International Journal of Advanced Technology and Engineering Exploration, Vol 3(14)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2016.314005

Review Article

A new hybrid encryption and steganography technique: a survey

Apoorva Shrivastava[1*] and Lokesh Singh[2]
M.Tech Student, Computer Science, T.I.T, Bhopal[1]
Assistant Professor, Computer Science, T.I.T, Bhopal[2]

Abstract
Security in data communication is a very important concern today. It is used in almost every region like e-commerce, education, and industry and data warehouse. Securely sending and receiving data in the above area is an important as the data is crucial. Maintain the security become tough as the data inherent characteristics are also different. So the main focus of this paper is to study and discuss the trends which are already been proposed in the direction of cryptography and steganography. The gap identification have been provided by this study and based on the identification future suggestions have been provided.

Keywords
Encryption, Chaos, Steganography, Security Measures.

1.Introduction
With the fast improvements and the data interchanges, a lot of concerns have been brought up in the security of information transmitted or put away over open channels. Particularly at the level of text and picture information. As indicated by [1] there are three fundamental routines for secured correspondence accessible, in particular, cryptography, steganography and watermarking. Among these three, the first one, cryptography [2]-[4], manages the improvement of procedures for changing over data in the middle of understandable and incomprehensible structures amid data trade. Steganography [5]-[6], then again, is a procedure for concealing and separating data to be passed on utilizing a transporter signal [1]. The third one, watermarking [7]-[8], is a method for creating legitimate strategies for concealing restrictive data in the perceptual information. In [9] authors have recommended that the vast majority of the common pictures, the neighboring's estimations pixels are unequivocally associated (i.e. the estimation of any given pixel can be sensibly anticipated from the estimations of its neighbors [10]-[12]. So keeping in mind the end goal to accomplish the higher relationship entropy among pixels and expanding the entropy quality is a developing examination range.

In case of text the data should be hiding with images so that more security will impose with RGB combinations and variations.

In [13] the most critical issues, which influence the mainstream data of advanced media, are the way to secure theft and possession. The watermarking of the prevalent methodologies consider ding as a new database for giving the copyright insurance, is a procedure in view of implanting a particular imprint or mark into the computerized items. While a few watermarking calculations have been proposed [14] in this heading.

So in the ensuing segment we talk about data Encryption method for picture encryption. We additionally talk about the pivotal angles which are utilized as a part of picture encryption with their points of interest and drawbacks. At long last taking into account the discourses we additionally recommend some future comment which may be productive in this bearing.

There are numerous essential techniques which are second-hand pervasive cryptography, for example, private or mystery key cryptography, open fundamental or kilter, computerized mark, and hash capacities [15]. In private key cryptography, a solitary key is leftover for both encryption and decoding. This obliges meander if all else fails part convey offering an impersonation of the key and the key be struck by be passed swear off a safe channel

*Author for correspondence

to the next individual [13-22]. Private-key calculations are level indestructible and effectively actualized in equipment. Along these lines they are over and again second-hand for mass measurements encryption. The vast please of the all-around adjusted encryption rely on upon plaintext, encryption calculation, key and unscrambling calculation. The plaintext is the size ahead requiring the encryption calculation. It is joining of the inputs to the encryption calculation. The encryption calculation is the calculation used to continue on b deal with the information stranger plaintext to figure relieve. The mystery key is a comparable to repel of the encryption calculation and of the plaintext and it is associate of the encryption's inputs calculation [23][24]. The figure content is the defiant content discover as yield [14][15]. The steganography technique with cryptography will enhance the security as the cryptic content and the randomization quality can be improved.

2.Literature survey

In 2005,Zhi-Hong Guan et al. [25] have introduced another picture encryption plan, in which rearranging the positions and changing the dark estimations of picture pixels are joined to confound the relationship between the figure picture and the plain picture.

In 2013, Praloy Shankar De et al. [26] endeavor has been made to concentrate on a calculation of cryptography that was made by utilizing old philosophies. DEDD Symmetric-key cryptosystem is the new way to deal with symmetric key calculation. By this technique they can doubly scramble and doubly decode the message. It implies the sender will produce the figure content from the plain content twice. The beneficiary will likewise need to decode the figures for two times and afterward the correspondence between them will be finished. For creating the key, they will take the message length in first encryption and in second encryption they will apply moving system.

