A New Randomized Cryptographic Image Base Key Generation

Prof.V.R.Raut PRMIT&R, BADNERA

B.P.Mohod PG STUDENT, PRMIT&R, BADNERA

Abstract*:- Information sharing via digital media is a vital and challenging one. Those challenges are addressed with the help of cryptographic and stenographic techniques.Cryptography is basically securing the data or information during the communication between different systems and parties . The Algorithm and Key are require to provide the security of data during communication in cryptography. The confidentiality and integrity of the data in communication depends partially on algorithm and partially on key. The size of key in cryptography is limited due to human memorizability.The main objective of this paper is to increase the security in communication by encrypting the information with the key generated by using an images in a session manner. Based on the session type a key is generated which is used for encrypting and decrypting the messages which is further transmitted and received between two sides. The length of the key changes in every session according to the session type. This is a reliable and flexible way to generate the key to secure the information which is transferred on the networks and it is easy to implement. This method try to ensures the prevention of guesses or breaking the key and provides a more secure way for information encryption.

Index Terms: **Cryptography**, **Key generation, Images, RGB image, Encryption,Decryption**

I. INTRODUCTION

We cannot think about a world without communication. With faster Growth of the internet makes communication easier and transferring of messages become secure. The cryptography has been proposed to ensure the confidentiality and authenticity of the information. The encryption key must be long,so it is difficult to remember the key and even storing the key in a database or in a file may be insecure. In addition the protection of the confidentiality of encryption keys is important issues to be handle. This issue can be efficiently solved by generating the key before starting the process of encryption and decryption, rather than storing it. Here we will use an image for generating the key. The main objective of this study is to increase security in communication by encrypting the information using a key that is created using a color image. Cryptography presents various methods for taking readable data and transforming it into unreadable data for the purpose of secure transmission, and then use a key to convert it back into readable data when it reaches to its destination [8]. Cryptography is one of the important building blocks of computer security [3]. The need of reliable and effective security mechanisms to secure information systems is increase day by day due to the rising magnitude of identity theft in our society.Although cryptography is a powerful tool to achieve information security, the security of cryptosystems relies on the fact that cryptographic keys are secret and these keys are known only to the right user. In secure communication, key generation phase suffer from many challenges and this problem can be solved if the sender and the receiver share the key in any secure form or if they generate the keys at time of encryption and decryption separately, thus, the concept of generating the key from an image came to the role [2]. The main objective of this method is to create a new algorithm to secure connection between users by using the content of an image. The algorithm uses a color RGB image to generate a key which will be used in the encryption and decryption operations.

Our algorithm is distinguished from the other ones as the generated key length is depend on the size of the message and the session type. This makes the encryption algorithm more powerful. The proposed algorithm is simple to implement and easy to use. This reliable and efficient security mechanism is to protect the information from the intruder.

II. RELATED WORK

Tawfiq S.Barhoom et al. [1] have proposed and produced an experimental result on the method which is more secure than traditional cryptographic processes. Cryptography provides security to the data which is transmitted between the communicators through a shared media. When the keys used for the encryption and decryption are too long, it is difficult to be remembered and unable to guess by the attacker. Storing the secret key in a database or in a file is insecure. The security of the cryptographic system relies on the fact called cryptographic keys which are secret and known only to the authorized user. Thus the new concept of Cryptography is being determined based on the key generated directly from an image stored in the database and the process of key generation is based on sessions. This method creates more complexity to crack or guess the keys by using the cryptanalysis techniques .So it impossible to break the algorithm unless we know the image from database, color image channel, the key value and the session type. This process has an advantage that key length varies according to the length of the message and it is more flexible on any RGB images.

B.Santhi et al. [2] have proposed a method which overcome the disadvantages of several methods such as steganography

and cryptography which deals with difficult in the size of information to be transferred and with encryption using the keys which is difficult in remembering and can be easily cracked. Thus, the author has determined the concept which should be flexible and should not be compromises in the strength of key generated and information security, their by proposing the secret key which is being generated from an image. Using the Gray Level Co-occurrence properties of the image, a 56-bit sub-key is generated. Therefore the sub- key is initialized as secret key to the encryption and decryption of the message which is to be transmitted securely and efficiently between the communicators. The strength of the key is much better than the key generation process of other algorithms because the key is based on the image properties, which is impossible to predict.

Dr.R.Seshadri et al. [3] have proposed an efficient cryptographic key generation algorithm using biometrics. As the conventional cryptographic keys are large they are very difficult to remember. Hence they have integrated biometrics like fingerprint, face, voice, iris etc. along with cryptography for an efficient secure key generation. In this paper finger prints are used for generating cryptographic keys. Finger print patterns are used for key generation as they are stable for a person's life time. Three models are used in the proposed system they are key release, key binding and key generation. In key release mode the key and the biometric are stored separately in a template and the key will be released only if the biometric matches. In key binding mode a cryptographic biometric matching algorithm is used for authentication and key release. In key generation mode key is generated based on the biometric data directly and it s not stored in the database.

