Multi Encryption and Block Cipher Techniques for Image Encryption: A Review

Srishti Sharma[1], Ankit Arora[2]
[1]M.Tech (CTA) Scholar, [2]Assistant Professor
[12]Department of CSE, Vishwavidyalaya Engineering College Lakhanpur,
Sant Gahira Guru Vishwavidyalaya, Sarguja, Ambikapur, Chhattisgarh, India

Abstract- This paper presents a comprehensive survey on multiple encoding and blocks cipher image secret writing schemes. among the fashionable time, because of the fast development of data communication and transmission application, security becomes an important issue of communication, storage and transmission of digital info like image, audio and video. Image secret writing has been a most well-liked analysis field in recent decades. Secret writing technique ar utilized in many fields like bioscience, military, geographic satellite pictures. we tend to provides a short summary of regular key block cipher for various algorithms given during this field in keeping with classified it in cryptography wherever we tend to classified into classes.

Keywords- *Block Cipher, Image Encryption, Multiple Encryption, image division, Secure image Transmission.*

I. INTRODUCTION

In the previous couple of days hugely growth of digital and transmission technology, image protection has become AN important issue for communication of digital pictures through the networks and secret writing is that the one in every of approaches to supply the protection of digital pictures. Image secret writing is that the technique of remodeling information mistreatment AN rule to form it unclear to anybody while not those possessing specific data, typically remarked as a key. In1970s,Chaos construct was planned, that was employed in a good vary of analysis areas, like arithmetic, engineering, physics, biology, and then on[1]. The difficult behavior of chaotic structures in nonlinear settled was delineate. the primary description of a chaotic techniques was created in 1963 via Lorenz[2], WHO developed a system grasp because the animal scientist attractor that coupled nonlinear differential equations.

Cryptography aims to realize the data security necessities as privacy or confidentiality, information integrity, authentication, non-repudiation and access management [4]. Cryptography it's the foremost vital thanks to shield many applications that required to be transmit quickly with a high level of security like pictures, text, voice and video[5]. Modern cryptography divided into symmetric key that uses one key in secret writing and coding, and uneven key (public key) that uses 2 totally different keys in secret writing method. typically symmetric key quicker than uneven key. mistreatment symmetric key cryptography will communicate 2 folks throughout secure channel, wherever to contact 2 folks across secure channel should initial agree on a secret key shared in between them [6].Symmetric-key cryptography classified into stream cipher and block cipher. during this paper can involved with symmetric key block cipher that operative on fastened length of bits divided into separate blocks of fastened size (for example, 32, 56, 64, 128, etc.) [7] such as DES and AES rule that are selected cryptography customary.

In this paper we've got planned a review on multiple secret writing techniques applied on pictures and transmission information. Here, we tend to target block cipher and multiple secret writing techniques of secret writing solely.

II. LITERATURE REVIEW

Sud, K.K. et.al.[8] during this document a brand new approach for image cryptography supported chaotic supplying maps to fulfill the necessities of secure image transfer. within the scientific discipline theme of the planned image, associate external 80-bit secret key and 2 chaotic supplying maps area unit used. Samsudin et.al.[9] planned a brand new algorithmic program of image cryptography supported the elliptical map of Jacobian was studied. This work is that the 1st commit to explore the elliptical maps of Jacobian as a cryptosystem. Experimental results and safety analysis indicate that the scientific discipline algorithmic program supported the chaotic elliptical map is advantageous from the purpose of read of huge key areas and a high level of security. The Electronic Cod Book (ECB) is settled mode of operation thought-about the foremost common means in ciphering a message. the most advantage of this mode, it's that the synchronization among secret writing and decipherment isn't necessary, during this case once the receiver not received all encrypted blocks as a result of occur issues in transmission method, the recipient will solely decode the received blocks with none downside. ECB mode provides high speed in implementation as a result of ECB mode operate parallel in ciphering process[10]. The Cipher Block Chaining (CBC) mode and also the Cipher Feedback (CFB) mode were build the blocks of cipher text hooked in to all the previous blocks of plain text through ciphering method [11]. B.V.Rama devi et al. planned a way

