NOVEL BLOCK BASED ALGORITHM FOR EFFICIENT IMAGE ENCRYPTION

Ashima Trehan[1], Saranjeet Singh[2]
[1]M.Tech Scholar, Electronics and Communication, Galaxy Global Group of Institutions, Haryana, India
[2]Faculty, Electronics and Communication, Galaxy Global Group of Institutions, Haryana, India

ABSTRACT

With the ever-increasing development of multimedia requests, protection is a vital subject in contact and storage of pictures, and encryption is one the methods to safeguard security. Picture encryption methods endeavor to change early picture to one more picture that is hard to understand; to retain the picture confidential amid users, in supplementary word, it is vital that nobody might become to understand the content lacking a key for decryption. Furthermore, distinct and reliable protection in Storage and transmission of digital pictures is demanded in countless requests, such as cable-TV, online confidential photograph album, health imaging arrangements, martial picture contact and confidential video sessions, etc. In order to fulfill such a task, countless picture encryption methods have been proposed. The encryption portion can be requested by employing an easy design that merely consists of frank mathematical procedures (AND, OR, XOR, XNOR, advancing, swapping). The Algorithm outperformed all the picture encryption algorithms encompassing RSA. Even the period intricacy of the algorithm is enhanced considerably, the algorithm is in finished 2-3x faster than RSA established Picture Encryption.

Keywords: *Security, Image encryption, Block based Ciphers, Chaotic systems.*

1 .CRYPTOGRAPHY

Cryptography [1] is the science of employing mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive data or send it across insecure webs (like the Internet) so that it cannot be elucidate by anybody except the aimed recipient. The consequence of forceful cryptography is cipher text that is extremely tough to decipher lacking ownership of the appropriate decoding tool. One should contemplate, next, that forceful cryptography should grasp up rather well opposing even a tremendously ambitious cryptanalyst. Who's truly to say? No one has proven that the strongest encryption obtainable nowadays will grasp up below tomorrow's computing manipulation.

1.1. HOW DOES CRYPTOGRAPHY WORK?

A cryptographic algorithm, or cipher, is a mathematical purpose utilized in the encryption and decryption process. A cryptographic algorithm works in combination alongside a key—a word, number, or phrase—to encrypt the plaintext. The alike plaintext encrypts to disparate cipher text alongside disparate keys. The protection of encrypted data is completely reliant on two things: the strength of the cryptographic algorithm and the secrecy of the key [2]. A cryptographic algorithm [3], plus all probable keys and all the protocols that make it work contain a cryptosystem. PGP is a cryptosystem.

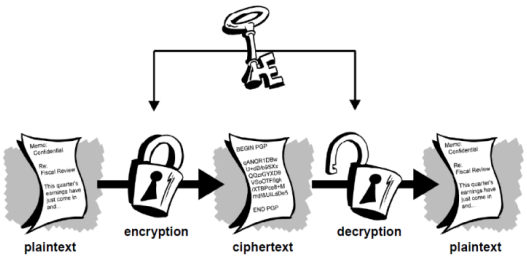

Figure- 1: Conventional encryption

1.2. CONVENTIONAL CRYPTOGRAPHY

Figure 1.is an illustration of the standard encryption procedure. The chaotic picture encryption [4] might be made by employing properties of disorder encompassing deterministic agents, unpredictable conduct and non-straight change. This believed prompts routines that can in the interim give protection limits and a finished discernible check, which could be suitable in a couple of demands. An alternate momentous examination nowadays is the manner by that to safeguard the licensed change of mass media substance in sight and sound systems. To grasp the enumerated difficulties, the two momentous picture protection advances are underutilizing:

(a) Image encryption procedures to give end-to-end security when dispersing advanced substance over a mixture of disseminations systems, and
(b) Watermarking systems as an instrument to accomplish copyright insurance, proprietorship follow, and verification.

In this paper, the flow scrutiny endeavors in picture encryption procedures concentrated concerning chaotic strategies are examined.

Interactive mass media protection as a law is given by an arrangement or a set of methods utilized to safeguard the sight and sound substance. These arrangements are intensely concentrated concerning cryptography and they inspire whichever correspondence protection, or protection opposing robbery (Digital Entitlements Association and watermarking), or both. Correspondence protection of computerized pictures and text established elevated mass media might be fulfilled by method for average symmetric key cryptography. Such mass media might be dealt alongside as parallel gathering and the whole data could be encoded employing a cryptosystem, for example, Elevated Encryption Average (AES) or Data Encryption Average (DES). As a law, after the interactive mass media data is static (not a constant streaming) it can have indulged as an average binary data and the consented encryption procedures could be utilized.. At present, there are countless adjacent picture encryption calculations, for example, Arnold map [5], Tangram algorithm [6], Baker's makeover [7], Magic 3D square makeover [8], and affine makeover [9] and so on.

