International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Image Enhancement Of Adaptive Encryption And Decryption Logic Design Using Cryptography

[1]Michael Cholines Pedapudi, [2]S Baba Fariddin, [3]S Ravindra
[1]*Associate Professor, Dept Of ECE, A.M Reddy Memorial College Of Engineering And Technology,Narasaraopet, A.P, India.*
[2,3]*Assistant Professor, Dept Of ECE, St.Marys Women's Engineering College, Guntur, Andhra Pradesh, India*

Abstract: Now a day's Cryptography is one of the broad areas for researchers; because of the conventional block cipher has lost its potency due to the sophistication of modern systems that can break it by brute force. Due to its importance, several cryptography techniques and algorithms are adopted by many authors to secure the data, but still there is a scope to improve the previous approaches. So in this paper a adaptive encryption and decryption logic using Blowish algorithm. It exploits the human visual system to read the secret message from some overlapped shares. This technique overcomes the disadvantage of complex computations required in traditional cryptography.

Key Words*:* Blowish algorithm, cryptography, Encryption, Decryption.

1. INTRODUCTION

One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication [1-8]. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

The necessity of information security within an organization has under gone major changes in the past and present times. A crypto system is an algorithm, plus all possible plain texts, cipher texts and keys. There are two general types of key based algorithms: symmetric and public key. Public Key algorithms use two keys, one key for encryption and the other for decryption. One key can be called as public key which can be declared public and the other one is private that is, the key is known only to the particular participating party. And also public key cryptography can be used for digital signing as it supports authentication of users. The information encrypted with one key will only be decrypted with the other key. Since Authentication of the users is very important in applications like ecommerce and other similar applications, public key cryptography is of much use.

An algorithm is unconditionally secure if, it is difficult to recover the plain text in spite of having substantial amount of cipher text. In such circumstances, only a one time pad is unbreakable in a cipher text only attack, simply by trying every possible key one by one and by checking whether the resulting plain text is meaningful. If the length of the key is k, then the processing complexity is given by 2k .It means that 2 k operations are required to break the algorithm. A desirable property of any encryption algorithm is that a small change in plaintext or the key should produce significant change in cipher text. Such an effect is known as avalanche effect. The more the avalanche effects of the algorithm, the better the security. It may also find weakness in a crypto system that identifies patterns which can be useful in knowing the previous results.

Basically, crypto system has been made to generate two algorithms which provide security to data transmitted. The first algorithm considers a random matrix key which on execution by a series of steps generates a sequence. This sequence is used a sub key to build three different encryption models. Each model can be used for encryption of data. The second algorithm considers not only the key but also initialization vector and a timestamp to generate sub keys which are used for encryption process. DES is a 56 bit key encryption algorithm, if we proceed by brute force attack, the number of keys that are required to break the algorithm is 256. But by differential crypto analysis, it has been proved that the key can be broken in 247 combinations of known

plain texts. By linear crypto analysis it has been proved that, it could be broken by 2 41combinations of plain text. With probabilistic encryption algorithms, a crypto analyst can no longer encrypt random plain texts looking for correct cipher text. Since multiple cipher texts will be developed for one plain text, even if he decrypts the message to plain text, he does not know how far he had guessed the message correctly. The sub key is added to the individual numerical values of the message to generate cipher text.

Complexities can also be expressed as orders of magnitude. Thus known the algorithm, known the cipher text it is quite difficult to generate the matrix key. In this model a sequence is generated and this sequence is substituted for the plaintext to generate cipher text. Depending on the key, the sequence will be generated. We will identify the variations in the sequence generated, by slight variations in the key. Thus we can identify the variations in the cipher text by slight variations in the key considered. We will also identify the variations in the cipher text by slight variations in the plain text. For example, considering different cases for slight variations in the key. The characters of plain text is replaced by set of basins based on chosen base value. The basins are replaced by random values of the corresponding basins. This provides the necessary strength to the algorithm. Thus known the algorithm, known the cipher text it is quite difficult to generate the matrix key.