that|during which|within which} the image which is to be transmitted is remodeled into a sequence referred to as Gödel range Sequence (GNS) employing a new technique referred to as Godelization [12]. Sesha Pallavi Indrakanti et.al.proposes a brand new image secret writing algorithmic program supported random constituent permutation with the motivation to take care of the standard of the image. The technique involves 3 completely different phases within the secret writing method. the primary section is that the image secret writing. The second section is that the key generation section. The third section is that the identification process[13]. [14] Ahmed Bashir Abugharsa at el. proposes a brand new algorithmic program. the primary a part of the algorithmic program aims to create a shifted table victimization hash operate inside secret writing section associated decipherment section to get an encrypted (shifted) image and also the original image. The second part of the algorithmic program uses the shifted table resulted from the primary part of the algorithmic program to get new shifted image (Encrypted) during which the rows and also the columns of the initial image area unit shifted and followed by secret writing technique to extend the protection of the image secret writing. Aditee Gautam, Meenakshi Panwar at el. discusses a block primarily based transformation algorithmic program during which image is split in to range of blocks. These blocks area unit remodeled before surfing associate secret writing method. At the receiver facet these blocks area unit retransformed in to their original position and performed a decipherment method which supplies the initial image[15]. associate secret writing technique to introduce the watermarking plan to encourage the protection was planned by mohammad Reza Keyvanpour, Famoosh Merrikh-Bayat . during this paper, a secure watermarking technique is employed that relies on the thought of writing the form image and applying the chaos operate. Here rearranging the position of image pixels were distributed by victimization the Arnold's Cat Map technique to possess a decent vary of security. additionally the chaotic pictures area unit divided into vary of blocks and domain of blocks to spot the self-similarity feature[16].

John Justin M, Manimurugan S., at el. focuses primarily on the various sorts of secret writing techniques that area unit existing, and framing all the techniques along as a literature survey. Aim an intensive experimental study of implementations of varied offered secret writing techniques. additionally focuses on image secret writing techniques, data secret writing techniques, double secret writing and Chaos-based secret writing techniques[17]. Amnesh Goel et. al planned this system. They slice the image into n elements and perform secret writing in every elements. to feature to the protection, this technique additionally iatrogenic the shuffling of the custom slices by lay dynamical the situation of those slices from its actual image place location to completely different location continuation the shift algorithmic program with the new arrangement of the slices[18]. Rawat A. et.al. [aims at rising the protection and potency of image secret writing by employing a extremely economical shuffle primarily based secret writing algorithmic program and a similar decipherment algorithmic program supported random values obtained by victimization pseudorandom range generator[19].

TABLE 1 PROBLEM IDENTIFICATION

Refer-ence	***Description***	***Problem Identified***	***Proposed Solution***
[13]	Uses random pixel permutation with motivation to maintain the quality of the image. The values used in the encryption process are preserved in the form of a 64 bit key and sent to the receivers.	Quality of the image decreases after decryption process.	A lossless encryption and decryption technique may be use full in such cases
[19]	Uses a highly efficient shuffle based encryption algorithm and an equivalent decryption algorithm based on random values obtained by using pseudorandom number generator.	More complex random number generator needed	Can generate using hash function
[20]	They proposed a method which includes pixels shuffling in rows and columns using two key vectors and then Zeta Function is used to further scramble the image. It is based on Rubiks Cube Principle	Tested on gray scale image only	Can apply to multi dimension images by de channalize the input image

III. DIFFERENT ENCRYPTION TECHNIQUES

A. Secret key cryptography

It is otherwise called symmetric key cryptography. With this kind of cryptography, both the sender and the collector know a similar mystery code, called the key. Messages are encoded

by the sender utilizing the key and unscrambled by the collector utilizing a similar key.

B. Public key cryptography

It is also called asymmetric key cryptography, uses a combination of keys for coding and decoding. With public key cryptography, keys used as a pairs of matched public and personal keys.

C. Substitution Techniques for Encryption

In substitution techniques the alphabets of input text are replaced by are substituted by different alphabets and numbers.If we see the plaintext as the sequence of bits then to generate the ciphertext these bits are replaced by some other bits.

D. Caesar Cipher

This is among one of the most famous substitution technique in this technique the alphabets of input text is replaced by a new alphabet which are exactly at distance 3 in alphabet table.

Plain text: are you ready
Cipher text: DUH BRX UHDGB

if we want to replace the alphabet with number corresponding to same position of alphabet then this method can be represent by following formula

$$c = E(3, p) = (p + 3) \bmod 26 \quad (1)$$

Where, E denotes the encryption. Here, mod represents the modulo division, which generates the reminders after performing division. We are apparently assuming case-insensitive encoding with the Caesar cipher.