Amrita sahu et al [4] has proposed an algorithm using cryptographic key generation to secure digital images. A palm image is taken for the generation of cryptographic key. The image is divided into a number of pixels. The binary values for the pixels are calculated and the binary values are converted into decimal form. The pixel grouping of pixels is done based on the decimal value calculated and they are grouped with the pixels having similar decimal values. Once the group is formed RMS value for each group is calculated. The RMS is the Root Mean Square method also called as the quadratic mean. Using the RMS value cryptographic key is generated. The generated cryptographic key is used to encrypt and decrypt the image. Thus an image can be transferred in a secure way over the network. Bit xor method is used to encrypt and decrypt the image with the cryptography key generated.

Lifang Wu et al. [5] have proposed an algorithm to share the pictures through a shared medium. Face biometrics is the most effective biometric feature universally known because it uniquely identifies the differences in the face features. During the encryption phase the face key features are extracted. Based upon the optimal bit order and the binarization which are saved in the look-up table the bio-keys are generated. The generated bio keys are then encrypted. The face images are unequalled because of the noise in the camera. It is solved by error-correct- code (ECC). While transmitting from the sender side the encrypted message is sent with the ECC code. At the receiver end the decrypted data is obtained using ECC code and the bio-keys are generated back with the help of the look-up table. By this approach a secure and stable binary key is generated for the transmission of images.

Damir Omerasevic et al [6] have proposed an algorithm in which the plaintext is shared with the help of images by establishing the cryptographic key. The size of the key and the space is limitless. The main objective of the paper is to share messages with the help of multimedia files. Any multimedia file of bigger size compared to the messages is chosen. The sender will choose an image from the set of images and selects the position for attaching the plain text. The plain text is then XOR-ed with the set of selected bits in the image and sent to the receiver with the details of the position of file and the index. Each message is encrypted separately with the unique key which is similar to one time padding. Selecting the multimedia file and the position where the plaintext is to be attached is selected using an algorithm. This method generates cryptographic keys that are not based on any particular size.

III. SESSION BASED KEY GENERATION ALGORITHM

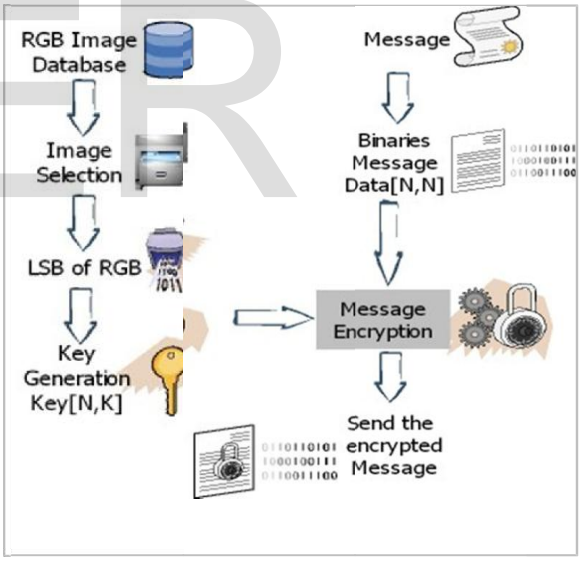

Figure 1: sender side block diagram.

A.Image Database:

In this phase as we use sessions, twenty four images are used on hourly basis. The images are the set of a color image. Once the sender and the receiver are ready for communication they have access to the image data base. Only legitimate sender and receiver can access the image database.

B.Key Generation:

Key generation is based on the image stored in the database according to the session type. Consider the pixel value of an image and extract one channel from RGB at a time. It may be either a red channel or green channel or blue channel. The values of the components are stored in an array with the size of array is p*q. where p and q are the resolution of an image. The generated key is based on the following steps. In our algorithm we considered all the channels form which key generation takes place.

1. ***Red channel:*** Only the diagonal values of the array are considered whose indexes (N) are N%8=0.

   i. The diagonal pixels are considered which is again stored in an array.

   ii. Root Mean Square value for those diagonal values are calculated

   iii. RMS=√ (a 12 +a 22 +a 32 +...+a n2)/n, Where a=diagonal pixels stored in the array.

   iv. The generated RMS value is considered as a part of the key and then it is stored in to a variable.

2 .Green channel:

i. Extract the green channel values and store it in an array.

ii. Sum up all the pixel values in a zigzag manner starting from 0x0 to (n-1) x (n-1),where n=size of the image and then store all the summed up value in a variable.

3 .Blue channel:

Repeat the steps of the red channel. Now, the value get from the red channel is appended with the value get from the green channel and thus the blue channel value is also appended to generate the key.