2. RELATED WORK

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or cleartext) into cipher text (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are i) Secret Key Cryptography which is also known as Symmetric Key Cryptography and ii) Public Key Cryptography which is also known as Asymmetric Key Cryptography. In other words, if the same key is used for encryption and decryption, we call the mechanism as Symmetric Key Cryptography. However, if two different keys are used in a cryptographic mechanism, wherein one key is used for encryption, and another, different key is used for decryption; we call the mechanism as Asymmetric Key Cryptography. In secret key cryptography, a single key is used for both encryption and decryption. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret.

In Security-as-a-Service model the security is delivered as a commodity through the cloud. The security is provided as one of cloud services through the cloud service delivery model in place of on-premise security implementations. The Security-as-a-Service model can increase the capability of existing on premise solutions. It can work with them in a hybrid manner. The idea here is to implement Intelligent and Transparent Encryption- Decryption as a cloud service. The user can use this service by accessing it through browser. The algorithm is made intelligent by classifying the Encryption-Decryption process into multiple Encryption levels.

The levels are classified as per the protection level needed by the user. The levels used in proof of concept (POC) implementation here are low, high and custom level. The encryption and decryption is done for user files. The objective also is to make the process of Encryption-Decryption transparent to the user application. In low level protection the symmetric AES128 algorithm is used with key being generated from passphrase provided by user. In high level mode two types of protection viz. AES-256 algorithm with higher key size and RC6-256 algorithm is used. In custom level the user is given a choice to choose from a variety of encryption algorithms or their combinations as desired viz. DES, Triple DES, Blowfish etc. The novelty in the approach is that the POC is integrated with other Security-as-a-Service options to provide a portal through which various security services can be provided

As services consumption is extended to mobile nodes some of the issues arising are protection and user privacy. Services that are consumed on the mobile node can be data, processes, and application states. Safeguarding these services can be a major requirement for certain enterprises such as healthcare. For instance, while it is efficient for mobile devices to be used to support remote healthcare delivery, it is also a requirement to protect the mobile health record in order to ensure privacy. In this regard, data level security must be applied to the backend, the communication protocol, and the mobile hosted health record. The need for data privacy can be seen in other enterprises such as e/m-commerce, homeland security, banking etc. Thus, services encryption and decryption (encryption decryption) methodologies have been employed over the years to enforce security.

However, when applications that are running on the mobile device consume high energy, the mobile will

die early and this can potentially lead to services unavailability. The concern that has been gravely ignored is the energy consumption cost of data encryption-decryption on battery-powered devices such as smart phones and tablets. In this article the emphasizes on protecting or encrypting data before it moves to the cloud so that it remains protected at rest and in use. The paper emphasizes to use sufficient durable encryption strength algorithms that comply with standards used for files that are maintained internally. The paper also recommends encryption of data in cloud databases. The key management issue has also been given due importance in this paper from Cloud Security Alliance.

The key management and distribution issues in symmetric key cryptography have been minimized by using the passphrase for generation of keys. The users still have to exchange their passphrase using some secure mechanism. Asymmetric algorithms can also be used for protection of resources. The users will have to share their public keys with each other as usual for availing the Encryption-Decryption services. In paper, the Encryption has been defined as one of the category that can be provided as cloud service.