1.3. Preliminaries

- **Plain Text**

The original message that the person wishes to communicate with the other is defined as plain text. In cryptography the actual message that has to be send to the other end is given a special name as plain text.

- **Cipher Text**

The message that cannot be understood by anyone or meaningless message is what we call as cipher text. In cryptography the original message is transformed into non-readable message before the transmission of actual message.

- **Encryption**

A process of converting plain text into cipher text is called as encryption.. The process of encryption requires two things—an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption.

- **Decryption**

A reverse procedure of encryption is shouted as decryption. It is a procedure of changing cipher text into plain text. The procedure of decryption needs two things—a decryption algorithm and a key.

- **Key**

A Key is a numeric or alpha numeric text or could be a distinct symbol. The key is utilized at the period of encryption seizes locale on the plain text and at the period of decryption seize locale on the cipher text. *

1.4.Purpose of cryptography

Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

- **Confidentiality**

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

- **Authentication**

The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

- **Integrity**

Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

- **Non Repudiation**

Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

- **Access Control**

Only the authorized parties are able to access the given information

1.5. Classification of Cryptography

Encryption algorithms can be classified into two broad categories—Symmetric and Asymmetric key encryption.

A. Symmetric Encryption

In symmetric cryptography the key utilized for encryption is comparable to the key utilized in decryption. There are assorted symmetric key algorithms such as DES [10], TRIPLE DES [11], AES [12], RC4 [13], RC6 [14], BLOWFISH [15]. The symmetric algorithms are of two kinds: Block ciphers and Stream ciphers

- **Block ciphers**

A block cipher [16] is a purpose that charts n bit plain text blocks to n bit cipher text blocks; n is shouted the block length .Use of plain text and cipher text blocks of equal size avoids data development. An n bit block cipher is a function E: $V_n \times K \rightarrow V_n$ such that for each key $\mathbb{K} \in K$, E (P; $\mathbb{K}$) is an invertible mapping (the encryption function for$\mathbb{K}$ from V_n to V_n, written $E_{\mathbb{K}}(P)$. The inverse mapping is the decryption function, denoted by $D_{\mathbb{K}}(C)$. $C = E_{\mathbb{K}}(P)$ denote that cipher text C results from encrypting plain text P under$\mathbb{K}$.

- **Stream Ciphers**

Stream ciphers [17] are a vital class of encryption algorithms. They encrypt individual acts (usually binary digits) of a plain text memo one at a period, employing an encryption makeover that varies alongside time. Stream ciphers are usually faster than block ciphers in hardware, and have less convoluted hardware circuitry .Stream .ciphers are usually categorized as being synchronous or self-synchronizing.Synchronous Stream Ciphers is one in which the key stream is generated independently of the plain text message and of the cipher text and *S*elf-synchronizing Stream Ciphers the key-stream is generated as a function of the key and a fixed number of previous cipher text digits.

B. Asymmetric encryption

Asymmetric cryptography or public-key cryptography is cryptography [18] in which a pair of keys is utilized to encrypt and decrypt a memo so that it arrives securely. Initially, a web user receives an area and confidential key pair from a certificate authority .Any supplementary user who wants to dispatch an encrypted message can become the aimed recipient's area key from a area directory. They use this key to encrypt the memo, and they dispatch it to the recipient. After the recipient gets the memo, they decrypt it alongside their confidential key, that one else ought to have admission too.

2. PROPOSED ALGORITHM

In our Thesis, we have designed a new image encryption algorithm for bulk of image data. Our Proposed Algorithm has basically two steps. Take two images which are to be transmitted over the network with security and then combine those two images to make one image by using the most significant bits of both images. In our project, we have worked on 256- gray level image. One pixel of this type of image takes 8 bits for storage.