C. Encryption:

The sender encrypts the confidential message using the RC5 algorithm . The key generated using an image is used as input for the encryption. As the images are considered on hourly basis, if the encryption is done on n^{th} hour then n^{th} image in the image database is considered. Once the encryption is done this encrypted message is sent to the receiver along with the session log. The session log contains the time in which the encryption is done.

D. Decryption:

According to the session log the receiver will consider the image in the image database and generate key from that image which is used for decryption. The generated key and the encrypted message both are send for decryption (RC5 Algorithm) and the original message is extracted.

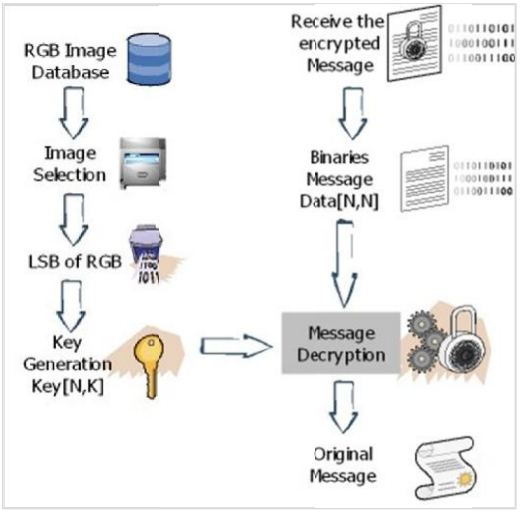

Figure 2: Receiver side block diagram

IV. SECURITY ANALYSIS

A. *Man in the middle attack (MIM)*

MIM attack happens when an intruder actively monitors captures and controls the information. But our algorithm greatly reduces the man in the middle attack. The sender and the receiver are to be authorized first before communication to access the image database. Once when they are authorized no other person is permitted to access the image database, even if the intruder captures the encrypted text it will be hard for him to generate the key. As we use sessions and also keys are generated based on the images it will be hard for him to capture the original message.

B. *Compromised key attack*

Compromised key attack occurs when the intruder generates key based on prediction and gains access over the confidential message. He can add, delete or modify the original text. But our proposed system also handles the compromised key attack. The keys that are generated are of variable length and are based on the images taken for encryption. As the keys are not of fixed length the intruder hardly predicts the key.

C.System attack

System attack is based on the security approach implemented in the system. As our proposed system concentrates on confidential message transfer it enforces the implementation of a good security to prevent the

system attack. The sender and the receiver are to be authorized to access the secure image database. A key of variable length is created based on the images and the key is taken as a seed for generating cipher text. They keys need not have to be transferred in the network they can be generated in the respective ends.

V. CONCLUSION

The communication technologies have major impact in this world hence to ensure security while transferring of information is important. Our proposed system focuses on generating key based on images. The generated key need not have to be stored. It can be generated anywhere using the image and the session. This creates more complexity to crack or guess the keys by using the cryptanalysis techniques. To break this algorithm, we need to know the images database,color image channel,the key value and the session type.This method is more secure than traditional cryptographic processes.The algorithm process has an advantages of key generation based on session and the key length varies according to the message length.This process is more flexible that any RGB image can be used for key generation as the key generation is directly based on the image content.

VI. REFERENCS

[1] Tawfiq S.Barhoom, Zakaria M.Abusilimiyeh, "A Novel Cryptography Method Based on Image for Key Generation". Proceedings on the Palestinian International Conference on Information and Communication Technology, 2013-IEEE, pp: 71-76.

[2] B.Santhi, K.S.Ravichandran, A.P.Arun and L.Chakkarapani, "A Novel Cryptographic Key Generation Method Using Image Features". Proceedings on the Research Journal of Information Technology2nd International Conference on Adaptive Science & Technology, 2012, Pp: 88-92.

[3] Dr.R.Seshadri, T.Raghu Trivedi, "Efficient Cryptographic Key Generation Using Biometrics". Proceedings on the International Journal on Computer Technology and Application, ISSN: 2229-6093, Vol-2, Pp: 183-187.

[4] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for securing Digital Image". Proceedings on the International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Pp: 285-291.

[5] Lifang Wu, Xingsheng Liu,Songlong Yuan, Peng Xiao Tawfiq S.Barhoom,Zakaria M.Abusilimiyeh , "A Novel Key Generation Cryptosystem Based on Face Features". Proceedings on ICSP, 2010-IEEE, Pp: 1675-1678.

[6] Damir Omerasevic,Narcis Behlilovic, Sasa Mrdovic,"CryptoStego-A Novel Approach for Creating Cryptographic Keys and Messages", 2013-IEEE, Pp: 83-86.

[7] Asha Ali, LiyamolAliyar andNisha V K, "RC5 Encryption Using Key Derived From Fingerprint Image", Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference, 28-29 Dec. 2011

[8] Priyanka.M, Lalitha Kumari.R, Lizyflorance.C and John Singh. K "A New Randomized Cryptographic Key Generation Using Image"International Journal Of Engineering Science and Innovation Technology(IJESI) Volume 2,Issue6,November2013