3. LITERATURE SURVEY

Adams, C et.al examines the cryptographic security of the CAST-256 symmetric block encryption algorithm. The CAST-256 cipher has been proposed as a candidate for the Advanced Encryption Standard currently under consideration by the U.S. National Institute of Standards and Technology (NTST). It has been designed for a 128-bit block size and variable key sizes of up to 256 bits to suit AES requirements. Specifically consider the cryptographic security of the cipher in relation to the cryptanalytic property of diffusion and the cryptanalysis techniques of linear and differential cryptanalysis. Weidong Shi et.al present a novel technique to hide the latency overhead of decrypting counter mode encrypted memory by predicting the sequence number and pre-computing the encryption pad that we call one-time-pad or OTP. In contrast to the prior techniques of sequence number caching, our mechanism solves the latency issue by using idle decryption engine cycles to speculatively predict and pre-compute OTPs before the corresponding sequence number is loaded. This technique incurs very little area overhead. In addition, a novel adaptive OTP prediction technique is also presented to further improve our regular OTP prediction and pre-computation mechanism. This adaptive scheme is not only able to predict encryption pads associated with static and infrequently updated cache lines but also those frequently updated ones as weAlKalbany, A et.al presents a hardware implementation of the algorithm, using field programmable gate arrays (FPGA). In this work, the authors discussed the algorithm, the implemented micro-architecture, and the simulation and implementation results. Moreover, a detailed comparison with other implemented standard algorithms was presented. In addition, the floor plan as well as the circuit diagrams of the various microarchitecture modules was presented.

Shiguo Lian et.al proposed a block cipher based on the chaotic standard map, which is composed of three parts: a confusion process based on chaotic standard map, a diffusion function, and a key generator. The parameter sensitivity of the standard map is analyzed, and the confusion process based on it is proposed. A diffusion function with high diffusion speed is designed, and a key generator based on the chaotic skew tent map is derived. Some cryptanalysis on the security of the designed cipher is carried out, and its computational complexity is analyzed. Experimental results show that the new cipher has satisfactory security with a low cost, which makes it a potential candidate for encryption of multimedia data such as images, audios and even videos. Guerreiro, Ana Maria G et.al explores the applicability of using an artificial Spiking Neural Network with a symmetric blockcipher. The goal is to develop a novel neural block cipher where the keys are generated by a spiking neural network and can have any desired block length. With the new algorithm the private keys do not have to be exchanged and present a stronger process of key scheduling. The system allows a rapid change in encryption keys and a network level encryption to be done at very high speed without the problem of factorization of other systems. The block cipher will be transformed in a public cryptosystem, less vulnerable to brute force attacks, and it is hoped to be also resistant to linear attacks since the spiking neuron network architecture brings non-linearity to the encryption/decryption process.

Iain Devlin, Alan Purvis introduces Deluge, a second generation FPGA based key search system that specifically targets stream ciphers. The economically feasible implementation described is in dramatic contrast to other attack techniques and lends weight to the argument that brute-force attacks are underestimated in the security evaluation of cipher designs. Moreover with exhaustive search substantially cheaper than state guessing it is suggested that the practice of designing the state to be twice key length is excessive. Debasis Das and Abhishek Ray deals with the Cellular Automata (CA)

in cryptography for a class of Block Ciphers through a new block encryption algorithm based on Reversible Programmable Cellular Automata Theory. The proposed algorithm belongs to the class of symmetric key systems. The encryption algorithm present in this paper is constructed using programmable CA based on rules. The rules specify the evolution of the CA from the neighbourhood configuration to the next state. In Cellular Automata, rules are being selected to reduce the circuit complexity. This work ensures to generate 2256 potential keys which means that a brute force attack impossible. This algorithm also uses 128 bit block size which, implies an increase in security but may slow down the encryption/decryption process.

Anantha Kumar, Kondra, U.V Ratna Kumari, introduced a new solution that helps to identify the errors in the shares and to verify the authentications. The CRC algorithm and VC scheme with error diffusion method generator the quality of the shares diffuses the error and provides security against the threats like modification of the message, fabrication interception etc. The author developers an encryption method to construct color [EVC] scheme with synchronization. It synchronization the position of the pixels that's Carrey visual color channels of original images across the color channels. So as to retain the original encryption cryptanalysis is also performed to show security concern of the method. M.karolin, Dr.T.Meyyappan, Information hiding in the communication spectrum became a critical task. The Visual Cryptography is a type of cryptography that allows the image to be divided into multiple numbers of shares called transparent shares and then transmission of images. The intruder hence cannot understand the distorted image and thus the data communication becomes secured. The Floyd – Steinberg dithering algorithm is used to manipulate the 256 color code image to reduce it to 16 standard colors code image.