In 2013, Seetaiah Kilaru et al. [27] propose that security is the principle worry in any field. With the successive assaults, it is a major test for the clients to secure the advanced pictures which are transmitting over web. Solitary Value Decomposition (SVD) gives an answer up to a more prominent degree. Creator proposes that by utilizing the Wavelets, undetectable watermark insert into the first watermark. The fundamental center focused on the remote interchanges; subsequently it is vital to think of some as components into thought, they are size of a picture and prerequisites of data transfer capacity. Keeping in perspective of every one of these parameters, pressure and transmission ought to be finished.

In 2012, Long Baoa et al. [28] proposed disordered framework indicates fantastic turbulent practices. To exhibit its application in picture preparing, another picture encryption plan utilizing the proposed disordered framework is likewise presented. PC reproduction and security investigation exhibit that the proposed picture encryption plan indicates phenomenal encryption execution, high affectability to the security keys, and an adequately huge key space to oppose the savage assault. In any case, in this paper irregular like nature of disarray is not considered.

In 2012, Abusukhon et al. [29] proposed a novel method for data encryption which is able to transformation file into an image file on both sides of system that is client and server. They have analyzed their algorithm by exploring the number of all possible key permutations.

In 2014, Mostaghim et al. [30] suggest making the visual cryptography more robust which can able to share sent and the received data with the generated message and will combine to the received share to reveal the hidden message. Their proposed scheme is evaluated in terms of Histogram, correlation coefficient, key sensitivity and key space. Their results are found to be improved in comparison to the traditional technique.

In 2015, Hassan et al. [31] proposed a secure communication scheme. It is a hyperchaotic system used as a carrier for the encoded data to be transmitted. At the transmitter end, two diverse disorganized frameworks are coupled and used to build another hyperchaotie framework. One of the yields of the hyperehaotie framework is utilized as a bearer for the scrambled information. At the less than desirable end, the discrete-time Regularized Least Square (RLS) estimator is utilized to remake the disorderly flag and consequently recover the encoded information. Their reproduction results are representing the viability of the proposed methodology.

In 2015, Li et al. [32] integrated the concept of session key establishment and extended chaotic maps for the fulfillment to allow data senders and data receivers to establish a secure common session key

through a trusted server over an insecure channel. They proposed a secure three-party authenticated key exchange protocol (3PAKE) which is based on extended chaotic maps in storage service without using smart card and timestamp. It requires neither long-term secret keys nor symmetric cryptosystems. It fulfill the protection requirement against various attacks. Their proposed protocol is more secure and practical for real environments.

In 2015, Haroun et al. [33] presented a key generation method which is based on the wireless fading channels. It is employed based on the broadband chaotic signal for data transmission so that it is frequency selective. Their proposed calculation misuses this property to produce an one of a kind shared key between two gatherings. The no periodicity of the turbulent sign gives an extraordinary sign to key era, which can be utilized even with static blurring channels. Their proposed methodology is powerful to timing contrasts between the gatherings in light of the fact that the recurrence range of the signs is utilized. The key's irregularity is affirmed, and the impacts of added substance white Gaussian clamor and timing contrasts on the calculation's execution are inspected.

3.Analysis

There are several cryptography algorithms are already discussed and several research work are carried out in this direction.Still there is a huge gap and research are left in this direction as several new cryptography techniques have been discovered till now. The hybridization of encryption techniques may be useful in this direction as they provides powerful encryption . If the key randomization procedure is applied it will become more powerful and to break it is tough. Based on the several research work we have presented the literature comparison with the gaps finding as shown in *Table 1*.

Table 1 Literature comparison

S. No	Author	Methodology	Results	Gap
1	[34]	Quadruple-State Chaotic Shift Keying (CSK)	The proposed configuration can be effectively amplified to other media signals and other streams. It inserted data into a solitary vector that jam the time scale and the size of these signs.	How to hide the data with other sources is not included.
2	[35]	3D chaotic map encryption	They implement three non linier differential chaos based encryption technique. For the data hiding binary forms embedded into encrypted image by using least significant bit algorithm.	How to apply to other information field is missing.
3	[36]	Fractional-order discrete chaotic system	An effective transmission plan taking into account the discrete-time fragmentary request tumultuous framework for private computerized correspondences is proposed. The partial request Modified-Henon guide is utilized. By changing the partial requests properly, it has been demonstrated that the partial request Modified-Henon framework has a confused conduct. The accurate synchronization taking into account the postponed eyewitness is composed.	Noise and channel robustness is not discussed.
4	[37]	Logistics based Encryption algorithm.	Their method of watermarking has efficient PSNR value retrieved and comparable similarity measurer in comparison to the related methods of this group.	What is the relevant size of the images are not discussed.
5	[29]	Encryption method based on transformation of a text file into an image file on both client and server machines.	It is moreover profitable for text data through regardless of all around messages put away in the form of divided pictures and in this way regardless of the fact that somebody leaves the email page on it is troublesome for others to figure the	How to Set the felicity into blocks and now affect each block into an image and thus create individual key for each block is not