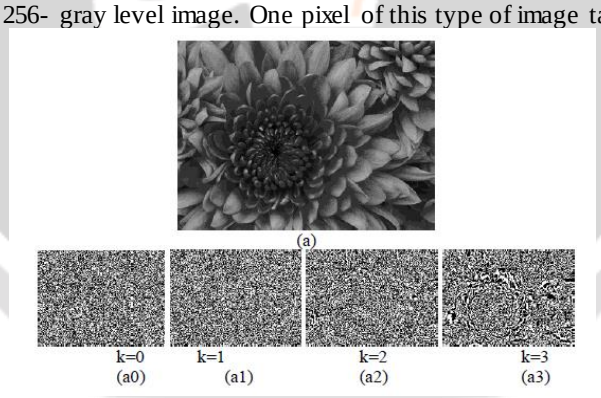

Fig. -2:1(a) shows an 8 bit gray-scale image and Fig.1(a0) through (a7) are its eight 1-bit planes.

It is observed from the figure that the four highest order bit planes, especially the last two, contain a significant amount of the visually significant data. The lower order planes contribute very less.

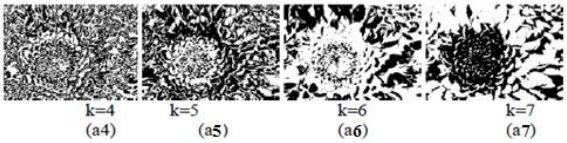

Fig.- 3 :shows the image formed from four most significant bit planes.

It is not visually differentiated from original image. This technique can reduce 50% storage and transmission cost.

Fig.-4: Images reconstructed using bit planes 8,7,6,5

2.1. Key Expansion Process

The key development procedure, that involves convoluted mathematical procedures (multiplication, permutation, transposition and rotation) to produce keys for the encryption procedure, is requested at the decoder. This advanced the computational burden to the decoder and indirectly, thi s will aid to rise the lifespan of the sensor nodes. Though, the generated keys have to be sent securely to the encoder for the encryption process. Overall, the procedure of algorithm consists of four main blocks:

- Key Expansion Block;
- Key Management Protocol;
- Encryption Block;
- Decryption Block.

Key development is the main procedure that is utilized to produce disparate keys for encryption and decryption. Disparate procedures are gave in order to craft confusion and diffusion. This is to cut the potential of frail key as well as to rise the key strength. The round keys (Kr) are derived from the input cipher key by way of the key schedule. The procedure consists of two components: key development and round key selection. The key development performs logical procedures (XOR, XNOR), left advancing (LS), matrix multiplication employing fix matrix (FM), permutation employing P-table and transposition employing T-table. The methodical block diagram of key development and round arranging is shown in Fig.2. The input cipher key (K) is a linear array of 64 bits, that is tear into 4 half's of 16 bits. Every single 16 bit is coordinated in to a 4*4 matrix row-wise on that left shift (LS) procedure is applied[19]. The resultant is next coordinated in a 4*4 matrix column wise and logical procedures (XOR, XNOR) are next performed. The output aftermath of these procedures are joined to form a 64 bit linear array. The obtained 64 bits are next bypassed across P- table and are coordinated in 4*4 matrix row-wise on that left shift (LS) procedure is gave later. The left advanced matrix is next increased alongside a fix matrix (FM) that transforms the 16 bits data into 64 bits. The transformed 64 bits are next coordinated row-wise and left shift (LS) is gave on it. Every single leftshifted 64 bits are next tear into four column-wise 16 bit blocks on that AND & XOR procedures are gave to change them to a solitary 16 bit block. Nowadays the generated 16 bit blocks are more sub tear in to 4 bits coordinated column wise and XOR procedure is requested to produce the 4 bit keys. These keys are utilized by substitution and transposition methods on the 16 bit blocks to produce 4 sub keys (K1, K2, K3, K4) of 16 bits that will be utilized in the early four encryption rounds. The fifth sub key (K5) is generated by XOR the 4 sub keys and will be utilized in the fifth encryption round.

3. RESULTS ANALYSIS

We have used four images in our project for comparison of image encryption schemes on the three parameters - **Encryption Quality, Correlation Coefficient and Entropy**. Images used are-

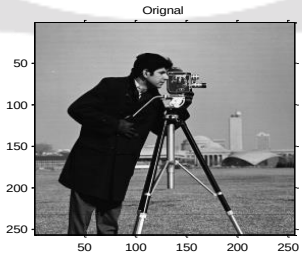

Fig-5: Image of a Cameraman taken for encryption, Encryption with various algorithms is available for this simage