4. PROPOSED SYSTEM

In this work a model is going to be used which develops data distributed over identified value which is used as nonce. The process is repeated for different timings which are used as time stamps in the encryption mechanism. The process is repeated for different timings which are used as time stamps in the encryption mechanism. This model is free from differential crypto analysis and since basins with different and variable values are mapped to the characters of plain text to form the cipher text, it is also free from linear crypto analysis. This algorithm is completely free from cipher text, known plain text, chosen plaintext, chosen cipher text attacks. This algorithm is also free from public key attacks. And also the given algorithm is free from differential and linear crypto analysis, which makes it suitable in data encryption.

The new encryption algorithm is based on the concept of Poly alphabet cipher which is an improvement over monoalphabetic technique. In this algorithm one character of plain text is replaced by set of values from different basins. Thus a polyalphabetic is maintained. The algorithm that is going to be discussed in this work is going to generate a Sequence. The algorithm considers a matrix key and executes a sequence of steps which generates this sequence. From the remaining basins each basin represents one character. Each Character in the plain text is replaced by a corresponding basin value. Thus the cipher text obtained becomes impossible to be broken without knowing the key.

Visual cryptography is a type of cryptography in which images can be securely encrypted by dividing them in a distorted image called transparent shares and transmitted physically by printing these shares on transparency sheets to the intended users. Visual cryptography assumes many forms such as for grayscale images, black and white images as well as color images. The basic model of visual cryptography for color images consists of three phases. The first phase to realize color visual cryptography scheme is to print the color in the secret image on the shares directly. It performs larger pixel expansions which reduce the quality of the divided color image. The second phases converts a color image into black and white image on the three color channels (Red, Green, Blue or equivalently cyan, magenta, yellow) respectively, and then applies the black and white visual cryptography scheme to each of the color channels.

