender will create the figure content from the plain substance twice. The recipient will in like manner need to disentangle the figures for two times and a short time later the correspondence between them will be done. For making the key, they will take the message length in first encryption and in second encryption they will apply moving framework.

In 2013, Seetaiah Kilaru et al. [27] suggest that security is the guideline stress in any field. With the progressive strikes, it is a noteworthy test for the customers to secure the propelled pictures which are transmitting over web. Lone Value Decomposition (SVD) surrenders a response to a more noticeable degree. Maker recommends that by using the Wavelets, imperceptible watermark embed into the principal watermark. The major focus concentrated on the remote trades; in this manner it is imperative to think about some as segments into thought, they are size of a photo and essentials of information exchange limit. Keeping in context of each one of these parameters, weight and transmission should be done.

In 2012, Long Baoa et al. [28] proposed confused structure shows fabulous turbulent practices. To show its application in picture get ready, another picture encryption arrangement using the proposed cluttered system is moreover introduced. PC generation and security examination display that the proposed picture encryption arrangement shows marvelous encryption execution, high affectability to the security keys, and an enough gigantic key space to contradict the savage attack. Regardless, in this paper sporadic like nature of disorder is not considered.

In 2012, Abusukhon et al. [29] proposed a novel strategy for information encryption which can change record into a picture document on both sides of framework that is customer and server. They have broken down their calculation by investigating the quantity of all conceivable key stages.

In 2014, Mostaghim et al. [30] recommend making the visual cryptography more hearty which can ready to impart sent and the got information to the produced message and will consolidate to the got offer to uncover the shrouded message. Their proposed plan is assessed as far as Histogram, connection coefficient, key affectability and key space. Their outcomes are observed to be enhanced in contrast with the customary procedure.

In 2015, Hassan et al. [31] proposed a protected correspondence plan. It is a hyper disordered framework utilized as a bearer for the encoded information to be transmitted. At the transmitter end, two various disrupted structures are coupled and used to manufacture another hyper tumultuous system. One of the yields of the hyper disordered system is used as a carrier for the mixed data. At the not exactly alluring end, the discrete-time Regularized Least Square (RLS) estimator is used to redo the jumbled banner and thusly recoup the encoded data. Their propagation results are speaking to the suitability of the proposed procedure.

In 2015, Li et al. [32] coordinated the idea of session key foundation and broadened confused maps for the satisfaction to permit information senders and information recipients to build up a protected normal session key through a trusted server over a frail channel. They proposed a protected three-party confirmed key trade convention (3PAKE) which depends on amplified turbulent maps away administration without utilizing savvy card and timestamp. It requires neither long haul mystery keys nor symmetric cryptosystems. It satisfy the assurance

necessity against different assaults. Their proposed convention is more secure and commonsense for genuine situations.

In 2015, Haroun et al. [33] introduced a key era technique which depends on the remote blurring channels. It is utilized in view of the broadband turbulent sign for information transmission with the goal that it is recurrence specific. Their proposed estimation abuses this property to create a unique shared key between two social affairs. The no periodicity of the turbulent sign gives a phenomenal sign to key time, which can be used even with static obscuring channels. Their proposed philosophy is intense to timing contrasts between the social affairs in light of the way that the repeat scope of the signs is used. The key's anomaly is certified, and the effects of included substance white Gaussian uproar and timing contrasts on the figuring's execution are investigated. The key based security and analysis is also presented with the problems in [34, 35, 36].

In 2015, Zaher et al. [37] proposed a new technique for secure correspondence that goes for robustifying established Chaotic Shift Keying (CSK) methods. A novel cryptography calculation is utilized to change the transmitter parameters such that they have a fourfold frame; along these lines, breaking into people in general correspondence channel utilizing return map assaults will come up short. At the recipient side, a versatile control strategy is utilized to assess the time-differing transmitter parameters through receiving a complete synchronization approach. Reenactment results illustrate the prevalent execution of the proposed method in both time and recurrence spaces. It is utilized to fabricate the proposed framework utilizing just the time arrangement for the yield. Different implementation issues are investigated for various digital multimedia data and an experimental investigation is carried out to verify the effectiveness of the proposed technique.

In 2015, Kharat et al. [38] proposed a three differential mayhem based straightforward encryption and information concealing system in which first time confusion is utilized for position stage and esteem change .With the assistance of this calculation they can accomplish high security reason. Intricacy of calculation is lessened by disposing of any progression from calculation for low medium. In any case, with the assistance of result they have demonstrated that this calculation is best for any attack.

3.Analysis

There are a few cryptography algorithms are now examined and a few examination work are completed in this respect. Still there is an immense crevice and analysis is needed for a new cryptography methods have been found till now. The hybridization of encryption methods might be valuable in this bearing as they give effective encryption. In the event that the key randomization methodology is connected it will turn out to be all the more effective and to break it is intense. Taking into account the few examination work we have given the writing correlation the gap finding as appeared in table 1.