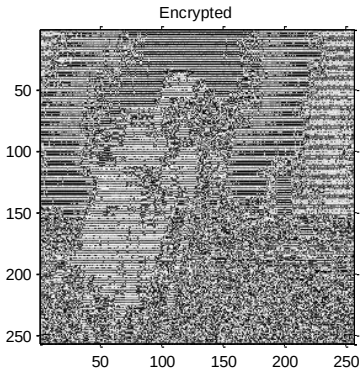

Fig.- 6 : Encrypted Image after Block Encryption

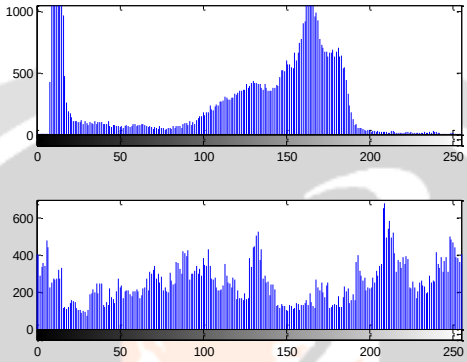

Fig-7: Histogram of Entropy of the image the upper histogram is original Entropy and the lower is achieved after application of proposed work

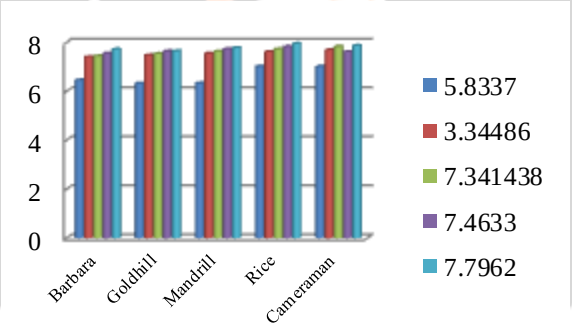

Chart-1: Correlation of all images compared using all algorithms, proposed work was better for all given images

Table-1: Comparison table between RSA and Proposed Algorithm only using Entropy Values

S.no	Image	RSA	Proposed
1	Lena	2.30285	1.302846
2	Barbara	2.42612	1.426124
3	Goldhill	2.44915	1.449154
4	Mandrill	2.37231	1.372308
5	Rice	2.29546	1.295462
6	Cameraman	2.31862	1.318616

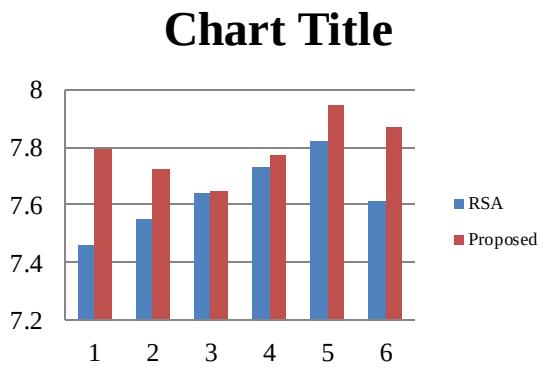

Chart-2: Perceived Entropy of the algorithm is much higher than RSA

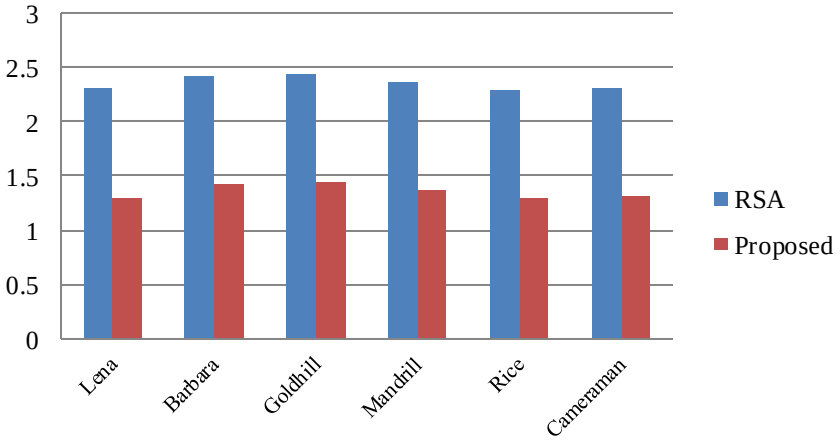

Chart-3*:* Time Complexity of the algorithm is much smaller than RSA, making it Twice as fast as RSA

Encryption and decryption consume a substantial number of time. As the encryption portion is requested by employing an easy design that merely consists of frank mathematical procedures AND, OR, XOR, XNOR, advancing, swapping. The Algorithm outperforms all the picture encryption algorithms encompassing RSA. Even the period intricacy of the algorithm is enhanced considerably, the algorithm is in finished 2-3x faster than RSA established Picture Encryption.