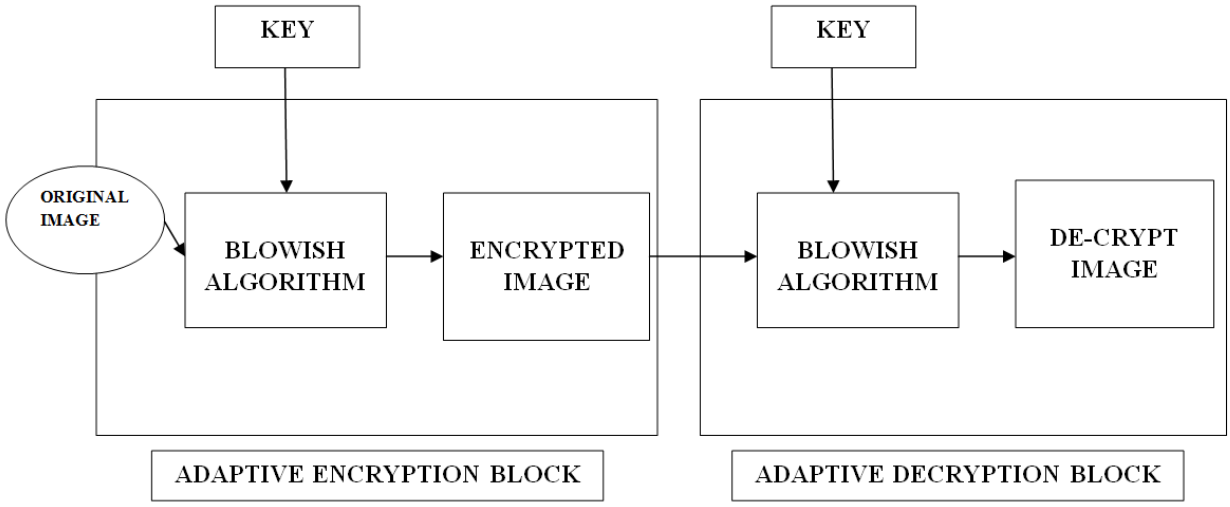

Fig. 1: PROPOSED SYSTEM

The above figure (1) shows the architecture of proposed system. Here Original image and encryption key are input to the encryption process. The bit stream of the original image is separated into blocks length of Blowfish algorithm. The encrypted image is divided into the same block length of blowfish algorithm from top to bottom. The blocks are subjected to decryption function. The same encryption key is used to decrypt the image by reversing the function of sub keys is reversed. Bruce Schneier designed blowfish as a fast, free different to existing encryption algorithms. Since then it has been analyze considerably, and it is slowly fast acceptance as a strong encryption algorithm. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no authorize is required. The basic operators of blowfish algorithm include table lookup, addition, and XOR. Blowfish is a cipher based on Feistel rounds, and the plan of the F-function used amounts to a generalization of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64-bit block cipher and is optional as a alternate for DES.

Blowfish is a fast and free algorithm and can encrypt data on 32-bit microprocessors. So in this paper, we are implementing blowfish algorithm which is strongest and fastest in data processing store evaluate to other algorithms. Blowfish algorithm is really secured because it has longer key length 32 to 448 bit (more no of key size).

Basically**, in** existing system they used attribute-based encryption and decryption. As they are using three levels user, role, attribute so depends on that they are providing security and efficiency. As we are using user, role and attribute they have their own disadvantages. To overcome this we introduced proposed system. The total probability of chances depends on the number of bits. As the bits are changing we are getting the number of combination. In local level the total channels are low. So we are using key-one as limited number of bits. Key-two used for national level encryption with more number of bits compared with local level. The total wanted channels in national level is more compared with local level. So we use more bit length than local level.

5. RESULTS

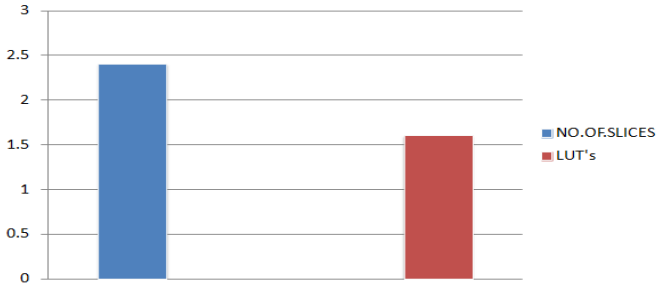

Fig. 2: NO. OF SLICES AND LUT'S IN PROPOSED SYSTEM

6. CONCLUSION

In this paper, a adaptive encryption and decryption technique is proposed to secure the transmitted digital images. This technique divides the image into multiple printable shares which exploits the human vision system. It overcomes the computational complexity of traditional cryptography. Blowfish algorithm with 64-bit block cipher and key values in the range 32 to 448 is adopted for securing the image. As the numbers of hackers are less. So, we provide less bits to choose combination cases. This process of security will be high in national, higher in international, very high in special case. So finally concluding that proposed system provides different security level depends on application and it is better than Existed system.

REFERENCES

[1] Shankar, K., and P. Eswaran. "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography." China Communications 14.2 (2017): 118-130.

[2] Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.

[3] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, "Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications Vol. 4, No. 2, April 2010.

[4] Sougata Mandal, Sankar Das and Asoke Nath, "Data Hiding and Retrieval using Visual Cryptography", in International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 1, April 2014, pp:102 – 110.

[5] J. Tamilarasi, V. Vanitha, T. Renuka, "Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion", in International Journal of Scientific & Technology Research, Volume 3, Issue 4, April 2014, pp:126-131.

[6] Anantha Kumar Kondra, Smt. U. V. Ratna Kumari, "An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion", in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, pp.1090- 1096.

[7] M.karolin Dr.T.Meyyappan,"RGB Based Secret Sharing Scheme in Color visual cryptography", in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2015.

[8] Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[9] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004.

[10] M. Naor and A. Shamir, "Visual cryptography," Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, pp. 1 - 12, 1995.

[11] L. N. Pandey and Neeraj Shukla, "Visual Cryptography Schemes using Compressed Random Shares", in International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62 – 66.

[12] Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique." Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.