Table 1 Literature comparison

S. No	Author	Methodology	Results	Gap
1	[39]	Fractional-order discrete chaotic system	A viable transmission arrangement taking into record the discrete-time fragmentary solicitation tumultuous structure for private mechanized correspondences is proposed. The incomplete solicitation Modified-Henon aide is used. By changing the halfway demands appropriately, it has been exhibited that the fractional solicitation Modified-Henon system has a confounded behavior. The precise synchronization considering the put off onlooker is made.	Noise and channel robustness is not discussed.
2	[40]	Random Pixel Permutation using Chaotic Mapping	The association results got by scrambling illustration pictures show significant changes in regards to security when diverged from existing procedures.	Quantitate examination should be possible remotely too.
3	[41]	Network Security Management Based on	The implied strategy and study introduced recommend adventitious to the scope of	The other parameters like data synthesis

S. No	Author	Methodology	Results	Gap
		Qualitative Risk Analysis	various information appraisal. The administrate additional structures in the host's vitality occasion computation. These cross sections ask pardon the threat unambiguousness adaptable and versatile, which is totally useful in the dynamic thought of security.	should be improved.
4	[42]	Digital image security improvement by integrating watermarking and encryption technique	They have used blind watermark extraction technique for extraction of the watermark. They have checked robustness, perceptual quality and security of the proposed algorithm.	How the performance is evaluated and compared is missing.
5	[43]	A hybrid approach for image security by combining encryption and steganography	They have presented hybrid approach for image security that combines both encryption and steganography. The image is encrypted using new version of AES algorithm, which is then hided into cover image using the steganography concept.	They have claimed that this approach provides greater security against attacks. But the attacks are not classified.

4.Problem identification

The gaps identified from this survey and analyses are as follows:

1) Key length can be expanded so that it can enhance the key security as compared to the traditional techniques.
2) Hybridization of different standard encryption techniques can be applied for the betterment.
3) There is the need of RGB based comparison and evaluation of images.
4) Information loss should be minimized.
5) Data hiding techniques with bit shuffling can be applied for enhancing the security.

5.Conclusion and future work

In this paper we have talks about a few parts of cryptography and steganography with their working drew closer and upgrades. In view of this analysis and review we have recommended encryption method like the combination of RSA and RC6. It is ideal to half breed distinctive encryption procedure. The expanding size of key with arbitrary characteristic is additionally a superior and effective security change.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Mitra A, Rao YS, Prasanna SR. A new image encryption approach using combinational permutation techniques. International Journal of Computer Science. 2006; 1(2):127-31.
[2] Elbirt AJ, Paar C. An instruction-level distributed processor for symmetric-key cryptography. IEEE Transactions on Parallel and Distributed Systems. 2005; 16(5):468-80.
[3] Diffie W, Hellman ME. New directions in cryptography. IEEE Transactions on Information Theory. 1976; 22(6):644-54.
[4] Stallings W. Cryptography and network security, 4/E. Pearson Education India; 2006.
[5] Beşdok E. Hiding information in multispectral spatial images. AEU-International Journal of Electronics and Communications. 2005; 59(1):15-24.
[6] Trivedi S, Chandramouli R. Secret key estimation in sequential steganography. IEEE Transactions on Signal Processing. 2005; 53(2):746-57.
[7] Sahu J. Design a New Methodology for Removing Fog from the Image. International Journal of Advanced Computer Research. 2012; 2(7): 62-5.
[8] Wu YT, Shih FY. An adjusted-purpose digital watermarking technique. Pattern Recognition. 2004; 37(12):2349-59.
[9] Bani Younes MA, Jantan A. Image Encryption Using Block Based Transformation Algorithm. IAENG International Journal of Computer Science. 2008; 35(1): 407-15.
[10] Nanavati SP, Panigrahi PK. Wavelets: applications to image compression-I. Resonance. 2005; 10(2):52-61.
[11] Gonzalez RC, Woods RE. Digital image processing. Prentice Hall, 2002.