This equation can be modified for any number of position shifting (k) as

$$c = E(k, p) = (p + k) \bmod 26 \quad (2)$$

The formula for decryption would be

$$p = D(k, c) = (c - k) \bmod 26 \quad (3)$$

In all formulas k represents the secrete key, E represents the Encryption process and D represents the Decryption process.

E. The Hill Cipher

The Hill cipher technique is based on the linear algebra, and it can be applied only if user have sufficient knowledge of matrix operations. It also uses modulo division, so it is completely based on mathematical calculations. However, it can be applied easily on large number of letters in less time. Hill cipher is a very different multiple letter substitution technique, in which number is assigned to each alphabet and then it creates 2*2 or 3*3 matrix for further process.

F. Symmetric-Key Block Cipher

Symmetric-key block ciphers are created from 2 algorithms E (Encryption) and D (Decryption) and every one these algorithms takes n bits' plaintext as input and offers precisely the equal range of bits as output by using k bits' secret key. Mode of operation ways in which of victimization block cipher for encoding, wont to apply block ciphers to larger plaintexts. here, Mode operation classified into settled and probabilistic.

G. Data Encryption Standard (DES)

DES is encryption normal design by IBM and regarded one amongst the foremost necessary algorithms, printed by National Institute of Standards and Technology and becomes a standard in 1974. DES structure consists of 64-bits input plain text and 64-bits output cipher texts and supported 56-bits key length [21]. Zibdeh et al. (2011) given a brand new modified DES algorithms (data encoding standard) to create it secure to the bit errors caused by the wireless networks. The changed algorithmic program improves the bit error rate (BER) performance as well as security compared to DES[22].

H. Substitution-Permutation Networks (SPN)

Substitution Permutation Network is another Method used for encryption. Substitution Permutation Network initial introduced by Feistel et al (1975) refert to as SPN. SPN is series of mathematical operations utilized in block cipher. Substitution- permutation network consisting of a sequence of rounds of substitutions known as S-boxes and connected by bit position permutations or transpositions [23] [24].

I. Advanced Encryption Standard (AES)

AES is the most widely used symmetric cipher. In 1997 call for AES by NIST, The method contains block size of 128-bits and supported three different lengths of keys i.e. 128 bit key, 192 bit key and 256 bit key. AES block cipher is efficiency in software and hardware, several industry and commercial systems include AES such as Internet security standard IPsec, IEEE 802.1, SSH (secure shell), etc. [25]. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen .In October 2, 2000 Rijndael's method was selected as the AES algorithm, Jamil, T. (2004) Presented paper about a new advanced encryption standard (AES) called Rijndael's algorithm approved by NIST. The Rijndael's algorithm processes blocks of size 128,192 or 256 bits and supports symmetric keys of size 128,192 or 256 bits and note that Rijndael's algorithm supporting larger key size than DES (Data Encryption Standard) supports. The Rijndael's rule consists of 3 steps initial round referred to as Add round Key, normal round consists of 4 transformations: Sub byte, Shift Row, combine Column and Add round Key, and {also the} final round also consists of Sub byte, Shift Row and Add round Key however not including the mix Column transformation. In overall performance, supported speed of encryption/decryption method and key set-up time. This algorithmic rule will apply in many applications like smart cards and different applications that required to storing and protective sensitive data from unauthorized access [26].

IV. CONCLUSION

As the use of transmission and storing pictures using digital techniques are increasing, it becomes an important concern that how to conserve the confidentiality, credibility and integrity of pictures. Secure and economic data transmission is the need of the today's world. Security of the digital pictures became an important issue since the communications of digital products over open network started occurring often. This paper reviews the present works on varied block cipher and permutation based encrypting techniques for image. we here conclude that the techniques square measure helpful for period systems and appropriate for applications. associate array of simulation tests done square measure compared with several necessary work in image cryptography field to prove the performance and security of the algorithms together with differential, statistical analysis and less execution time shows that these methods can perform better for encryption purpose.

V. REFERENCES

[1]. H.L.Mandoria,Samridhi Singh et al(2017)" A Review on Image Encryption Technique and to Extract Feature from Image" IJCA International Journal of Computer Application.