S. No	Author	Methodology	Results	Gap
			significance (the first content) of these pictures.	determined.
6	[38]	Data Encryption Standard (DES) using 64 bit block size of plaintext & 56 bits of Secrete key.	It changes the intensity of the pixels so the safety of the encryption scheme is improved.	There is a scope for improvement as there are several new and strong encryption methods have been proposed.
7	[39]	Gray Image Encryption Scheme by Discrete Logarithm with Logistic and HEH64 Chaotic Functions	It is useful for the huge dark level Pictures. It holds better results in crypto examination assault, and brute force attack.	There is a scope of minimization of Information loss.
8	[40]	Random Pixel Permutation using Chaotic Mapping	The connection results got by scrambling example pictures demonstrate noteworthy changes regarding security when contrasted with existing strategies.	Quantitate examination should be possible remotely too.
9	[41]	Network Security Management Based on Qualitative Risk Analysis	The purported method and study presented suggest adscititious to the range of different data assessment. The administrate extra frameworks in the host's essentialness event calculation. These lattices ask pardon the danger unambiguousness flexible and movable, which is completely helpful in the dynamic idea of security.	The other parameters like data synthesis should be improved.

4.Problem identification

After the study and analysis of the research paper the following gaps are identified:

1) The need of multi-level key security with random key generation is arises so that the data security will become more robust.
2) Data partitioning is needed based on subset and super set approach so that level wise security can be applied to make the hacker unreachable [42].
3) The length of the key should be maximized up to 256 to 512 bytes.
4) RGB Entropy should be randomized to change the pixel positions.
5) The combination of cryptography with steganography is a stronger way to enhance the security.
6) The uses of steganography methods with the help of image encryption enhance the retrieval complexity.

5.Conclusion and future work

In this paper we have discusses several aspects of cryptography and steganography with their working approached and enhancements. Based on the analysis and observations we have suggested encryption technique like RC6. It would be better to hybrid different encryption technique. The increasing size of key with random attribute is also a better and powerful security improvement.

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] William S, 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] Wu Y. On the security of an SVD-based ownership watermarking. IEEE Transactions on Multimedia. 2005; 7(4):624-7.
[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):15-23.
[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. Publishing House of Electronics Industry. Beijing, China. 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(1):41-5.
[14] Voyatzis G, Nikolaidis N, Pitas I. Digital watermarking: an overview. Ninth European signal processing conference, 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 e-Print Archive: Report. 2004; 374(2004):1-20.
[18] Bhalshankar S, Gulve AK. Audio steganography: LSB technique using a pyramid structure and range of bytes. International Journal of Advanced Computer Research. 2015; 5(20); 233-48.
[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):973-8.
[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. CSI sixth international conference in 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(16):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 (IJATEE). 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. 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. 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. International ISC conference in information security and cryptology (ISCISC) 2014 (pp. 44-8). IEEE.
[31] Hassan MF. Synchronization of hyperchaotic systems with application to secure communication. In 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 M, Gulliver T. Secret key generation using chaotic signals over frequency selective fading channels. IEEE Transactions on Information Forensics and Security. 2015; 10(8):1764-75.
[34] 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.
[35] 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.
[36] Hamiche H, Kassim S, Djennoune S, Guermah S, Lahdir M, Bettayeb M. Secure data transmission scheme based on fractional-order discrete chaotic system. In international conference on control, engineering & information technology (CEIT) 2015 (pp. 1-6). IEEE.
[37] Sethi N, Sharma D. A new cryptology approach for image encryption. In international conference on parallel, distributed and grid computing 2012 (pp. 905-8). IEEE.
[38] Ramaiya MK, Hemrajani N, Saxena AK. Improvisation of security aspect in steganography

applying DES. In international conference on communication systems and network technologies (CSNT) 2013 (pp. 431-6). IEEE.

[39] Paul A, Das N, Prusty AK. An advanced gray image encryption scheme by using discrete logarithm with logistic and HEH64 chaotic functions. In IEEE 3rd international advance computing conference (IACC) 2013 (pp. 1114-20). 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 (IM 2013) 2013 (pp. 244-51). IEEE.

[42] Dubey AK, Dubey AK, Agarwal V, Khandagre Y. Knowledge discovery with a subset-superset approach for mining heterogeneous data with dynamic support. In CSI sixth international conference on software engineering (CONSEG) 2012 (pp. 1-6). IEEE.