[12] Vitali AL, Borneo A, Fumagalli M, Rinaldo R. Video over IP using standard-compatible multiple description coding: an IETF proposal. Journal of Zhejiang University SCIENCE A. 2006; 7(5):668-76.
[13] Chauhan N, Waoo AA, Patheja PS. Attack Detection in watermarked images with PSNR and RGB Intensity. International Journal of Advanced Computer Research.2013; 3(9): 41-5.
[14] Voyatzis G, Nikolaidis N, Pitas I. Digital watermarking: an overview. In ninth european signal processing conference signal processing IX, theories and applications: proceedings of Eusipco-98, Rhodes, Greece 1998 (pp. 8-11).
[15] Joshi S, Jain P. A secure data sharing and communication with multiple cloud environments with java API. International Journal of Advanced Computer Research.2012; 2(4):135-43.
[16] Sinha A, Singh K. A technique for image encryption using digital signature. Optics Communications. 2003; 218(4):229-34.
[17] Li S, Li C, Chen G, Zhang D, Bourbakis NG. A general cryptanalysis of permutation-only multimedia encryption algorithms. IACR's Cryptology ePrint Archive: Report. 2004.
[18] Bhalshankar S, Gulve AK. Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes. arXiv preprint arXiv:1509.02630. 2015.
[19] Khanapur NH, Patro A. Design and Implementation of Enhanced version of MRC6 algorithm for data security. International Journal of Advanced Computer Research. 2015; 5(19): 225-32.
[20] Manajaih DH. Modular arithmetic in RSA cryptography. International Journal of Advanced Computer Research. 2014; 4(4):973-78.
[21] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering (CONSEG) 2012 (pp. 1-8). IEEE.
[22] Tavse P, Khandelwal A. A critical review on data clustering in wireless network. International Journal of Advanced Computer Research. 2014; 4(3):795-8.
[23] Nath A, Basu D, Bhowmik S, Bose A, Chatterjee S. Multi way feedback encryption standard ver-2 (MWFES-2). International Journal of Advanced Computer Research. 2013; 3(13):28-34.
[24] Shukla N. Data mining based result analysis of document fraud detection. International Journal of Advanced Technology and Engineering Exploration. 2014; 1(1):21-5.
[25] Guan ZH, Huang F, Guan W. Chaos-based image encryption algorithm. Physics Letters A. 2005; 346(1):153-7.
[26] De PS, Maiti P. DEDD symmetric-key cryptosystem. International Journal of Advanced Computer Research.2013; 3(8):171-6.
[27] Kilaru S, Kanukuntla Y, Chary KB. An effective algorithm for Image security based on compression and decomposition method. International Journal of Advanced Computer Research. 2013; 3(8):289-94.
[28] Bao L, Zhou Y, Chen CP, Liu H. A new chaotic system for image encryption. In international conference on system science and engineering (ICSSE) 2012 (pp. 69-73). IEEE.
[29] Abusukhon A, Talib M. A Novel network security algorithm based on private key encryption. In international conference on cyber security, cyber warfare and digital forensic (CyberSec) 2012 (pp. 33-7). IEEE.
[30] Mostaghim M, Boostani R. CVC: Chaotic visual cryptography to enhance steganography. In 11th international ISC conference on information security and cryptology (ISCISC) 2014 (pp. 44-8). IEEE.
[31] Hassan MF. Synchronization of hyperchaotic systems with application to secure communication. In 9th annual IEEE international systems conference (Sys Con) 2015 (pp. 121-6). IEEE.
[32] Li CT, Lee CW, Shen JJ. A secure three-party authenticated key exchange protocol based on extended chaotic maps in cloud storage service. In international conference on information networking (ICOIN) 2015 (pp. 31-6). IEEE.
[33] Haroun MF, Gulliver TA. Secret key generation using chaotic signals over frequency selective fading channels. IEEE Transactions on Information Forensics and Security. 2015; 10(8):1764-75.
[34] Shrivastava A, Singh L. A new hybrid encryption and steganography technique: a survey. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(14):8-13.
[35] Singhai P, Shrivastava A. An efficient image security mechanism based on advanced encryption standard. International Journal of Advanced Technology and Engineering Exploration. 2015; 2(13): 175-82.
[36] Deshmukh P, Rai Y, Kushwaha S. Identifying malicious behavior in MANET: a survey. International Journal of Advanced Technology and Engineering Exploration. 2015; 2(4):43-8.
[37] Zaher AA. A cryptography algorithm for transmitting multimedia data using quadruple-state CSK. In international conference on computer, communications, and control technology (I4CT) 2015 (pp. 87-92). IEEE.
[38] Kharat PH, Shriramwar SS. A secured Transmission of data using 3D chaotic map encryption and data hiding technique. In international conference on industrial instrumentation and control (ICIC) 2015 (pp.1243-47). IEEE.
[39] Hamiche H, Kassim S, Djennoune S, Guermah S, Lahdir M, Bettayeb M. Secure data transmission scheme based on fractional-order discrete chaotic system. In 3rd international conference on control, engineering & information technology (CEIT) 2015 (pp. 1-6). IEEE.
[40] Sathishkumar GA, Ramachandran S, Bagan KB. Image encryption using random pixel permutation by chaotic mapping. In IEEE symposium on computers & informatics (ISCI) 2012 (pp. 247-51). IEEE.
[41] Rahman MA, Al-Shaer E. A formal approach for

network security management based on qualitative risk analysis. In international symposium on integrated network management 2013 (pp. 244-51). IEEE.

[42] Metkar SP, Lichade MV. Digital image security improvement by integrating watermarking and encryption technique. In IEEE international conference on signal processing, computing and control (ISPCC) 2013 (pp. 1-6). IEEE.

[43] Saini JK, Verma HK. A hybrid approach for image security by combining encryption and steganography. In second international conference on image information processing (ICIIP) 2013 (pp. 607-11). IEEE.