[2]. Asia Mahdi, Naser Alzubaidi, "Selective Image Encryption with Diffusion and Confusion Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) - Volume 4, Issue 7, July 2014.

[3]. Coron, J.-S, "What is cryptography?", Security & Privacy, IEEE (Volume:4, Issue: 1), pp. 70- 73, 2006

[4]. William stalling, "Cryptography and Network Security", 2011

[5]. Ali M Alshahrani and Prof. Stuart Walker, "New Approach in Symmetric Block Cipher Security Using a New Cubical Technique", International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 1, February 2015

[6]. Hans Delfs, Helmut Knebl, "Symmetric-Key Encryption", Springer Berlin Heidelberg, Introduction to Cryptography, Information Security and Cryptography, pp. 11-31, 2007

[7]. Thomas W. Cusick and PantelimonStanica, "Cryptographic Boolean Functions and Applications", Academic Press, 2009

[8]. Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image & Vision Computing, 24(9), 926-934.

[9]. Behnia, S., Akhavan, A., Akhshani, A., & Samsudin, A. (2013). Image encryption based on the jacobian elliptic maps. Journal of Systems & Software, 86(86), 2429-2438.

[10]. C. Paar and Pelzl, Jan, "Understanding Cryptography, A textbook for students and Practitioners",Copyright Springer-Verlag , pp. 125

[11]. Eli Biham, "On modes of operation", Fast Software Encryption, Lecture Notes in Computer Science Volume 809, pp. 116-120, 1994.

[12]. B.V.Rama Devi, D.Lalitha Bhaskari, P.Prapoorna Roja, P.S.Avadhani "A New Encryption Method for Secure Transmission of Images", (IJCSE)
Internation Journal on Computer Science and Engineering Vol.02,No.09,2010,2801-2804.

[13]. Sesha Pallavi Indrakanti , P.S.Avadhani,ll Permutation based Image Encryption Techniquell, International Journal of Computer Application (0975-8887)volume 28-No.8,2011.

[14]. Ahmed Bashir Abugharsa et. Al. "A New Image Encryption Approach using Block-Based on Shifted Algorithm", 2011, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.12, December 2011, pp 123-126.

[15]. Aditee Gautam, Meenakshi Panwar at el. *"A New Image Encryption Approach Using Block Based Transformation Algorithm",* (Ijaest) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 8, Issue No. 1, 090 - 096 *2011*.

[16]. Mohammad Reza Keyanpour, Famoosh Merrikh-Bayat, "A New Encryption Method for Secure Embedding in Image Watermarking", IEEE Transactions on Advanced Computer Theory & Engineering pp. 403-407, 2011.

[17]. A. N. Pisarchik and M. Zanin, "*Image Encryption with Chaotically Coupled Chaotic Maps,"* Physica D, 237, 20, pp. 2638–2648, 2008.

[18]. Amnesh Goel, Reji Mathews and Nidhi Chandra "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887) Volume 36– No.3, December 2011.

[19]. Aditya Rawat, Ipshita Gupta, Yash Goel, Nishith Sinha," Permutation Based Image Encryption Algorithm using Block Cipher Approach" 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE,2015.

[20]. Zaheer Abbas Balouch, Muhammad Imran Aslam, Irfan Ahmed," Energy Efficient Image Encryption Algorithm" IEEE, 2017.

[21]. Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[22]. Zibideh, W.Y.; Matalgah, Mustafa M. "Modified DES encryption algorithm with improved BER performance in wireless communication," Radio and Wireless Symposium (RWS), 2011 IEEE, pp.219-222, Jan. 2011.

[23]. Howard M. Heys, Stafford E. Tavares,"Substitution-permutation networks resistant to differential and linear cryptanalysis", Journal of Cryptology, March 1996, Volume 9, Issue 1, pp. 1-19

[24]. H. Feistel, W. A. Notz, and J. L. Smith. Some cryptographic techniques for machine-to-machine datacommunications. Proceedings of the IEEE, Vol.63 (Issue 11): pp.1545–1554, 1975

[25]. Paar, Christof, Pelzl, Jan, "The Advanced Encryption Standard (AES)" Understanding Cryptography, A textbook for students and Practitioners", Copyright Springer-Verlag, Pages 87-121

[26]. Jamil, T. "The Rijndael algorithm" Potentials, IEEE (Volume:23, Issue: 2) pp. 36 – 38, 2004