4. CONCLUSION AND FUTURE SCOPE

In this work we counsel a novel low-complexity symmetric cryptographic algorithm. It is industrialized established on the block encryption construction. Public key cryptography is an change and is an unavoidable portion of nearly all protection protocol and application. Being able to debate a public hidden amid two mechanisms online lacking the demand of each transaction of hidden data crafted a breakthrough in safeguard network/internet communication. Nevertheless hypothetically it is probable to find the public hidden from the obtainable area data, it will seize exponentially longer period making it usefully impossible. It is the belief in age-old mathematics, that discovering an facile method for reverse procedure of one-way purpose is unlikely, keeps the area key cryptography going. In upcoming we will work on multimedia Encryption such as AVI, MPEG and H.264 established videos, there additionally exists a potential.

5. REFERENCES

[1]. Buchmann, Johannes. Introduction to cryptography. Springer Science & Business Media, 2013.
[2]. Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." Theoretical computer science 560 (2014): 7-11.
[3]. Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.
[4]. Zhang, Leo Yu, Xiaobo Hu, Yuansheng Liu, Kwok-Wo Wong, and JieGan. "A chaotic image encryption scheme owning temp-value feedback." Communications in Nonlinear Science and Numerical Simulation 19, no. 10 (2014): 3653-3659.
[5]. Ye, Guodong, and Kwok-Wo Wong. "An efficient chaotic image encryption algorithm based on a generalized Arnold map." Nonlinear dynamics 69, no. 4 (2012): 2079-2087.
[6]. Qi, Dongxu, Wei Ding, and Huashan Li. "Tangram algorithm: Image transformation for storing and transmitting visual secrets." In Proc. Of the 5th International Conference on Computer-Aided Design & Computer Graphics, International Academic Publishers, vol. 1, p. 11. 1997.

[7]. Carrière, Philippe. "On a three-dimensional implementation of the baker's transformation." Physics of Fluids (1994-present) 19, no. 11 (2007): 118110.
[8]. Zhang, Yun Peng, Shuai Wang, Peng Xu, Liang Cao, and Yi Wang. "A New Image Cipher Algorithm Based on Chaos." In Applied Mechanics and Materials, vol. 427, pp. 1781-1784. 2013.
[9]. Dong, Ping, and Nikolas P. Galatsanos. "Affine transformation resistant watermarking based on image normalization." In Image Processing. 2002. Proceedings. 2002 International Conference on, vol. 3, pp. 489-492. IEEE, 2002.
[10]. Yun-Peng, Zhang, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, and Dai Wei-di. "Digital image encryption algorithm based on chaos and improved DES." In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, pp. 474-479. IEEE, 2009.
[11]. Hämäläinen, Panu, Marko Hännikäinen, TimoHämäläinen, and Jukka Saarinen. "Configurable hardware implementation of triple-DES encryption algorithm for wireless local area network." In Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP'01). 2001 IEEE International Conference on, vol. 2, pp. 1221-1224. IEEE, 2001.
[12]. Lu, Chih-Chung, and Shau-Yin Tseng. "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter." In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on, pp. 277-285. IEEE, 2002.
[13]. Mousa, Allam, and Ahmad Hamad. "Evaluation of the RC4 Algorithm for Data Encryption." IJCSA 3, no. 2 (2006): 44-56.
[14]. Wu, Kaijie, and Ramesh Karri. "Idle cycles based concurrent error detection of RC6 encryption." In dft, p. 0200. IEEE, 2001.
[15]. Mousa, Allam. "Data encryption performance based on Blowfish." In ELMAR, 2005. 47th International Symposium, pp. 131-134. IEEE, 2005.
[16]. Rogaway, Phillip, MihirBellare, and John Black. "OCB: A block-cipher mode of operation for efficient authenticated encryption." ACM Transactions on Information and System Security (TISSEC) 6, no. 3 (2003): 365-403.
[17]. Ekdahl, Patrik, and Thomas Johansson. "A new version of the stream cipher SNOW." In Selected Areas in Cryptography, pp. 47-61. Springer Berlin Heidelberg, 2002.
[18]. Gaubatz, Gunnar, Jens-Peter Kaps, and BerkSunar. "Public key cryptography in sensor networks—revisited." In Security in Ad-hoc and Sensor Networks, pp. 2-18. Springer Berlin Heidelberg, 2004.
[19]. Xing-Yuan Wang, Sheng-Xian Gu , Ying-Qian Zhang ,"Novel image encryption algorithm based on cycle shift and chaotic system",2014